



# Joint Task Force National Capital Region Medical **INSTRUCTION**

**NUMBER 8500.02**

**DEC 08 2011**

---

---

J-6

**SUBJECT:** DoD Information Assurance Certification and Accreditation Process (DIACAP)  
Interim Authorization to Test (IATT)

- Reference:**
- (a) Deputy Secretary of Defense Memorandum, “Establishing Authority for Joint Task Force – National Capital Region/Medical (JTF CapMed) and JTF CapMed Transition Team (Unclassified),” September 12, 2007
  - (b) Deputy Secretary of Defense Action Memo, “Civilian and Military Personnel Management Structures for the Joint Task Force National Capital Region – Medical,” January 15, 2009
  - (c) Comprehensive Master Plan for the National Capital Region Medical, April 23, 2010
  - (d) Supplement to the Comprehensive Master Plan for the National Capital Region Medical, August 31, 2010
  - (e) DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007

1. PURPOSE. This Instruction, in accordance with the authority in References (a) through (d), provides Information Assurance (IA) requirements for an IATT and describes the process for obtaining an accreditation decision for an IATT.

2. APPLICABILITY. This Instruction applies to the Joint Task Force National Capital Region Medical (JTF CapMed) and all Joint Medical Treatment Facilities and Centers in the National Capital Region (i.e., Fort Belvoir Community Hospital, Walter Reed National Military Medical Center, and Joint Pathology Center).

3. DEFINITIONS. See Glossary

4. POLICY. It is JTF CapMed policy that all information systems, applications and services (referred to collectively as (information system (IS))) will be certified through the appropriate processes as identified in Reference (e). In the process of certification it may be required to test

DEC 08 2011

the IS on the Joint Medical Network (JMED). All uncertified ISS must receive an IATT prior to connecting to the live (production) network referred to as JMED for testing. ISS receiving an IATT will not be used for operational activities; the IATT is granted for testing purposes only. This testing may include limited user testing, independent validation and verification testing to facilitate DIACAP certification.

5. RESPONSIBILITIES. See Enclosure 1

6. PROCEDURES. See Enclosure 2

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from JTF CapMed Issuances website at: [www.capmed.mil](http://www.capmed.mil).

8. EFFECTIVE DATE. This Instruction is effective immediately.



SCOTT WARDELL

Executive Director for Administrative Operations  
By direction of the Commander

Enclosures

1. Responsibilities
2. Procedures
3. JTF CapMed IATT Request Memorandum Template
4. IAM Memorandum Template
5. MOA Template
6. POA&M

Glossary

ENCLOSURE 1

RESPONSIBILITIES

1. JTF CAPMED DIRECTOR, J-6. JTF CapMed Director, J-6 shall:

- a. Oversee and ensure IATTs are applied for and granted by an appropriate Designated Accrediting Authority (DAA) prior to allowing ISs to be install onto the JMED.
- b. Provide an Independent Validation and Verification capability to process IATT requests from systems owners, vendors, and other customers referred to collectively as customers.
- c. Establish procedures for customers to apply for IATT consideration by the DAA.
- d. Monitor and manage compliance with IATT limitations and termination dates.
- e. Align all IATT procedures and policies with the Military Health Systems DIACAP processes.
- f. Terminate JMED network access to testing ISs upon completion of the IATT performance period and/or lack of compliance with the terms and conditions of the IATT.
- g. Coordinate approved IATTs with the network managers and medical treatment facility IA staff to make appropriate configuration changes to the network to support the testing ISs.

2. SITE INFORMATION ASSURANCE (IA) MANAGER AND SYSTEM OWNERS. The Site IA Manager and System Owners shall:

- a. Use the procedures listed below in applying to the JTF CapMed J-6 Certifying Authority for IATT approval.
- b. Follow the policy, procedures, and limitations specified in Reference (e) for the approval and/or appeal of DAA disapproval to the IATT.
- c. Not connect unapproved ISs to the JMED prior to receiving an IATT from the JTF DAA.
- d. Terminate IS connectivity to the JMED upon direction from the JTF CA, or the termination date stipulated in the IS's IATT.

