# CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive Current as of 19 November 2014

J-8 CJCSI 8410.02
DISTRIBUTION: A, B, C, JS-LAN 8 February 2012

## WARFIGHTING MISSION AREA (WMA) PRINCIPAL ACCREDITING AUTHORITY (PAA) AND WMA AUTHORIZING OFFICIALS: POLICY AND RESPONSIBILITIES

References: See Enclosure C.

1. Purpose. This instruction establishes policy and responsibilities for the Warfighting Mission Area (WMA) Principal Accrediting Authority (PAA), Joint Staff J-8 Deputy Director for Command, Control, Communications, and Computer Systems (DDC4), and WMA Authorizing Officials in accordance with DOD Instruction (DODI) 8510.01, "DOD Information Assurance Certification and Accreditation Process (DIACAP)" (reference a) and DOD Directive (DODD) 8115.01, "Information Technology Portfolio Management" (reference b) for information systems (ISs) designated as within the WMA.

2. Cancellation. None.

3. Applicability. This instruction applies to Department of Defense (DOD) information technology (IT) investments that are part of the WMA. CJCSI 8410.02 applies to the Joint Staff; combatant commands, Services, and Defense agencies (CC/S/As); and DOD field and joint activities, including DOD and Service non-appropriated fund instrumentalities. The requirements in this instruction should be applied to contracts for services that maintain WMA information systems (ISs) residing in contractor facilities either owned by the Department of Defense and operated by the contractor or operated as a service on behalf of the Department of Defense.

4. Policy. See Enclosure A.

5. Definitions. See Glossary. Note: Titles used in this instruction have been aligned with the terminology in Committee on National Security Systems Instruction (CNSSI) No. 4009, "National Information Assurance (IA) Glossary"

(reference c). The Department of Defense is in the process of updating a number of terms used in the current certification and accreditation process. Throughout this instruction, the new terms are followed by the current terms in parentheses. This instruction changes the title Designated Accrediting Authority (DAA) to Authorizing Official, Information Assurance Manager (IAM) to Information Systems Security Manager (ISSM), and Information Assurance Officer (IAO) to Information Systems Security Officer (ISSO). Reference c also replaces certification with security control assessment and replaces accreditation with authorization (to operate). The next version of this instruction will permanently replace the terms to align them with the updated DODI 8510.01 (reference a).

6. Responsibilities. See Enclosure B.

7. Summary of Changes. None.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

CRAIG A. FRANKLIN
Major General, USAF
Vice Director, Joint Staff

Enclosures:
A -- WMA PAA and Authorizing Officials Policy
B -- Responsibilities
C -- References
GL -- Glossary

## TABLE OF CONTENTS

Page

ENCLOSURE A -- WMA PAA and Authorizing Officials Policy
WMA PAA Background ........ A-1
Appointment of WMA Authorizing Officials........ A-1
Appointment of WMA Certification Authorities (CAs) ........ A-3
Accreditation Implementation Guidance ........ A-3
Compliance with DISN/GIG Flag Panel Guidance ........ A-8
Compliance with DOD Baseline Security Controls........ A-8
Training ........ A-8
Certification and Accreditation Reciprocity ........ A-8
Post-Accreditation Activities ........ A-9
Conflict Resolution ........ A-10

ENCLOSURE B -- RESPONSIBILITIES
Chairman of the Joint Chiefs of Staff (CJCS)........ B-1
DISN/GIG Flag Panel ........ B-1
DSAWG ........ B-1
WMA PAA........ B-1
WMA PAA Representative ........ B-2
Heads of DOD Components ........ B-2
DOD Component Chief Information Officers (CIOs) ........ B-2
WMA IS Authorizing Official........ B-2
Program Manager…........ B-3
CA........ ........ B-4
User Representative........ B-5
ISSM ........ B-5
ISSE …........ B-6
WMA ISSOs........ B-6

ENCLOSURE C -- REFERENCES........ C-1

GLOSSARY
Part I -- Abbreviations and Acronyms ........ GL-1
Part II -- Definitions........ GL-3

(INTENTIONALLY BLANK)

## ENCLOSURE A

## WMA PAA AND AUTHORIZING OFFICIALS POLICY

1. WMA PAA Background. A successful risk management program is predicated on the Authorizing Official's (i.e., DAA's) ability to ensure security requirements are integrated in the acquisition process and life cycle of ISs. This goal must be attained while satisfying the intended design or architecture, complying with selected security controls and safeguards, and managing security changes throughout the designated IS life cycle. The Chairman of the Joint Chiefs of Staff appoints a PAA for DOD ISs governed by the WMA in accordance with DODI 8510.01 (reference a). The WMA PAA, Joint Staff J-8 DDC4, oversees the security risk management framework of the ISs in the mission area and, as required, issues authorization (i.e., accreditation) guidance specific to the mission area per reference a.

