

UNCLASSIFIED



**Net-Enabled Command Capability  
CERTIFICATION AND ACCREDITATION (C&A)  
PROCESS**

**Version 1.0**

**1 October 2008**

**CM#: NECC-CA-00185**

Prepared by:

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

In Collaboration with USJFCOM and the NECC Component Program Managers for the Navy,  
Air Force, Army, Marine Corps, and DISA

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

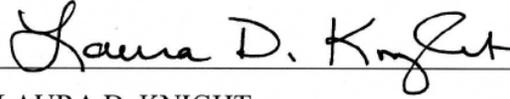
DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

UNCLASSIFIED

UNCLASSIFIED

**APPROVAL PAGE**

Approved by:



Date:

10/3/08

LAURA D. KNIGHT

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

**REVISION HISTORY**

<b>REVISION NUMBER</b>	<b>REVIEWER / ORG</b>	<b>CHANGES</b>	<b>REVISION DATE</b>	<b>DATE ENTERED</b>	<b>NAME OF PERSON ENTERING CHANGE</b>
1.0	DLB/JPMO	Put document into NECC template	30 Sep 08		Dustan Brown

TABLE OF CONTENTS

**APPROVAL PAGE.....II**

**REVISION HISTORY ..... III**

**1 INTRODUCTION..... 1**

**2 PURPOSE..... 1**

2.1 HOW TO USE THIS DOCUMENT..... 2

2.2 ASSUMPTIONS AND CONDITIONS..... 2

2.3 APPLICABILITY..... 2

**3 GENERAL INFORMATION ..... 3**

3.1 INFORMATION ASSURANCE WORKFORCE TRAINING REQUIREMENTS ..... 3

3.2 IA MEETINGS & PLANNING ACTIVITIES ..... 3

3.2.1 *DIACAP Team Meetings*..... 3

3.3 NECC IA MANAGEMENT TOOLS ..... 4

3.3.1 *Federal Development & Certification Environment (FDCE)*..... 6

3.3.2 *Enterprise Mission Assurance Support Service (eMASS)*..... 6

3.3.3 *Vulnerability Management System (VMS)*..... 7

**4 C&A PROCESS ..... 7**

4.1 DIACAP TEAM ROLES ..... 7

4.1.1 *NECC Designated Accrediting Authority (DAA)*..... 8

4.1.2 *NECC Certifying Authority (CA)*..... 9

4.1.3 *User Representative*..... 10

4.1.4 *IA Validation Team*..... 10

4.1.5 *NECC Information Assurance Manager (IAM)*..... 11

4.1.6 *CPMO Information Assurance Officers (IAOs)*..... 12

4.1.7 *Matériel Developer*..... 13

4.2 NECC DIACAP WORKFLOW ..... 13

4.3 INITIATE AND PLAN IA C&A ..... 16

4.3.1 *Assign IA Requirements*..... 16

4.3.2 *Register the CM*..... 17

4.3.3 *Conduct Analysis of System Life Cycle Status & Configuration*..... 17

4.4 IMPLEMENT & VALIDATE ASSIGNED IA CONTROLS..... 19

4.4.1 *Conduct Self Assessment*..... 19

4.4.2 *IA Validation Readiness Reviews*..... 19

4.4.3 *Validate IA Requirements* ..... 20

4.4.4 *Compile Validation Results in DIACAP Scorecard*..... 20

4.4.5 *Perform IA Risk Assessment* ..... 21

4.4.6 *Develop Security Plan of Action & Milestones (POA&M)*..... 22

4.5 CERTIFICATION RECOMMENDATION & ACCREDITATION DECISION ..... 23

4.5.1 *Certification Recommendation* ..... 23

4.5.2 *Accreditation Decision* ..... 24

4.5.3 *NECC Capstone DIACAP Package*..... 25

4.5.4 *Maintain Authorization to Operate and Conduct Reviews* ..... 25

4.6 PORTS, PROTOCOLS & SERVICES MANAGEMENT ..... 27

4.7 DECOMMISSION..... 27

4.8 PROGRESSION THROUGH FDCE STAGES ..... 27

4.8.1 *Development Stage* ..... 27

4.8.2 *Developmental Piloting Stage*..... 27

4.8.3 *Operational Piloting Stage*..... 28

4.8.4 *Network Operations*..... 28

**APPENDIX A – REFERENCES ..... 29**

UNCLASSIFIED

**APPENDIX B – ACRONYMS .....30**  
**APPENDIX C – GLOSSARY OF TERMS .....33**  
**APPENDIX D-H .....38**  
**APPENDIX D - SYSTEM IDENTIFICATION PROFILE TEMPLATE .....38**  
**APPENDIX E - DIACAP IMPLEMENTATION PLAN TEMPLATE .....38**

**LIST OF FIGURES**

Figure 1: NECC IA Roles ..... 8  
Figure 2: DIACAP Workflow..... 16

**LIST OF TABLES**

Table 1: IA Management Tools ..... 4  
Table 2: Categories and Descriptions ..... 23

## 1 INTRODUCTION

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD) principal command and control (C2) capability that will be accessible in a net-centric environment and will focus on providing element commanders with the data and information needed to make timely, effective, and informed decisions.<sup>1</sup> NECC capabilities utilize the Federated Development and Certification Environment (FDCE) which provides the policies, processes, and infrastructure to allow Capability Modules (CMs) to be progressively developed, refined, tested, certified, and accredited in increasingly rigorous situations leading to an operational deployment.<sup>2</sup>

As CMs are developed, certified, and accredited in a net-centric environment, they will evolve in parallel with changing community requirements for consumption on the Secure Internet Protocol Router Network (SIPRNet) and Non-Classified Internet Protocol Router Network (NIPRNet) architectures.

All CMs (including the specific version, increment, and spiral) accredited through the NECC Certification and Accreditation (C&A) process are evaluated for the impact to the NECC portfolio of capabilities and managed in the NECC Capstone accreditation.

## 2 PURPOSE

This document describes the C&A process through which all NECC capabilities will be accredited. The NECC C&A process describes the NECC implementation of existing DoD C&A policies, instructions, and directives, and it is based on the DoD Information Assurance Certification and Accreditation Process (DIACAP). This document identifies C&A procedures for use by the NECC Designated Accrediting Authority (DAA), Certifying Authority (CA), Joint System Team (JST), Capability Module Test Team, Component Program Management Office (CPMO) and Materiel Developer. The NECC C&A process is closely aligned with NECC Systems Engineering (SE) and Test & Evaluation (T&E) processes. The C&A process is also integrated into the stages of CM development and fielding:

- Development
- Developmental Piloting
- Operational Piloting
- Network Operations (NetOps)

The Information Assurance (IA) requirements identification and certification testing and analysis is planned early in the Software Development Life Cycle (SDLC), allowing for the implementation of security solutions within the beginning stages of life cycle development.

Earlier insights of security implementations are identified through the NECC SE process, allowing for a better understanding of the C&A Level of Effort (LOE) for each CM prior to funding allocation for development.

---

<sup>1</sup> <http://www.disa.mil/necc/index.html>

<sup>2</sup> [http://fdce.netcentriclab.com/FDCE\\_Portal/appmanager/FDCE/FDCE](http://fdce.netcentriclab.com/FDCE_Portal/appmanager/FDCE/FDCE)

Once the CM enters the FDCE, the FDCE allows the tracking of progress with the developer implementation of IA requirements. FDCE also allows visibility of validation results by the NECC CA for making certification recommendations and providing the body of evidence needed for the Designated Accrediting Authority (DAA) to assert an accreditation decision.

The artifacts that make up the NECC DIACAP Package will be made accessible to the DIACAP Team through the FDCE, reducing the time required to reach an accreditation decision.

This process also describes requirements and procedures for CMs to be provisioned onto the Global Information Grid (GIG).

## **2.1 How to Use This Document**

Sections 1 and 2 describe the purpose, assumptions, and conditions applied during the usage of the document itself.

Section 3 gives a detailed description of the tools used throughout the NECC C&A process. It also describes the collaboration methods of the NECC community in which the NECC C&A process applies.

Section 4 defines the C&A roles and responsibilities and additional communities that participate in the C&A policy development for NECC. Section 4 also outlines details of the NECC C&A approach, including key C&A activities, such as the development of the NECC DIACAP Package artifacts, and accreditation boundaries of each capability.

## **2.2 Assumptions and Conditions**

An NECC CM may be classified as Unclassified, Secret, or Top Secret. This NECC C&A process addresses the assignment of security requirements for Unclassified and Secret CMs only. CMs classified as Top Secret shall follow procedures defined by the Director of Central Intelligence (DCI).

Each CM will be independently certified and accredited, complete with its own certification letter. This will allow the CM to be hosted at multiple sites without repeating the baseline tests conducted during the certification effort.

## **2.3 Applicability**

The NECC C&A process applies to NECC stakeholders contracted by the NECC Joint Program Management Office (JPMO) to develop and supply capabilities within the NECC environment. The intended audiences within the NECC stakeholder organizations are varied and include the following:

- Personnel assigned to the Joint Forces Command (JFCOM) as the NECC User Representative to represent the Warfighter mission needs.
- IA professionals assigned to C&A roles within NECC, including personnel assigned to CMTTs, JPMO, Component Program Management Offices (CPMOs), CA office, and DAA office.
- Personnel assigned to a NECC CPMO assigned as the lead materiel developer for a NECC CM.

- System owners that already possess an accreditation for a system and are issued a work package that identifies the need for a NECC accreditation.
- Engineers and architects designing and implementing logic for services accessible in the NECC environment.