DEC 08 2011

ENCLOSURE 2PROCEDURES

1. ACTIONS REQUIRED BY JOINT MTF AND CENTER PROGRAM MANAGERS FOR INITIATION OF IATT. The JTF CapMed Certifying Authority (CA) and the DAA established the following requirements for obtaining an IATT accreditation decision. To initiate the official determination process, system Program Managers (PMs) must submit the following documents/information to the JTF CapMed IA Branch:

a. IATT Request Memorandum. The request memorandum describes the system and its mission. In addition to the description, it includes key milestones with end dates for system testing. The memorandum allows the CA to clearly understand the Program Office's justification for the IATT. The IATT Request Memorandum template is provided in Enclosure 3.

b. Information Assurance Manager (IAM) Memorandum. The IAM Memorandum provides a written or DoD Public Key Infrastructure (PKI)-certified digitally signed statement to the CA indicating the self-assessment has been accomplished. The IAM Memorandum template is provided in Enclosure 4. The following documents are submitted as attachments to the IAM Memorandum:

(1) Information System (IS) Core. The IS Core Artifact provides guidance to system planners, managers, and integrators to assist them in understanding the systems architecture design, operation, data flow and security policy while planning and implementing the IS. Additionally, it describes the IS components and the role of each component in providing operational support. The IS Core template is available within the DIACAP Tool Kit, [http://www.tricare.mil/tmis\\_new/IA.htm#diacap](http://www.tricare.mil/tmis_new/IA.htm#diacap).

(2) Certification and Accreditation (C&A) Boundary Device Matrix. The C&A Boundary Device Matrix lists the hardware and software used within the C&A boundary. The Matrix template is available within the DIACAP Tool Kit, [http://www.tricare.mil/tmis\\_new/IA.htm#diacap](http://www.tricare.mil/tmis_new/IA.htm#diacap).

(3) Memorandum of Agreement (MOA). The MOA defines support and coordination requirements between affected fielding sites, thereby documenting the agreement. The memorandum template is provided in Enclosure 5.

(4) IATT Test Plan. All applicable IA Controls will be tested and satisfied prior to testing in an operational environment or with live data, except for those which can only be tested in an operational environment. In consultation with the PM or System Manager, the CA will determine which IA Controls can only be tested in an operational environment.

2. IATT TEST PLAN. The following items must be addressed in the Program Office's (PO) IATT test plan:

DEC 08 2011

- a. Specific details on the criteria, dates, responsibilities, etc., to include tests procedures and measurable performance criteria.
- b. Configuration (e.g., hardware, software, boundary diagram) must be identified along with interfaces.
- c. Written agreements should be executed for any systems connecting as well as any hosting activity.
- d. IA Controls that have been validated and by whom.
- e. System must be terminated or disconnected when tests are not being run (e.g., during reconfiguration, fixes, or maintenance time).
- f. Procedures and mitigations required/performed while the system is connected to the operational environment or using live data (e.g., disconnecting between tests by whom and how verified and documented).
- g. Identify the responsible personnel (e.g., IAM/IAO) for the ongoing security monitoring, ensuring any security updates or patches are incorporated.
- h. State how changes to the configuration or IA security fixes will be reported.
- i. Identify any follow-on actions.

3. SELF ASSESSMENT RESULTS. A self assessment is conducted by the PO. The self assessment identifies vulnerabilities that may be identified during an actual security test and evaluation; it also allows the PO an opportunity to mitigate Category (CAT) I IA control weaknesses.

4. FILE OUTPUT TYPE. The PO must provide the following file output type for each assessment tool to the JTF CapMed IA Branch at [jtf\\_capmed\\_dropbox@nsoc.med.osd.mil](mailto:jtf_capmed_dropbox@nsoc.med.osd.mil), the email must be encrypted. Subject line: SYSTEM NAME IATT Results.

a. Retina. A Remediation Report in .doc format as well as a generated Vulnerability Management System (VMS) Export .xml file. The “All Audits” setting must be selected for the assessment.

b. Gold Disk. A Vulnerability Status Open Findings report in .rtf as well as a VMS 6.X .xml file. Testing is to include the manual portion of the assessment.

c. Database Security Readiness Review. The output .xml files produced by the script as well as the report .txt files.

DEC 08 2011

d. UNIX Security Readiness Review. The packaged (zipped) results file for each host with an OPEN findings report included.

e. Checklists. Results recorded for all open and closed checks with notes for each. Results can be provided in whatever format works for the site (.pdf, .doc, .xls).

5. PLAN OF ACTION AND MILESTONES (POA&M). The POA&M is required for any accreditation decision that requires corrective action. Weaknesses identified on the POA&M reflects residual risk to the system. The POA&M template is provided in Enclosure 6.