2. Appointment of WMA Authorizing Officials

a. Conditions for Requests. The WMA PAA may receive a request to appoint an Authorizing Official (DAA) for enterprise WMA ISs.

b. Submission of Requests

(1) A request to appoint an Authorizing Official (DAA) for a WMA IS should be submitted in writing to the WMA PAA Representative directly from the DOD component's Office of the Chief Information Officer (CIO) or through the organization's Defense Information Assurance Security Accreditation Working Group (DSAWG) Representative. In discussions with the WMA PAA Representative, a determination will be made on the information required to assist the WMA PAA in making the Authorizing Official (DAA) appointment decision.

(2) All requests for WMA Authorizing Official (DAA) appointments must be sent in the form of an official memorandum signed by the requesting DOD component head. The memorandum will include the following:

(a) Identification of the IS for which an Authorizing Official (i.e., DAA) is being requested.

(b) Confirmation the system is designated as a WMA IS.

(c) Identification of the recommended and/or preferred organizations to appoint as the IS Authorizing Official (i.e., DAA).

(d) Identification of a funding source to support Authorizing Official (i.e., DAA) activities.

(e) Points of contact.

(3) If possible, attach a memorandum from the preferred organization indicating its willingness and ability to accept the role of IS Authorizing Official (i.e., DAA).

(4) In the case that an IS falls under the portfolio purview of multiple PAAs, the PAAs will determine which mission area PAA is the primary PAA responsible for appointing an Authorizing Official (i.e., DAA).

c. Selection Process/Criteria

(1) The WMA PAA will use the following desired generic Authorizing Official (DAA) traits as criteria for selecting the best organization to act as Authorizing Official (DAA) for a WMA IS:

(a) Ability to assess technical risk while considering mission needs.

(b) Appropriate community view; adequate resources.

(c) Technical expertise.

(d) WMA authorization (i.e., accreditation) experience.

(e) Community trust and confidence.

(f) Independence from Program Manager (PM).

(g) Familiarity with program and experience in meeting the needs and requirements of the WMA community.

(h) Familiarity with dependent systems and role in family of systems.

(2) All potential Authorizing Official (i.e., DAA) appointments will be coordinated among the WMA PAA, the selected WMA IS Authorizing Official (i.e., DAA), and the WMA IS PM.

d. Notification of WMA Authorizing Official (DAA) Appointment

(1) The WMA PAA will respond to the DOD component(s) responsible for the WMA IS and the appointed IS Authorizing Official (i.e., DAA) in writing.

(2) Once the WMA PAA has appointed the WMA IS Authorizing Official (i.e., DAA), the Authorizing Official (DAA) will execute the duties and responsibilities consistent with this instruction and reference a until relieved of the responsibility.

3. Appointment of WMA Certification Authorities (CAs)

a. In accordance with reference a, the Senior Information Assurance Officer of the component that manages the WMA IS will act as the CA for the WMA IS or formally delegate the CA role as appropriate.

b. The CA role must be independent of the PM role for the WMA IS in accordance with reference a guidance pertaining to allowable relationships among DOD Information Assurance Certification and Process (DIACAP) team members.

4. Accreditation Implementation Guidance

a. Information Assurance (IA) Requirements

(1) IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all WMA ISs.

(2) Each WMA IS will have a Mission Assurance Category (MAC) assigned to comply with reference d.

(3) IA requirements will address availability, integrity, and confidentiality. These requirements will primarily be addressed as IA controls. Availability and integrity requirements will be associated with the MAC. Confidentiality requirements will be associated with information classification and need-to-know. Both sets of requirements will be expressed as IA controls for a WMA IS.

b. Standards/Accreditation Tools

(1) WMA CAs will use the IA tools identified in the DOD Information Assurance Support Environment as a basis for conducting security control assessment (i.e., certification, test, and evaluation (CT&E)) activities on WMA ISs.

(a) These tools include Security Requirement Guides, Security Readiness Review scripts (SRRs), security checklists, Security Technical Implementation Guides (STIGs), and National Security Agency (NSA) guides.

(b) Additional tools may be used at the CA's discretion to maximize the effort to identify security vulnerabilities and improve the security posture of WMA ISs.