### **3 GENERAL INFORMATION**

#### **3.1 Information Assurance Workforce Training Requirements**

DoD 8570.1-M, Information Assurance Workforce Improvement Program provides guidance and procedures for the training, certification, and management of the DoD workforce conducting IA functions in assigned duty positions. In accordance with DoD 8570.1-M, all IA requirements to be performed by contractors shall be identified in their statement of work/contract. These statement of work and contract documents must stipulate that compliance with the certification requirements described in DoD 8570.1-M for those serving in IA capacities is mandatory.

#### **3.2 IA Meetings & Planning Activities**

##### **3.2.1 DIACAP Team Meetings**

The NECC DIACAP Team meetings are designed to bring communities of interest into a single meeting to discuss the activities of the C&A effort, and to gain an understanding of the IA requirements, testing methodologies, and expectations related to the C&A effort. A DIACAP Team meeting for each CPMO will be held weekly, or as necessary, to ensure sufficient collaboration is maintained for the CMs. The CPMO DIACAP Team meetings will be scheduled and managed by the assigned CPMO Information Assurance Officer (IAO). All meetings will be announced and tracked through the Defense Knowledge Online (DKO) IA site.

Attendance of weekly CPMO DIACAP Team meetings is mandatory for the team members assigned to the DIACAP roles identified within this section. If an individual is not available to attend, the team member shall send a substitute to represent their interests.

At a minimum, the CPMO DIACAP Team meeting agenda shall include a schedule and status report of each CM. These meetings will ensure that time sensitive items are being updated throughout CM development. Meeting minutes will be documented and posted to the DKO IA site.

**3.3 NECC IA Management Tools**

NECC IA management tools have been selected to effectively manage IA requirements, certification evidence, and C&A workflow. During tools analysis, IA stakeholders evaluated the functionality provided by enterprise tools available throughout the DoD along with leveraging capabilities being used by the NECC program. This section describes the tools used for IA management within NECC.

A summary of the tools analysis and the activities these tools support is identified in Table 1.

**Table 1: IA Management Tools**

		<i>Capabilities /Tools</i>	VMS	eMASS	FDCE	Templates (DKS & NECC)	Validator DB
DIACAP Package	Vulnerability Management	IA Controls - Tracking Findings	✓	✓			
		IA Controls - Recording POA&M	✓	✓			
		IA Controls - POA&M Electronic Workflow	✓	✓			
		IA Controls - Non-Functional Allocated		✓	✓		
		STIG - Tracking Findings	✓				
		STIG - Recording POA&M	✓				
		STIG - POA&M Electronic Workflow	✓				
		STIG - Findings Reporting	✓				
		STIG – Assignment				✓	
		IAVM - Notification, Tracking, and Oversight	✓				
	IAVM - POA&M	✓					
		System Identification Profile (SIP)		✓		✓	
	DIACAP Implementation Plan (DIP)		✓		✓		

UNCLASSIFIED

		<i>Capabilities /Tools</i>	VMS	eMASS	FDCE	Templates (DKS & NECC)	Validator DB
		Residual Risk Report					✓
		DIACAP Package Electronic Workflow		✓			
Other		Centralized Access w/ Access Control	✓	✓	✓		
		TECC Assertion and Validation			✓		
		Artifact Electronic Storage		✓			
		Certification Body of Evidence Electronic Storage	✓				

### **3.3.1 Federal Development & Certification Environment (FDCE)**

The FDCE allows the tracking of progress and visibility by the NECC CA for making certification recommendations and providing the body of evidence needed for the Designated Accrediting Authority (DAA) to assert an accreditation decision. FDCE is conceived as a virtual environment that is intended to address the challenges associated with concurrent and distributed service management. Its purpose is to provide the policies, processes, and infrastructure that allow capabilities to be progressively refined, tested, and certified in increasingly rigorous situations leading to an operational environment.

The FDCE is used to track and monitor NECC C&A and other test activities by NECC stakeholders assigned to functional roles with the appropriate need-to-know.

The NECC Test, Evaluation, and Certification Criteria (TECC) is managed in the FDCE. For specific guidance in managing the IA criteria included in the TECC, refer to the NECC TECC Standard Operating Procedure.

### **3.3.2 Enterprise Mission Assurance Support Service (eMASS)**

eMASS facilitates robust, measurable IA Program Management (PM) through the following capabilities:

- Security-process management and reporting based on compliance with IA Controls
- Standardized information exchange to facilitate dynamic connection decisions
- Workflow automation
- Simplified management of the entire C&A process from C&A package submission through completion
- Traceable systems-security engineering across the entire system-development life cycle
- Facilitation of regulatory and IA management-reporting requirements, such as those contained in the Federal Information Security Management Act (FISMA)

The NECC instantiation of eMASS is maintained by USSTRATCOM, NECC DAA and is operational only on the SIPRNet.

Register for an eMASS account on SIPRNet using the following link: <https://emass-joint.csd.disa.smil.mil/Default.aspx> (PKI cert required)

Along with details provided below, additional information is located in the NECC Reference Library eMASS folder.

- NECC DIACAP Team members shall register for the NECC eMASS server through the eMASS administrators (JPMO IA)
- NECC DIACAP Team members will be assigned to the appropriate eMASS roles following eMASS registration and account approval.
- DIACAP artifacts shall be updated in eMASS by the CPMO IAO
- NECC DIACAP workflow enforces DIACAP Package submission by the NECC IAM.

### **3.3.3 Vulnerability Management System (VMS)**

VMS was built in recognition that all DoD agencies require the ability to identify security vulnerabilities, mediate the risks, and track the issues throughout the life cycle of their existence. DIACAP Team members must have access to and be trained in VMS. NECC leverages the SIPRNet instantiation of VMS, which is maintained by DISA. Refer to directions located in the NECC Reference Library for obtaining access to VMS.

- NECC DIACAP Team members shall register for VMS through the NECC IAM
- NECC DIACAP Team members shall also obtain a SIPR PKI certificate to access the system
- VMS shall be used for the tracking of emerging vulnerabilities in accordance with the NECC Information Assurance Vulnerability Management (IAVM) Plan
- VMS shall be used to track the body of evidence resulting from self assessment and validation testing

Access to VMS SIPRNet using the following link: <http://vms.disa.smil.mil> (No PKI cert required)

## **4 C&A PROCESS**

### **4.1 DIACAP Team Roles**

DIACAP establishes the assignment of organizational roles and responsibilities for individuals involved in supporting IA and C&A activities. The DIACAP Team consists of the following roles:

- NECC Designated Accrediting Authority (DAA)
- NECC Certification Authority (CA)
- User Representative
- IA Validation Team
- NECC Information Assurance Manager (IAM)
- CPMO Information Assurance Officers (IAOs)
- Material Developer

Figure 1 represents all NECC IA roles that support NECC CM development efforts, to include DIACAP Team members.

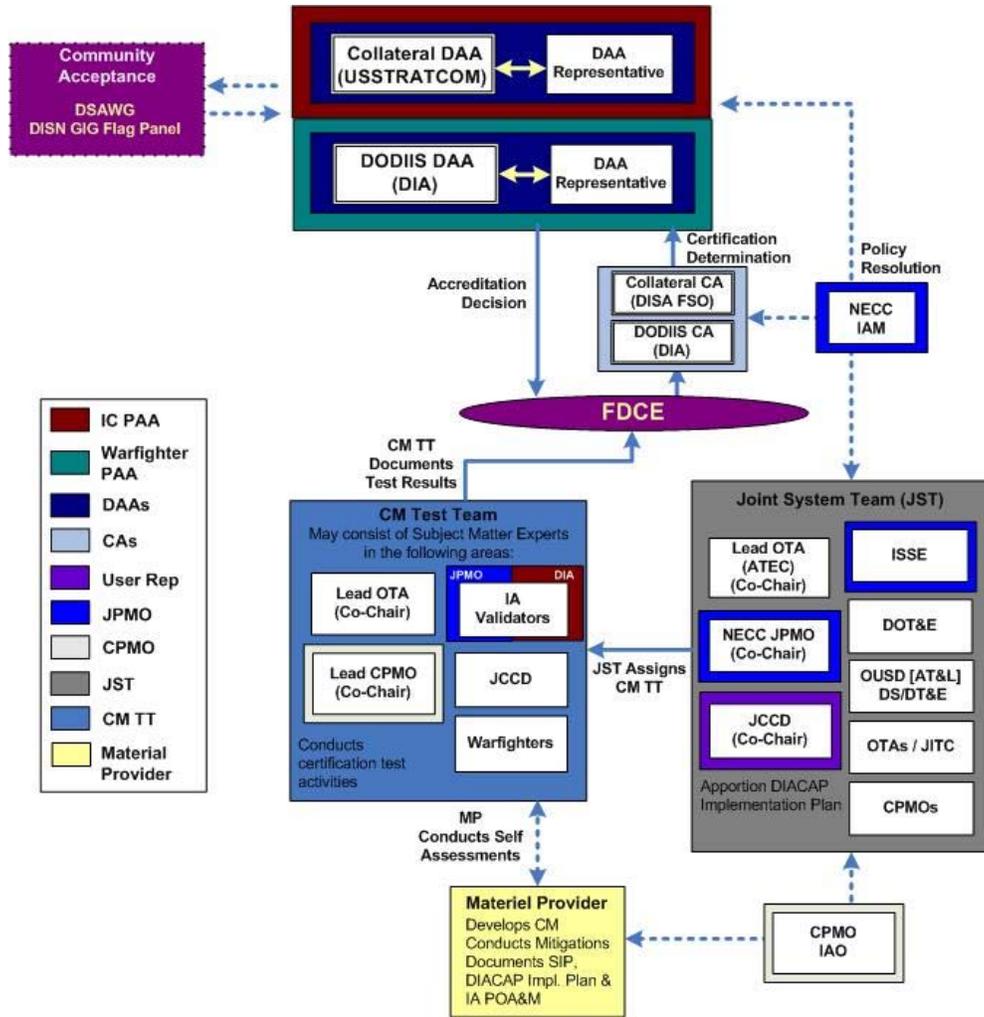


Figure 1: NECC IA Roles

**4.1.1 NECC Designated Accrediting Authority (DAA)**

Deputy Commander of USSTRATCOM has been appointed as the NECC DAA for the accreditation of all non-Sensitive Compartmented Information (SCI) capabilities.