6. JTF CAPMED METHOD OF ASSESSMENT. The Joint MTF and Center Program Management Offices (PMOs) are to ensure all applicable IA controls are tested and satisfied prior to testing in an operational environment or with live data, except for those which can only be tested in an operational environment. The JTF CapMed IA Branch will assess the PMO's POA&M and self assessment results to ensure the system does not have CAT I weakness, and mitigation strategies for CAT II and III weakness are in place. The JTF CapMed CA will review the package and issue a Determination Statement. The DAA will review the information and the CA's determination, and issue an accreditation decision. IATT accreditations are granted to PMOs to test for a limited period of time in an operational environment.

DEC 08 2011

ENCLOSURE 3JTF CAPMED IATT REQUEST MEMORANDUM TEMPLATE

&lt;Official Letterhead&gt;

DD Month YYYY

MEMORANDUM FOR JOINT TASK FORCE NATIONAL CAPITAL REGION  
MEDICAL (JTF CAPMED) CERTIFYING AUTHORITYFROM: Program Office  
Street Address  
City, State Zip CodeSUBJECT: Request for Interim Authorization to Test (IATT) Application Name (Application  
Acronym)**EXAMPLE TEXT:** This IATT request is in support of the setup and configuration of Application Acronym testing environment on Name of Network.**EXAMPLE TEXT:** The Application Acronym will allow healthcare organizations to capture, manage, and analyze anonymously reported medical errors and high-risk events, from near misses to adverse events. Utilizing a refined taxonomy or classification of more than pre-defined medical events that can lead to patient injury, the Application Acronym will track a vast number of performance measures, grouped into various categories, and uniformly trends the experience across the health care enterprise. Events may be reported directly into the system by staff members and/or electronically transferred from an organization's ancillary systems. After an event has been reported automated workflows within the application provide immediate notification to managers regarding required actions.**EXAMPLE TEXT:** Key milestones with end dates for Application Acronym testing effort are as follows:

## Testing Milestones:

- Setup/Configuration: DD Month YYYY
- Self Assessment Scans: DD Month YYYY - DD Month YYYY
- Self Assessment Scans to JTF CapMed: DD Month YYYY
- Promote to production environment to support activities: DD Month YYYY
- Test: DD Month YYYY - DD Month YYYY

**EXAMPLE TEXT:** All of the servers will be tested and compliant before promotion to production environment. Servers will be isolated in the production environment throughout the

DEC 08 2011

IATT process.

**EXAMPLE TEXT:** Program Office understands that Name of Network, as the controlling authority, has the right to monitor network traffic and deny access to the network for violations of their rules and regulations. All requests for connections to the network are made through the Program Office Information Assurance (IA) Office. Any changes made to the hardware or software configuration of this network must be documented and approved by the respective approval authorities.

**EXAMPLE TEXT:** Usage of Non-Secure Internet Protocol Router Network (NIPRNet) environment at Site Name for Application Acronym test environment will be setup and configured within Site Name's enclave, which is governed, managed, and monitored by Governing Agency policies and regulations.

**EXAMPLE TEXT:** Access Control

- Application Acronym Program Office in conjunction with the Site Network support team will establish and control user accounts in the Application Acronym test environment.
- All Application Acronym personnel with user accounts in the Application Acronym test environment have up-to-date Health Insurance Portability and Accountability Act (HIPAA) and IA training.
- All Application Acronym personnel with user accounts in the Application Acronym test environment have active Secret or Automatic Data Processing (ADP) II clearance.

The Point of Contact (POC) for this request is Name of POC.

---

Name of POC  
POC Title / Government PM  
Application Acronym  
POC Email Address  
POC Phone Number

DEC 08 2011

ENCLOSURE 4

IAM MEMORANDUM TEMPLATE

<Official Letterhead>

DD Month YYYY

MEMORANDUM FOR JOINT TASK FORCE NATIONAL CAPITAL REGION MEDICAL  
(JTF CAPMED) CERTIFYING AUTHORITY

FROM: Program Office  
Street Address  
City, State Zip Code

SUBJECT: Information Assurance Manager (IAM) Memorandum Application Name  
(Application Acronym)

As the designated IAM for Application Acronym, in accordance with Department of Defense Instruction (DoDI) 8510.01, Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP), paragraph 5.18.2, I hereby attest the attached Plan of Action & Milestones (POA&M) dated DD Month YYYY accurately depicts the current, known security risk status of this system version. This risk status is based on a self assessment review of Application Acronym conducted DD Month YYYY to identify any weaknesses to the security posture of the system.