The primary responsibilities of the non-SCI NECC DAA are established in DoDI 8500.2 and DoDI 8510.01. According to this guidance, the NECC DAA shall:

- Enforce the NECC C&A Process and provide update to the process, as necessary.
- Track C&A status of CMs that are included in NECCs baseline through C&A management tools.
- Ensure CMs comply with applicable DoD IA requirements.
- Ensure compliance with the NECC Security Classification Guide (SCG).
- Participate in C&A activities through membership on each CPMO DIACAP team.

## UNCLASSIFIED

- Ensure individuals filling IA positions are assigned in writing, trained, certified, and sign a statement of responsibilities.
- Ensure that NECC IA-related events or configuration changes that may impact accreditation are reported to affected parties, such as Information Owners and DAAs of interconnected information systems.
- Enforce existing agreements between the NECC JPMO and NECC CPMOs requiring timely disclosure of security-related events that could negatively affect the performance of one or more NECC CM.
- Contribute recommendations and guidance throughout the implementation of IA requirements for each CM and accept the certification of each individual IA Control prior to accreditation.
- Determine the acceptable operating risk level for NECC CMs.
- Accept the risks of the capability and authorize inclusion of the certified CM in the NECC Capstone Accreditation.
- Conditionally accept the risks involved in testing of the capability in an operational environment through the issuance of an Interim Authorization to Test (IATT).
- Issue a Denial of Authorization to Operate (DATO) for capabilities operating at an unacceptable level of risk.
- Complete the required DoD DAA training and certification as identified in DoD 8570.1M.

### **4.1.2 NECC Certifying Authority (CA)**

DISA Field Security Operations (FSO) is assigned as the Certifying Authority (CA) for NECC. In addition to the responsibilities established in DoDI 8500.2 and the DIACAP Guidance, the NECC CA shall:

- Participate in C&A activities as a member of the DIACAP team.
- Ensure and oversee a qualified certification cadre to include: IA Validators, analysts, and CA Representatives.
- Perform a comprehensive evaluation of the CMs compliance with security features and safeguards with respect to the IA requirements based on the evidence provided by the IA Validator.
- Ensure all security documentation and testing has been adequately completed.
- Issue a certification recommendation to the DAA that includes an assessment of risk of operating the capability.
- Determine and provide evidence that the overall risk associated with a vulnerability identified during IA certification testing can be reduced due to mitigating factors, such as a specific implementation of Computer Network Defense (CND).
- Ensure that the DIACAP scorecard for each CM is accurate and included in the DIACAP Package.

- Participate in the annual review, recertification, and reaccreditation of the NECC Capstone Accreditation and CMs as required.

#### **4.1.3 User Representative**

Joint Forces Command (JFCOM) is identified as the NECC User Representative. The User Representative represents the operational interests and mission needs of the organizational user community. The User Representative shall:

- Serve as the liaison for the user community throughout the life cycle of the system.
- Participate in C&A activities as a member of the DIACAP Team.
- Assist in defining the Mission Assurance Category (MAC) and Confidentiality Level (CL) and supporting the IA requirements validation process, when required, to ensure mission requirements are met.
- Assist in the development of data management and NECC SCG, as required.
- Assist in the development of role-based access policies for information being processed by the assigned DoD information systems that are consistent with defined enterprise roles and privileges, as required.
- Assist in the development of DIACAP-related information exchange requirements and notification thresholds for data and process owners and system users as required.

#### **4.1.4 IA Validation Team**

As Agents of the CA (ACA), the IA Validator(s) assigned to CMTTs shall interface with the CPMO and perform the following functions:

- Maintains appropriate IA training and certifications compliant with IA workforce requirements (DoD 8570.1-M).
- TPT IA Test Coordinator participates as a member of the Test Planning Team (TPT).
- Provide inputs and changes to the lead Operational Test Agency (OTA) for input into the [Test and Evaluation Master Plan \(TEMP\)](#).<sup>3</sup>
- Analyze and leverages previously conducted IA testing to minimize redundancy.
- Provides status report to the JST, TPT, and CMTT on progress/results of IA testing, as needed.
- Applies risk management at each stage of development to determine level of IA involvement.
- Assures the IA risk analysis and mitigation determination results are provided in Joint Test Report.
- Provides comments/recommendations during the CM apportionment, as well as Capability Provisioning Events (CPE).

---

<sup>3</sup> NECC Increment 1 Capstone Test and Evaluation Master Plan (TEMP), v1.0, 6 August 2007, URL: <https://www.us.army.mil/suite/page/491726>

## UNCLASSIFIED

- Conduct IA certification testing and risk analysis on the CM security configuration and IA implementation.
- Participate in C&A activities as a member of the DIACAP Team.
- Ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate security configuration guidelines.
- Participate in all test planning activities, including planning meetings and working groups.
- Document the IA-related information in the Detailed Test Plan (DTP) for assigned CMs and provide to the materiel developer for use during IA self assessment.
- Document IA test procedures in the DTP to relate the testing standard identified by the DAA and CA.
- Support the materiel developer during IA self assessment.
- Evaluate IA self assessment results to determine if entrance criteria for IA certification testing has been met.
- Support the Information Assurance Validation Readiness Review (IAVRR).
- Scope, coordinate, and schedule IA validation test events.
- Execute CM-level testing and identify all residual risks.
- Coordinate with and assist with CM developer to establish mitigation plans for residual risks.
- Review all C&A documentation to ensure the information is current and accurate.
- Adhere to certification guidance received from the CA and perform actions necessary to complete certification of CMs within the FDCE.
- Coordinate with the CA during the IA risk assessment and elevate any concerns or questions to the CA, as needed.
- Update the Security Plan of Action and Milestones (POA&M) for each CM.
- Initiate DIACAP Scorecard for each CM.
- Compile the certification documentation through validation activities, conduct risk analysis, and document a residual risk report for delivery to the CA as the Comprehensive DIACAP Package. Deliver certification documentation to the NECC IAM in a trusted manner.
- Coordinate with the CA for issuance of a certification recommendation and update of the NECC accreditation in accordance with the NECC C&A Process, DIACAP, and DoDIIS.
- Ensure that compliance monitoring occurs, and review the results of such monitoring.
- Carry out all other required technical certification tasks necessary to implement the C&A process.

### **4.1.5 NECC Information Assurance Manager (IAM)**

The NECC Information Assurance Manager (IAM) shall:

- Implement the NECC security program. Ensures NECC security policies are prepared, maintained, and implemented.

## UNCLASSIFIED

- Maintain appropriate IA training and certifications compliant with IA workforce requirements (DoD 8570.1-M).
- Ensure users are provided annual IA awareness training, and System Administrators (SAs) and IA professional complete appropriate systems security certification in accordance with CJCSM 6510.01 and DoD 8570.1-M.
- Participate in C&A efforts as a member of the DIACAP Team.
- Support the CPMOs in implementing the C&A process.
- Advise and inform the governing DoD Component, Intelligence Community (IC), or Federal Agency on C&A status, information, and issues.
- Comply with information and process requirements for the governing C&A policy guidance.
- Provide direction to the CMTT as needed.
- Coordinate and ensure issues affecting NECC's overall security are addressed in a timely and appropriate manner.
- Participate as a member of the NECC Configuration Control Board (CCB).
- Submit the Comprehensive DIACAP Package to the CA in a trusted manner.
- Ensure the NECC Information Assurance Vulnerability Management (IAVM) plan is current and executed in accordance with governing policy.

### **4.1.6 CPMO Information Assurance Officers (IAOs)**

The CPMO IAO shall:

- Participate in C&A activities as a member of the DIACAP Team.
- Maintain appropriate IA training and certifications compliant with IA workforce requirements (DoD 8570.1-M)
- Coordinate, schedule, and participate in DIACAP Team meetings for CMs under their purview.
- Ensure developers and privileged users have the requisite security clearances and are aware of their IA responsibilities before developing or accessing the software or system.
- Support the SE process prior to work package development to ensure IA requirements are adequately documented in the development statement of work.
- Support the Developer during Preliminary Design Review (PDR) and Critical Design Review (CDR) to adequately assign DISA Security Technical Implementation Guides (STIGs)
- Support the Developer in implementing the C&A process during development and IA self assessment.
- In coordination with the IAM, initiate protective or corrective measures when an IA incident or vulnerability is discovered.
- Ensure that IA and IA-enabled software, hardware, and firmware comply with DOD Directives, guidelines, and instructions, and NSA and NIAP certification procedures as specified in DoDI 8500.1, Section 4.17.

- Ensure that compliance monitoring occurs and review the results of such monitoring.
- Execute the Information Assurance Vulnerability Management (IAVM) process for the respective CMs that have been implemented within their component.
- Ensure that all IA-related documentation is current and accessible to properly authorized individuals.
- Implement and enforce all IA policies and procedures, as defined by security C&A documentation.
- Ensure self assessments for CMs under development are performed as needed.

#### **4.1.7 Materiel Developer**

The Materiel Developer shall:

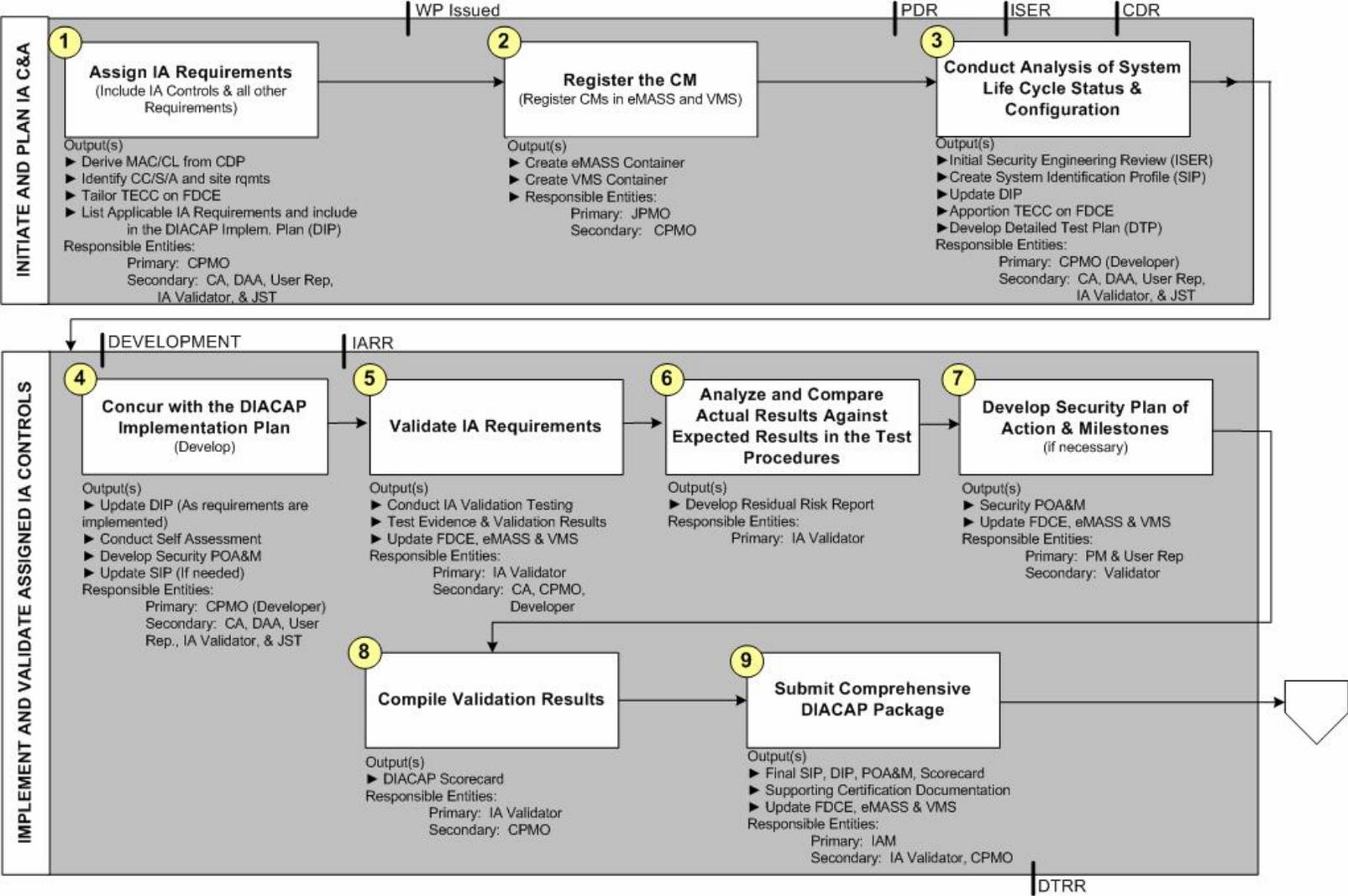
- Participate in C&A activities as a member of the DIACAP Team.
- Ensure personnel comply with DoD 8570.1-M certification and training requirements.
- Ensure all COTS and GOTS IA Products and IA enabled products comply with NSTISSP No. 11.
- Support IA certification test activities in accordance with the DTP.
- Assist and coordinate with the IA validator for test activities.
- Execute IA self assessments.
- Prepare, update, and maintain a Security POA&M that describes how the risks identified will be remediated throughout the development process.
- Prepare, update, and maintain a SIP for each CM.
- Prepare, update, and maintain a DIP for each CM.
- Assert compliance with IA requirements in the FDCE.
- Adhere to all guidelines set forth in the [NECC Developers Handbook](#)<sup>4</sup> and DoD IA guidance.
- Participate in all CPMO DIACAP Team meetings and/or other IA related meetings, as required.
- In coordination with the CPMO, perform self assessments on developmental CMs as necessary.
- Correct security deficiencies as identified in the Security POA&M

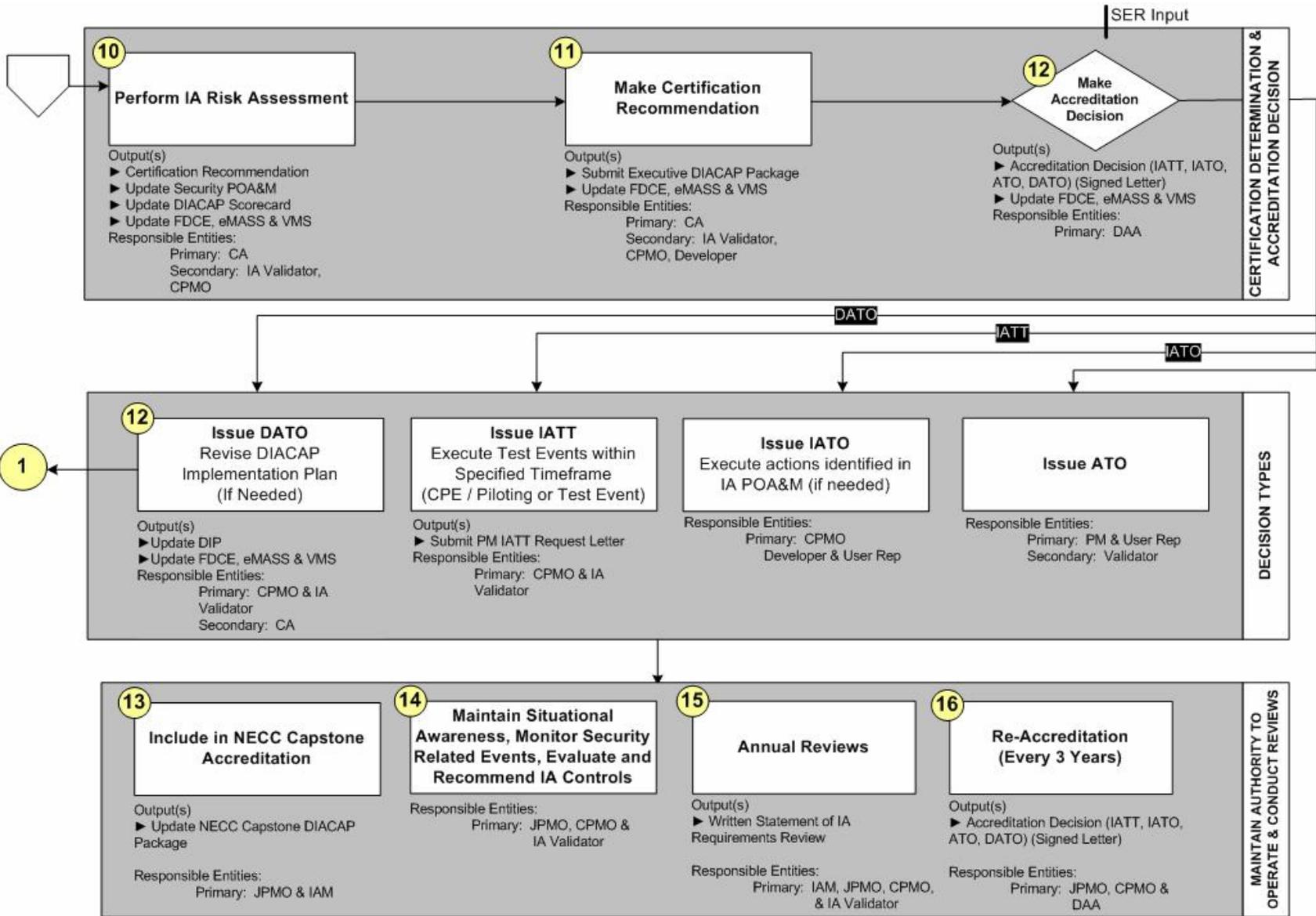
#### **4.2 NECC DIACAP Workflow**

The NECC C&A process follows the traditional DIACAP. The following sections will describe what is included in the diagram below.