All applicable IA controls were tested and satisfied except for those which can only be tested in an operational environment. The table below depicts untested IA controls:

Control Number	Control Name
EBRU-1	Remote Access for Privileged Functions

The Program Manager for Application Acronym is Name of POC. PM Phone Number, (DSN Phone Number), PM Email Address

\_\_\_\_\_  
Name of IAM  
Information Assurance Manager  
Application Acronym  
IAM Email Address  
IAM Phone Number

DEC 08 2011

Attachments:

1. Information System (IS) Core
2. Certification & Accreditation (C&A) Boundary Matrix
3. Memorandum of Agreement (MOA)
4. Interim Authorization to Test (IATT) Test Plan
5. Self Assessment Results
6. Plan of Action & Milestones (POA&M)

DEC 08 2011

ENCLOSURE 5MOA TEMPLATE

**HOST SITE NAME**  
and  
**PROGRAM OFFICE**

**Purpose:**

This Memorandum of Agreement (MOA) establishes an agreement between the **Host Site Name** and the **Program Office (Program Office Acronym)**. This agreement is effective when signed by **Host Site Name** and the **Program Office Acronym**.

**Scope:**

Under this MOA, **Host Site Name** will provide support services to the **Program Office Acronym** in support of an Interim Approval to Test (IATT) for the period of **DD Month YYYY to DD Month YYYY**.

**Responsibilities:**

**EXAMPLE TEXT:** The **Host Site Name** agrees to:

- Provide to the Customer the requirements for accessing and utilizing the interface to effect bi-directional data exchange between the Customer's case management system and the legacy transactional system(s).
- Provide technical and customer support during regular business hours (7:30 a.m. to 5:30 p.m. Monday through Friday, excluding holidays).
- Notify the Customer of any changes in contact personnel, mail, email, or telephone.
- Notify Customer System Administrator of interruptions in the interface and the legacy system that will impact data flow and production during the business day.
- Make the transfer of data to the legacy system transparent to the Customer's end user.
- Allow the predetermine IP range entrance through the firewall.

**EXAMPLE TEXT:** The **Program Office Acronym** agrees to:

- Configure user workstations so they do not cache any confidential client data obtained from the interface with a legacy system.
- Maintain one point of contact for the Host Site System Administrator
- Notify the Host Site Administrator immediately of changes in contact personnel, address, email, or telephone number.
- Notify the Host Site System Administrator immediately of disconnections between the customer case management system and the interface.
- Develop and maintain a business continuity plan, acceptable to the Host Site, for use in the event of an unforeseen disconnection from the interface.
- Provide a range of IP addresses from which messages will originate. The Host Site will use this range to allow entrance through the firewall.
- Modify, test and certify compliance with all mandatory file layout changes by production date in the legacy system(s), or have users key directly into the legacy system(s) until all

DEC 08 2011

system testing is successful.

- Notify Host Site System Administrator of testing schedules and issues which impact production compliance as soon as they are known.
- Notify the Host Site System Administrator of any known modifications in the customer case management system that could impact the interface and provide test plans and schedules for maintaining the interface.

**Program Office Acronym**

**Host Site Name**

---

Name of POC  
POC Title  
POC Email  
POC Address

---

Name of POC  
POC Title  
POC Email  
POC Address

---

DD Month YYYY

---

DD Month YYYY

DEC 08 2011

ENCLOSURE 6

POA&M TEMPLATE

<b>Date Initiated:</b>					<b>IS Type:</b>					<b>OMB Project ID:</b>			
<b>Date Last Updated:</b>					<b>POC Name:</b>								
<b>Component Name:</b>					<b>POC Phone:</b>								
<b>System / Project Name:</b>					<b>POC E-Mail:</b>								
<b>DoD IT Registration No:</b>													
<b>Weakness (1)</b>	<b>CAT (2)</b>	<b>IA Control &amp; Impact Code (3)</b>	<b>POC (4)</b>	<b>Resources Required (5)</b>	<b>Scheduled Completion Date (6)</b>	<b>Milestones with Completion Dates (7)</b>	<b>Milestone Changes (8)</b>	<b>Source Identifying Weakness (9)</b>	<b>Status (10)</b>	<b>Comments (11)</b>			
1													
2													
3													
4													
5													
6													
7													
8													

GLOSSARY

ABBREVIATIONS AND ACRONYMS

C&A	certification and accreditation
CA	Certifying Authority
CAT	category
DAA	Designated Accrediting Authority
DIACAP	DoD Information Assurance Certification Accreditation Process
IAM	Information Assurance Memorandum
IATT	interim authorization to test
IS	information system
JMED	Joint Military Education Division
JTF CAPMED	Joint Task Force National Capital Region Medical
MOA	Memorandum of Agreement
PM	Program Manager
PMO	Program Management Office
PO	Program Office
POA&M	Plan of Action and Milestones
VMS	Vulnerability Management System