---

<sup>4</sup> NECC Developers Handbook, v1.5, 26 September 2008, URL: <https://www.us.army.mil/suite/page/491726>





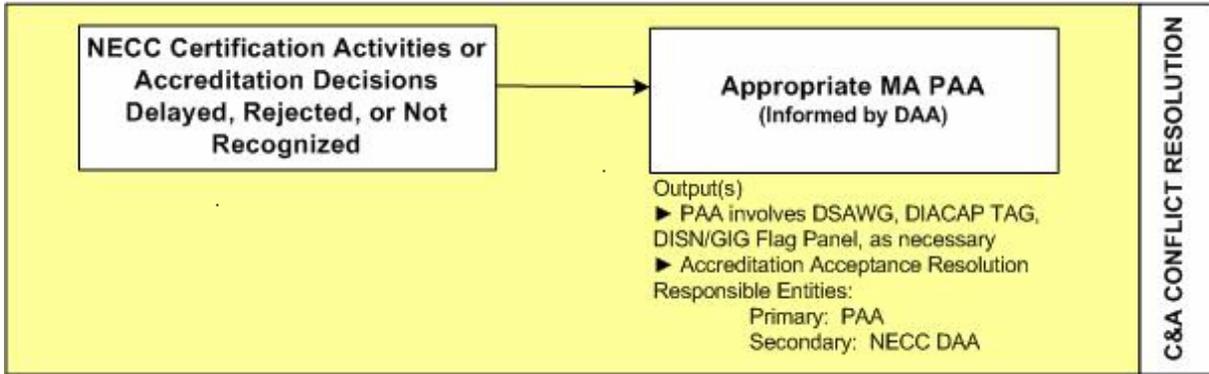


Figure 2: DIACAP Workflow

### 4.3 Initiate and Plan IA C&A

This activity includes registering the system with the governing NECC C&A Management tools, assigning IA requirements based on MAC and CL, identifying the DIACAP Team for the CM, and initiating the CM DIP.

This activity aligns with the NECC Systems Engineering Steps 2-4 and is executed by the NECC Information System Security Engineer (ISSE) in conjunction with the DIACAP Team.

Technical requirements will be included in the Spiral Allocated CM (SACM) Specification during this activity.

#### 4.3.1 Assign IA Requirements

IA requirements are allocated to an individual CM and documented in the Requirements Management System (RMS) and DIACAP Implementation Plan (DIP) for inclusion in the Development Work Package (DWP). The baseline IA requirements are managed by the DIACAP Team using the DIP and are initiated into the DIP by the NECC ISSE. The CPMO IAO will add any additional requirements, if needed, to augment the baseline based on the intended hosting environment.

The DIP may be updated throughout the Preliminary Design Review (PDR), Initial Security Engineering Review, and Critical Design Review (CDR) activities, or once the STIGs, implementation guidance, and requirements derived from the hosting site are identified. As these new requirements are identified, the Development WP and statement of work (SOW) change requests may need to be submitted.

### **4.3.2 Register the CM**

DISA CIO uses the DITPR for IA registration. NECC has been registered as a capstone system within DITPR.

As CM work packages are approved, the DIACAP Team will coordinate the FDCE, eMASS, and Vulnerability Management System (VMS) entries for that CM. The materiel developer (CPMO and Developer) shall complete IA registration for each CM in FDCE. Although the FDCE may already contain baseline information about the CM, specific input of IA-related information is required to adequately determine and manage the risks.

### **4.3.3 Conduct Analysis of System Life Cycle Status & Configuration**

#### **4.3.3.1 Update DIACAP Implementation Plan**

The DIACAP Implementation Plan contains the assigned IA requirements for the CM. The plan also includes the implementation/inheritance status (Inherited, Planned, or Implemented); resources; Estimated Completion Date (ECD); and criteria for entrance into the next CPAS phase. The DIP is a living document which is developed before the PDR, during Step 3 of the SE process and will be continuously updated through the SDLC. The plan also references applicable supporting implementation material and artifacts.

The materiel developer executes the DIP throughout development by implementing IA requirements. If the Developer determines that a specific IA requirement cannot be implemented, they will identify the requirement to the DIACAP Team. The CA will assess the risks associated with not implementing the requirement and the DAA will determine if the mitigating factors are acceptable. All accepted risks will be documented in the IT Security POA&M.

#### **4.3.3.2 Document System Identification Profile (SIP)**

The SIP is generated during the registration process by the materiel developer and becomes part of the DIACAP Package for the CM. The SIP documents the accreditation boundary, security features, architecture description, vulnerabilities, certification plans, and supporting artifacts that express or enforce the programs IA posture of a CM as it is hosted and moves through the various stages of the registration process. System Engineering (SE) artifacts are provided as evidence to support the completion of the SIP.

#### **4.3.3.3 Conduct Preliminary Design Review**

The DIACAP Team shall participate in the Preliminary Design Reviews (PDRs) for all CMs and spirals to evaluate the security features included in the initial design. Refer to the NECC Systems Engineering Plan (SEP) for IA entrance and exit criteria, checklists, and details of the PDR.

#### **4.3.3.4 Conduct Initial Security Engineering Review**

The Initial Security Engineering Review (ISER) shall be conducted when the materiel developer has determined the security features of CM and has documented those details in the System Identification Profile (SIP). The intent of the ISER is for engagement of the DIACAP Team with the development team to verify that the system design meets the intent of the security

requirements and will be implemented in accordance with appropriate security configuration guidance.

The ISER shall be held in conjunction with or immediately following the PDR. Attendees shall include the same audience required for the PDR, to include key members of the development staff. The ISER will be scheduled and coordinated by the lead CPMO IAO.

At a minimum, the materiel developer shall cover the following information, in detail, during the ISER:

- Functional Architecture
- Data Flow
- System Interfaces
- Interconnections
- Ports, Protocols, and Services (PPS)
- Software baseline (Include NSTISSP No. 11 Compliance, COTS, GOTS, source code, open-source, free-ware, share-ware, anti-virus, mobile code, etc.)
- Compliance with Application Security and Development STIG
- Selection of STIGs
- Development, Integration, and Hosting Sites
- Delivery schedule
- Desired accreditation decision
- DIACAP schedule

The following is exit criteria for the ISER:

- Acceptance of the software baseline by the DAA
- Allocation of STIGs for TECC apportionment
- Receipt of the updated DIP
- Receipt of the updated SIP
- Completion of all action items resulting from the PDR and ISER

ISER slide template is available in the FDCE Reference Library.

#### 4.3.3.5 Conduct Critical Design Review

The DIACAP Team shall participate in the Critical Design Reviews (CDRs) for all CMs and spirals to evaluate the security features included in the design. Refer to the NECC Systems Engineering Plan (SEP) for IA entrance and exit criteria, checklists, and details of the CDR.

## 4.4 Implement & Validate Assigned IA Controls

### 4.4.1 Conduct Self Assessment

Self assessments, which are conducted by the materiel developer in coordination with the CPMO, are intended to determine the survivability of security features of the capability, the logic supporting the capability, and layered security supporting the code throughout development. Self assessments shall adhere to the Detailed Test Plan (DTP) provided by JPMO IA.

The purpose of self assessment is to determine the readiness for validation testing and accreditation. This is accomplished by identifying security weaknesses, validating the effectiveness of requirements applied, and implementing mitigation strategies to reduce the threat of the known risks to an acceptable level earlier in development. The following activities shall be conducted during self assessment:

- Execute all automated and manual tests in accordance with the IA DTP
- Execute all Security Readiness Review (SRR) scripts for the applicable STIGs and STIG checklist manual checks
- Vulnerability scan using the agreed vulnerability scanning tools
- IA Requirement Validation
- CPMO IAO will coordinate any required waivers or port exceptions
- Create any required Memorandums of Agreement (MOAs)
- Document all residual risks identified during self assessment in the IT Security POA&M

Self assessment results will be entered into VMS by the CPMO IA SME, used by the CPMO to assert compliance with requirements in the FDCE, and repeated as necessary. Successful completion of IA self assessment is entrance criteria into IA validation testing.

### 4.4.2 IA Validation Readiness Reviews

Information Assurance Readiness Reviews (IAVRRs) must be conducted to evaluate the results of the self assessment and to determine whether the security posture and readiness of a NECC CM or CMs is sufficient for participation in an IA validation test activity.

IAVRRs will be scheduled to align with the CPMO DIACAP Team meeting and included in the IMS for tracking by the JPMO. The lead CPMO IA SME is responsible for coordinating any support needed from the materiel developer.

The IAVRR activity is synonymous with IA Readiness Review (IARR). Any reference to IARRs in any legacy or historical references found in NECC documentation shall follow the guidance contained within this paragraph.

The following is entrance criteria for an IAVRR:

- Self-assessment conducted on all applicable technologies
  - Results of self assessment are entered into VMS
  - Minimal CAT I findings
  - Number of CAT II / III findings meet minimum closure rates

- No vulnerabilities in “Not Reviewed” status in VMS
- Updated DIACAP Package is submitted
  - Up-to-date SIP
  - Up-to-date DIP
  - Up-to-date Security POA&M
- IA requirements are asserted as “Met” on the FDCE

The following is exit criteria for an IAVRR:

- Acceptance of documentation by DIACAP Team
- CA acceptance of mitigating factors for reduction of any CAT I risks
- IA requirements are asserted as “Met” on the FDCE

#### **4.4.3 Validate IA Requirements**

Certification testing occurs when the materiel developer conducts self assessment and IAVRR for the article of test. JPMO IA maintains a central pool of qualified IA Validators authorized to conduct certification test activities.

The JPMO TPT IA Test Coordinator shall assign an IA test lead to participate on the CM Test Team. The CMTT IA test lead shall coordinate test activities with the materiel developer.

Validation includes all tasks related to the execution of the Validation Procedures that are associated with assigned IA Controls. Validation Procedures are maintained through the JPMO and are submitted for inclusion in the DTP for a test event. The DTP will be made available 2-3 weeks after CDR and before self assessment. Each Validation Procedure describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results. It may also include associated supporting background material, sample results, or links to automated testing tools. Actual results are recorded according to the criteria and protocols specified in the Validation Procedure. The body of evidence becomes a permanent part of the comprehensive DIACAP Package, along with any artifacts produced during the validation, e.g., output from automated test tools or screen shots that depict aspects of system configuration. The status of actual results for all assigned Validation Procedures is compiled into a DIACAP Scorecard.

The IA Validator will validate TECC IA requirements asserted in the FDCE as ‘Met’, ‘Not Met’, or ‘Partially Met’ in accordance with the TECC SOP.

#### **4.4.4 Compile Validation Results in DIACAP Scorecard**

The DIACAP Scorecard is a summary report that shows the compliance / non-compliance with the CM’s assigned IA requirements and is intended to convey a certification determination and/or accreditation decision. The DIACAP Scorecard is developed by the IA Validator after IA validation testing and is submitted to the CA in the Comprehensive DIACAP Package. The CA may update the DIACAP Scorecard, if needed.

#### 4.4.5 Perform IA Risk Assessment

The IA Validator drafts the IA Risk Assessment for the CA. The IA Risk Assessment is to be performed subsequent to self assessments and remediation cycles. The IA Risk Assessment includes a summary of categorized findings listed in the test report and an overall risk statement for the system.

The NECC IA Risk Assessment shall contain the following information:

- **Threat Identification:** CPMOs identify circumstances or events that could potentially cause harm to the system. These threat-agents may be natural, human, or environmental.
- **Vulnerability Identification:** CPMOs identify vulnerabilities that threat-agents could exercise. Vulnerability is defined as a flaw or weakness in an information system, system security procedures, or internal controls.
- **Findings Categorization:** CPMOs assign each finding into a Severity Category (CAT) of I, II, or III. During this step, CPMOs must present Risk Assessment artifacts to the JPMO.
- **Countermeasure Recommendations:** Identify countermeasures to mitigate or eliminate the identified risks, as appropriate to the organization's operations.
  - Important factors include:
    - Criticality of the system and its data
    - Likelihood of successful exploitation (how likely is it this vulnerability will be exploited)
    - Magnitude of the impact of an attack (what is the loss experienced if the vulnerability is exploited)
    - Assigned severity code
  - The DIACAP Team may schedule a classified session to discuss the facets of the IA Risk Assessment:
    - Operational consequences
    - Cost/Time Analysis
    - Implementation
    - Sustainment
    - Configuration Management

The IA Risk Assessment reports a list of the IA requirements with associated findings, along with a description of the mitigation, and the logic used to derive the residual risk to the system or network.

Based on the number of findings identified and the threat environment in which the system operates, the overall assessment of residual risks is derived. Analysis is conducted by analyzing each individual risk item using the following guidelines:

- If there is at least one high individual risk, the overall residual risk must be high.

- If there is at least one moderate individual risk, the overall residual risk must be at least moderate.
- If there are only low individual risk items, the overall residual risk is low.
- Medium risks may aggregate to high risk and low risks may aggregate to medium risk if the aggregation of medium or low risks is sufficient to constitute the higher risk level.

#### **4.4.6 Develop Security Plan of Action & Milestones (POA&M)**

A Security Plan of Action and Milestones (POA&M) shall be developed by the IA Validators and maintained by CPMOs to record the status of any corrective actions directed in association with an accreditation decision. The NECC Security POA&M identifies tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan and milestones for completing tasks, along with their scheduled completion dates. Security POA&Ms are permanent records. Once posted, weaknesses will be updated, but not removed, after correction or mitigation actions are completed. Inherited weaknesses are reflected on the Security POA&Ms.

Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system-level Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted.

The NECC DAA is responsible for monitoring and tracking overall execution of system-level Security POA&Ms.

The Lead CPMO is responsible for implementing the corrective actions identified in the Security POA&M and, with the support and assistance of the NECC IAM and CPMO IA SME, provides visibility and status to the DAA, the SIAO, and the governing DoD Component CIO. In order to reflect the complete IA posture of a DoD IS at all times in a single document, the Security POA&M is also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are N/A because of the nature of the system.

The NECC Security POA&M is required for any accreditation decision that requires corrective actions. Security POA&Ms are also required for the following reasons:

- Begin IA Validation Testing. Note: A Developmental Security POA&M is required to be produced before an IAVRR can be held.
- CMs requesting an IATT or IATO. Note: A Security POA&M must be attached to any requests for an accreditation decision.
- CMs operating under an ATO with newly identified (not contained within the current risk analysis) significant security weakness. The CA will determine the security weakness impact through the CCB.
- Security weaknesses identified during an audit or review (e.g., SIPRNet Compliance Visit, IA Red Team Assessment, Inspector General (IG) Review, or annual security review.)

The Security POA&M outlines the security weakness, resources required to mitigate the weakness, milestones in meeting the task, and scheduled completion dates for the milestones.

**4.4.6.1 Finalize Security POA&M**

The CPMO is responsible for executing the continued implementation and progress of risks identified in the Security POA&M, in coordination with the materiel developer. The CPMO shall manage the implementation of the Security POA&M throughout development and will ensure that Security POA&M items are included in the next spiral or software release. The CPMO shall notify the DIACAP Team of any updates or changes to the Security POA&M.

**4.5 Certification Recommendation & Accreditation Decision**

**4.5.1 Certification Recommendation**

**4.5.1.1 Submitting a DIACAP Package to the CA**

The Comprehensive DIACAP Package is submitted to the CA by the IAM using eMASS. Upon direction of the Materiel Developer, the CPMO IAO shall coordinate and schedule an IARR with members of the DIACAP Team. The Comprehensive Package consists of the following artifacts:

- System Identification Profile
- DIACAP Implementation Plan (DIP)
- Supporting Certification Documentation
  - Actual validation results
  - Artifacts associated with implementation of IA controls
  - Risk Assessment
- DIACAP Scorecard
- Security POA&M

**4.5.1.2 Package Processing Priority**

Priorities are determined by the User Representative for packages processed through the CA and DAA. CPMOs are asked to supply priority category, date needed, and supporting justification when submitting the DIACAP Package.

**Table 2: Categories and Descriptions**

CATEGORY	DESCRIPTION
1a	Piloting Event Commitment (Impact date is <= 14 days)
1b	Operational Test Event Commitment (Impact date is <= 14 days)
1c	IATT Change Authorization Request (Impact date is <= 3 days)
2	In CA or DAA Hold Queue > 30 days
3	First In / First Out (normal processing)
Exception 1	Flag Request

#### 4.5.1.3 Processing Status of a DIACAP Package

DIACAP Packages will be stored and processed using eMASS. Testing evidence will also be linked to the FDCE, as they are made available to the CA and DAA for review. Using the DIACAP workflow in eMASS, the DIACAP Package will be routed to the appropriate roles as required throughout the process.

#### 4.5.1.4 Make Certification Determination

The CA representative conducts analysis and validation of the IA Risk Assessment and evaluates the assessment for consideration of any residual risks that may be reduced due to mitigating factors. The CA is the only authorized role allowed to reduce residual risks. The CA provides the overall IA Risk Assessment and recommendation to the DAA for consideration prior to making an accreditation decision and will assert the certification recommendation through eMASS.

### **4.5.2 Accreditation Decision**

The CA shall submit the Executive DIACAP Package to the DAA and it will be tracked through eMASS. The Executive Package consists of the following artifacts:

- SIP
- DIACAP Scorecard
- Security POA&M

#### 4.5.2.1 Decision Types

Accreditation decisions are the official determination made by the DAA regarding the acceptance of risk associated with the web service capability. The NECC DAA accreditation decisions include: ATO, IATO, IATT, and Denial of Authorization to Operate (DATO). Accreditation decisions are issued with an Authorization Termination Date (ATD), identifying the date the authorization will terminate for an ATO, IATO, or IATT.

#### 4.5.2.2 Authorization to Operate (ATO)

An ATO may be issued for up to three years. Reviews for NECC CMs shall be conducted at least annually to validate the correct implementation of assigned IA requirements. An ATO may be granted with CAT II weaknesses, when clear evidence is provided that the CAT II weaknesses can be corrected or mitigated within six months of the accreditation decision. If CAT II weaknesses cannot be satisfactorily corrected or mitigate within six months of issuance, the DAA must document that the NECC CM is critical to mission accomplishment or terminate operations.

#### 4.5.2.3 Interim Authorization to Operate (IATO)

An IATO may be issued for up to 180 days for temporary authorization to operate NECC CMs under the conditions or constraints identified as part of the accreditation decision. The IATO accreditation decision must specify an ATD that is within 180 days of the authorization date.

#### 4.5.2.4 Interim Authorization to Test (IATT)

The CPMO may determine that the CM requires connection to operational systems, networks, or with live data to complete certification testing before full accreditation will be granted. In such cases, the request for an IATT shall submit the request for IATT via the FDCE, and will be available to the CA to determine whether to forward the request to the DAA for approval. IATTs are issued for a specified period of limited time. IATT extension requests may be considered by the DAA on an as-needed basis. An IATT extension request letter, is available on the FDCE Reference Library, must be submitted to the DAA prior to reconnection of the CMs.

#### 4.5.2.5 Denial of Authorization to Operate (DATO)

Corrective actions specified in the Security POA&M must be achievable within the authorization period and must be resourced accordingly. If, at the end of a second consecutive IATO, the NECC CM weaknesses have not been corrected or satisfactorily mitigated, the DAA shall issue a Denial of Authorization to Operate (DATO). The DATO shall remain in effect until all corrective actions identified in the Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO.

### **4.5.3 NECC Capstone DIACAP Package**

The “NECC Capstone” DIACAP Package has been developed to document the Inherited IA Controls that apply to all NECC CMs. JPMO IA maintains the NECC Capstone Package and shall make this information available through the FDCE Reference Library.

The NECC Capstone DIACAP Package includes the following NECC documentation:

- Security Plan
- Capstone SIP
- Capstone DIP
- Continuity of Operations Plan (COOP)
- Incident Response Plan
- Security Education Training and Awareness (SETA)
- Information Assurance Vulnerability Management (IAVM) Plan
- Configuration Management Plan
- Enterprise Service Level Agreements (SLAs)

### **4.5.4 Maintain Authorization to Operate and Conduct Reviews**

#### 4.5.4.1 Maintain Situational Awareness

The NECC program shall ensure that IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations are funded and exercised throughout the SDLC. The NECC IAM shall continuously maintain situational awareness of the NECC security posture and monitor the information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically

assesses the quality of IA controls implementation against performance indicators such as security incidents; feedback from external inspection agencies. In addition, the IAM may independently or at the direction of the CA or DAA schedule a revalidation of any or all IA controls at any time. Revalidation of IA controls is required to be conducted at least annually.

#### 4.5.4.2 Maintain IA Posture

The IAM may recommend changes or improvement to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements to the design of the CM itself.

DoD ISs with a current ATO that are found to be operating in an unacceptable IA posture through GAO audits, IG DoD audits, or other reviews or events such as an annual security review or compliance validation shall have the newly identified weakness added to an existing or newly created IT Security POA&M.

If a newly discovered CAT I weakness on an NECC CM operating with an ATO cannot be corrected within 30 days, the system can only continue operation under the terms of DIACAP.

If a newly discovered CAT II weakness on an NECC CM operating with a current ATO cannot be corrected or satisfactorily mitigated within 90 days, the system can only continue operation under the terms prescribed in DIACAP.

#### 4.5.4.3 Conduct Periodic Annual Reviews

The NECC IAM shall provide a written statement to the DAA(s) and CA(s) annually, based on the review of all IA requirements and testing of selected IA requirements for CMs accredited in the NECC Capstone Accreditation. The DAA and CA review the NECC IAM statement in light of mission and environment indicators and determine a course of action. The review and determination is recorded in the NECC Capstone SIP and is made visible to the DoD CIO/SIAO for FISMA reporting.

#### 4.5.4.4 Reaccreditation

Reaccreditation is required if any of the following occur:

- Addition or replacement of a major component or a significant part of architecture
- Change in security mode of operation
- Significant change to the web platform
- Breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation
- Significant change to the availability of safeguards
- Significant change to the threat that could impact the system
- Significant changes to the WSDL or software code

#### 4.5.4.5 Changes to the Security Baseline

Through the NECC Configuration Management (CM) process, the CPMO is responsible to identify changes to the baseline configuration of the CM. The CA may participate as a Subject

Matter Expert (SME) on the CCB to assist in determining if the changes to the baseline configuration indicate a significant change to the security baseline. All architecture documentation (diagrams, topologies, and supporting narratives) will be updated. Certification testing of the changes, conducted by the CMTT, will also require additional coordination through the JST.

#### **4.6 Ports, Protocols & Services Management**

NECC requires compliance with existing DoD guidance on ports, protocols, and services (PPS) and NECC CMs shall use only standard ports and protocols. Ports, Protocol, and Services Management (PPSM) is an operational program required to meet current and future network operations and Computer Network Defense (CND) requirements. These requirements are generated by DODI 8551.1 and daily operational support activities for the JTF-GNO. The PPSM Program is evolving to support the hierarchy of all DoD Global Information Grid (GIG) and Intelligence Community (IC) Networks.

The CPMO IA SME will assist in the coordination of registering PPS at all enterprise and hosting sites. The DIACAP Team shall coordinate with the Implementation WG to ensure all IA guidance for implementation is widely known and included in the implementation schedule.

#### **4.7 Decommission**

When a DoD IS is removed from operation, a number of DIACAP-related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, Lines 8, “DIACAP Activity,” and 9, “System Life Cycle Phase,” of the SIP should be updated to reflect the IS decommissioned status. Concurrently, the DIACAP Scorecard and any POA&Ms should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management should be reviewed for impact.

#### **4.8 Progression through FDCE Stages**

NECC has identified minimum IA criteria that must be met prior to graduating from one FDCE to another. Regardless of the FDCE stage, the DAA must issue an accreditation decision prior to connection to any operational environment.

##### **4.8.1 Development Stage**

The minimal criteria for entry into the Development Stage:

- Work Package (WP) approval
- Successful completion of CDR Checklist
- Apportioned Test Evaluation and Certification Criteria (TECC) Matrix and DIP

##### **4.8.2 Developmental Piloting Stage**

The minimal criteria for entrance into Developmental Piloting Stage:

- Completion of designated IA Requirements identified in TECC and DIP
- Completion of a Comprehensive DIACAP Package
- Issuance of an accreditation decision for the NECC configuration managed CM
- Comply with IAVM
- Successful completion of the IA criteria defined in the Developmental Test Readiness Review (DTRR) Checklist

#### **4.8.3 Operational Piloting Stage**

The minimal criteria for entrance into Operational Piloting Stage:

- Completion of designated IA Requirements identified in TECC and DIP
- Completion of a Comprehensive DIACAP Package
- Issuance of an IATO for the NECC configuration managed CM
- Comply with IAVM

#### **4.8.4 Network Operations**

Entrance criteria for this stage necessitates that all IA requirements be satisfied or residual risks are at an acceptable level for the DAA to grant the CM an ATO. In addition to the issuance of an accreditation decision, the NECC CM may require additional, non-IA associated, entrance criteria for NetOps. These considerations will not be addressed as part of the C&A process.

VMS is the central resource for monitoring and tracking IA compliance for NECC capabilities in NetOps. C&A must be maintained throughout the life cycle of the CM.

- Maintain Situational Awareness
- Comply with IAVM
- Exercise Incident Response Plan
- Exercise COOP annually
- Annual Security Review
- Reaccreditation

**APPENDIX A – REFERENCES****Federal or National Level Guidance**

- Public Law 107-347 (Title III), Federal Information Security Management Act (FISMA), December 17, 2002
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, 8 February 1996
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-95, Guide to Secure Web Services (DRAFT) Recommendations of the National Institute of Standards and Technology, September 2006<sup>5</sup>
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000

**Department of Defense (DoD) Level Guidance**

- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CNA), 25 March 2003
- DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007 (This DoD Instruction replaces existing DITSCAP guidance under DoDI 5200.40 and DoD 8510.1-M)
- DoDI 8500.1, Information Assurance (IA), 24 October 2002
- DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003<sup>6</sup>
- DoDD 8570.1, Information Assurance Training, Certification, and Workforce Management, 15 August 2004
- DoD 8570.1-M, Information Assurance Workforce Improvement Program, 19 December 2005
- DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004
- DoD Net-Centric Checklist Version 2.1.4, July 30, 2004<sup>7</sup>

**Local NECC Guidance**

- Test and Evaluation (T&E) Criteria Matrix
- Federated Development and Certification Environment (FDCE) Concept of Operations (CONOPS), Version 0.31, October 2006

---

<sup>5</sup> <http://src.nist.gov/publications/drafts/Draft-SP800-95.pdf>

<sup>6</sup> [http://www.dtic.mil/whs/directives/corres/pdf/i85002\\_020603/i85002p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf)

<sup>7</sup> [http://www.ndu.edu/CTNSP/S&R\\_workshop3/Net\\_Centric\\_Checklist\\_2\\_1\\_4.pdf](http://www.ndu.edu/CTNSP/S&R_workshop3/Net_Centric_Checklist_2_1_4.pdf)

**APPENDIX B – ACRONYMS**

<b>Acronym</b>	<b>Definition</b>
ATC	Authorization to Connect
ATO	Authorization to Operate
C&A	Certification and Accreditation
CA	Certifying Authority
C2	Command and Control
CCB	Configuration Control Board
CDD	Capability Development Document
CDR	Critical Design Review
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CM	Capability Module
CND	Computer Network Defense
CNSS	Committee for National Security Systems
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
CPA	Capability Provisioning Activity
CPAS	Capability Provisioning Activity Stages
CPE	Capability Provisioning Events
CPMO	Component Program Management Office
CSP	Capability Security Plan
DAA	Designated Accrediting Authority
DATO	Denial of Authorization to Operate
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DITPR	DoD Information Technology Portfolio Repository

UNCLASSIFIED

<b>Acronym</b>	<b>Definition</b>
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information System
DOT&E	Director, Operational Test and Evaluation
DSAWG	DISN Security Accreditation Working Group
DTP	Detailed Test Plan
<i>e</i> MASS	Enterprise Mission Assurance Support System
FISMA	Federal Information Security Management Act
ERB	Engineering Review Board
FDCE	Federated Development and Certification Environment
FSO	Field Security Operations
GCCS	Global Command and Control System
GCN	GIG Computing Node
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVRR	Information Assurance Validation Readiness Review
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IAV	Information Assurance Vulnerability
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
ISER	Initial Security Engineering Review
ISSE	Information System Security Engineer
JITC	Joint Interoperability Test Command
JMUA	Joint Military Utility Assessment
JPMO	Joint Program Management Office
JTF-GNO	Joint Task Force, Global Network Operations
KS	Knowledge Service

UNCLASSIFIED

<b>Acronym</b>	<b>Definition</b>
LOE	Level of Effort
MAC	Mission Assurance Category
MDA	Milestone Decision Authority
NCPO	Net-Centric Programs Office
NECC	Net-Enabled Command Capability
NetOps	Network Operations
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
OT	Operational Tester
OTA	Operational Testing Authority
PEO	Program Executive Office
POA&M	Plan of Actions and Milestones
SDLC	Software Development Life Cycle
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SPAWAR	Space and Naval Warfare
SSC-C	SPAWAR Systems Center - Charleston
SP	Special Publication
STIG	Security Technical Implementation Guide
TE&C	Test, Evaluation, and Certification
TEMP	Test and Evaluation Master Plan
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WP	Work Package
WSDL	Web Service Description Language

**APPENDIX C – GLOSSARY OF TERMS**

**Accreditation:** Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations.

**Accreditation Boundary:** Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged.

**Accreditation Decision:** An official designation from a DAA, in writing or digitally signed, and made visible to the DoD CIO, regarding acceptance of the risk associating with operating a DoD Information System or web service capability. Expressed as an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO).

**Artifacts:** System policies, documentation, plans, test results, and other supporting evidence that express or enforce the IA posture of the web service capability, that make up the C&A information and provide evidence of compliance with the assigned IA requirements.

**Assurance:** The degree of confidence that a safeguard(s) correctly implement(s) the system specific security policy.

**Authorization Termination Date (ATD):** The date assigned by the DAA that indicates the date upon which authorization to operate is terminated for an ATO, IATO, or IATT.

**Authorization to Operate (ATO):** The authorization granted by a DAA for a DoD information system to process, store, or transmit information. Authorization is based on acceptability of the IA component, the system architecture and implementation of assigned IA requirements.

**Availability:** The accessibility of systems, programs, services and information when needed and without undue delay.

**Back-End Code:** The Back-End Code is the balance of the resources comprising an NECC Web Service. The Back-End Code, and the system upon which it runs, are maintained by the Materiel Developer. It is reasonable to expect that Materiel Developers will make constant changes to the Back-End Code and associated system in support of their mission and to allow for evolving web service capabilities.

**Capability:** The ability of a threat agent to act, or to be effective.

**Category I (CAT I) Severity Code:** Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges, and usually cannot be mitigated.

**Category II (CAT II) Severity Code:** Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings can usually be mitigated and will not prevent an ATO from being granted.

**Category III (CAT III) Severity Code:** Assigned to recommendations that will improve IA posture but are not required for an authorization to operate.

**Certification:** The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation, which establishes the extent to which a system satisfies a specified security policy.

**Certifying Authority (CA):** The senior official with the authority and responsibility for the certification of CMs for NECC.

**Certifying Authority (CA) Representative:** The official acting on behalf of the Certifying Authority.

**Compromise:** Unauthorized disclosure, destruction, removal, modification, or interruption to an IT system asset.

**Confidentiality Level (CL):** Primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-share determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). DoDI 8500.2 defines three confidentiality levels: Classified, Sensitive, and Public.

**Denial of Authorization to Operate (DATO):** DAA determination that a DoD information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA requirements, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

**Designated Accrediting Authority (DAA):** The official with the authority to formally assume responsibility for a web service capability at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

**DoD Information Technology Portfolio Repository (DITPR):** In July 2004, DoD issued guidance on a new database, entitled the DITPR, which will support DoD portfolio management by collecting data on DoD information systems in all mission areas and domains. The guidance requires submission of information on selected business systems, with data on remaining DoD information systems to be collected later. In October 2004, DoD issued additional guidance requiring data to be submitted on remaining business systems or families of business systems.

**Engineering Review Board (ERB):** The ERB organizational steering committee that manages and controls product development and configuration management.

**Enterprise GCN:** An NECC GCN located at an NECC enterprise site.

**Enterprise Site:** NECC site that provides NECC capabilities to large number of geographically distributed users over wide-area network.

**Environment:** An environment represents a portal within the SOA and the associated set of Core Services supporting the environment. Separate environments are used for testing component software in various stages of the SOA's evolution.

**Event:** A change in system state. In general, an event has a trigger, a means or mechanism, and an effect or consequence. An event may be undesirable from a security point of view, in which case it is called a threat event.

**Federal Information Security Management Act:** The Federal Information Security Management Act (FISMA) provides the framework for securing the federal government's information technology. All agencies covered by the Paperwork Reduction Act must implement the requirements of FISMA and report annually to the Office of Management and Budget and Congress on the effectiveness of the agency's security programs. The reports must also include independent evaluations by the agency Inspector General.

**GIG Computing Node (GCN):** Standard hardware and software platform for hosting NECC capability modules.

**Global Command and Control System (GCCS):** GCCS is a highly mobile, deployable command and control system supporting forces for joint and multinational operations across the range of military operations, any time and anywhere in the world with compatible, interoperable, and integrated command, control, communications, computers, and intelligence systems.

**Global Information Grid (GIG):** The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

**Information Assurance (IA) Kit:** Collection of forms and tools provided by NECC to the Materiel Developers to ensure they can follow the C&A process as required for NECC.

**Interface:** The Interface consists of the WSDL and associated functions including WSDL configuration management, WSDL version control, and WSDL standards conformance. The WSDL provides information about how a web service communicates with another web service(s). This information is used by capability providers' software developers to ensure that information technology resources and software code conform to NECC standards while continuing to offer the flexibility necessary to build the NECC capability. NECC JPMO will ensure only approved NECC Web Service Interfaces are used. Multiple, competing versions of an NECC WSDL could be an IA issue and adversely affect NECC capability modules. Consequently, the NECC DAA should administer and approve NECC configuration management, version control, and standards conformance activities.

**Interim Authorization to Operate (IATO):** Temporary authorization to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision.

**Interim Authorization to Test (IATT):** Temporary authorization to test a DoD information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

**Local GCN:** An NECC GCN located at an NECC LAN-supported site.

**Local Area Network (LAN)-Supported Site:** NECC site that provides NECC capabilities to a small number of users over local area network and has consumers that must use NECC capabilities while disconnected from or intermittently connected to the wide area network.

**Materiel Developer:** Owner of a service that engineers software solutions to integrate new code into the SOA.

**Net-Centric:** DoD strategy of global, web-enabled, user-centric information sharing and fusion across the battlefield.

**Network Operations (NetOps):** NetOps is essential for enabling net-centricity. IT is an operational construct within Information Operations consisting of the essential tasks, situational awareness (SA), and C2 that the commander requires to operate and defend the GIG.

**Plan of Actions and Milestones (POA&M):** A POA&M is required for any accreditation decision that requires corrective actions. It is a tool identifying tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

**Protection Level (PL):** An indication of the implicit level of trust that is placed in a system's technical capabilities. A PL is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review.

**Risk:** A measure indicating the likelihood and consequence of events or acts that could cause an impact to one or more of system asset(s).

**Risk Assessment:** An evaluation of risk based on the effectiveness of existing security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets

**Secret Internet Protocol Router Network (SIPRNet):** SIPRNet is the Worldwide Secret level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry.

**Service-Oriented Architecture (SOA):** A web-based architecture that connects various services in a platform-independent environment.

**Site:** Physical location accessible to the GIG that either provides NECC capabilities to consumers or has consumers that use NECC capabilities.

**System:** Any assembly of computer hardware, software, or firmware configured to collect, create, store, or control data or information in electronic form. .

**Test and Evaluation Master Plan (TEMP):** The TEMP describes the program Test and Evaluation policy, objectives, requirements, general methodology (test flow and description of each testing phase), responsibilities, and scheduling of test phases. The TEMP is a program-level management planning document for all SOA test activities.

**Type Accreditation:** A DoD Information System or NECC CM developed for deployment to multiple locations with the same type of computing environment. The application or system

usually consists of a common set of hardware, software, or firmware. Type accreditations tend to significantly reduce the field-level assessment activities.

**Vulnerability:** A characteristic of the system which allows a successful threat event to occur.

**Web Service:** A software component or system designed to support interoperable machine or application-oriented interaction over a network.

**Web Service Description Language (WSDL):** An extensible markup language (XML) format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.<sup>8</sup>

---

<sup>8</sup> <http://www.w3.org/TR/wsdl>

UNCLASSIFIED

**APPENDIX D-H**

**APPENDIX D - SYSTEM IDENTIFICATION PROFILE TEMPLATE**

<https://www.us.army.mil/suite/page/465320>

**APPENDIX E - DIACAP IMPLEMENTATION PLAN TEMPLATE**

<https://www.us.army.mil/suite/page/465320>

**APPENDIX F - DIACAP SCORECARD TEMPLATE**

<https://www.us.army.mil/suite/page/465320>

**APPENDIX G - RESIDUAL RISK REPORT TEMPLATE**

<https://www.us.army.mil/suite/page/465320>

**APPENDIX H - SECURITY POA&M TEMPLATE**

<https://www.us.army.mil/suite/page/465320>