(c) The DIACAP Knowledge Service is a recommended source to provide policy and implementation guidelines, community forums, and the latest information and developments concerning the DIACAP.

c. Risk Assessment

(1) Any risk assessment conducted on a WMA IS must be made by weighing the system mission requirements against the identified, implemented countermeasures to known vulnerabilities.

(2) Additional factors to consider include the following.

(a) System architecture.

(b) System security measures.

(c) System operations policy.

(d) System security plan.

(e) Provisions for system operator and end-user training.

(3) A statement of risk acceptance identifying the residual risks being accepted, signed by the WMA ISs Authorizing Official (i.e., DAA), must be included in all authorization (i.e., accreditation) decisions for ISs.

d. Enterprise-Wide Operation and Acceptance of Risk

(1) All WMA IS Authorizing Officials (i.e., DAAs) must coordinate with the WMA PAA representative to the Defense Information Systems Network/Global Information Grid (DISN/GIG) Flag Panel on connecting enterprise WMA ISs to the DISN.

(2) The DISN/GIG Flag Panel will determine if a WMA IS requires its approval for enterprise deployment and acceptance of risk. See reference e for details on the approval process.

e. Certification Determination. The WMA IS CA representative must follow the guidance in reference a for completing a certification determination.

(1) In addition to the requirements in reference a, the CA must submit a certification determination memorandum summarizing the security control assessment (i.e., certification, test, and evaluation (CT&E)) efforts and providing an authorization (i.e., accreditation) recommendation to the WMA IS Authorizing Official (i.e., DAA). This authorization (i.e., accreditation) recommendation will assist the Authorizing Official (i.e., DAA) in making an authorization (i.e., accreditation) decision.

(2) The authorization (i.e., accreditation) recommendation will provide an overview of the security vulnerabilities, implemented countermeasures, and level of risk acceptance associated with the vulnerabilities.

(3) The authorization (accreditation) recommendation will provide advice on an authorization (accreditation) decision for the WMA IS expressed as a recommendation for an Authorization to Operate (ATO), Interim Authorization to Operate (IATO), Interim Authorization to Test (IATT), or Denial of Authorization to Operate (DATO).

f. Authorization (i.e., Accreditation) Decisions

(1) The WMA IS Authorizing Official (i.e., DAA) must follow guidance in reference a for completing an authorization (i.e., accreditation) decision.

(2) WMA IS authorization (accreditation) decisions must be expressed as an ATO, IATO, IATT, or DATO.

(3) In addition to the requirements in reference a, the WMA IS Authorizing Official (DAA) must complete an authorization (accreditation) decision memorandum that summarizes the authorization (accreditation) decision and includes a statement of risk acceptance.

(a) The authorization (accreditation) decision memorandum is a written statement that documents the authorization (accreditation) decision and states the specific reasons for issuance of the identified authorization (accreditation) decision. The authorization (accreditation) decision memorandum will be signed by the WMA IS Authorizing Official (DAA) and sent to the WMA IS PM to maintain it as proof of authorization (accreditation).

(b) The statement of risk acceptance must identify the residual risks and confirm that the level of risk associated with an ATO or IATO decision is at an acceptable level. If the level of risk is unacceptable, the statement must include information explaining this position and the corresponding DATO decision.

g. Authorization (Accreditation) Artifacts. These artifacts are used to document and track the status of corrective actions associated with the authorization (accreditation) decision. Additional documentation may be developed at the discretion of the WMA IS Authorizing Official (DAA).

(1) WMA ISs must be registered in the DOD Information Technology Portfolio Registry (DITPR) or the Secret Internet Protocol Routing Network (SIPRNET) IT Registry and have a corresponding System Identification Profile (SIP) documenting its registration in accordance with reference a.

(2) WMA ISs must have a DIACAP Implementation Plan (DIP) that defines its inherited and implemented IA controls.

(3) At a minimum, an Executive Package consisting of a DIACAP Scorecard, SIP, and an IT Security Plan of Actions and Milestones (POA&M) will be created for each WMA IS.

(4) Each WMA IS must also have an authorization (i.e., accreditation) decision memorandum signed by its IS Authorizing Official (i.e., DAA).

(5) A Security Classification Guide (SCG) will be developed for each WMA IS that processes both unclassified and classified information. An SCG is required to receive an authorization (i.e., accreditation) decision from the Authorizing Official (i.e., DAA). The SCG must specifically address any requirements or conditions that will be imposed if the WMA IS is connected to allied/Coalition networks.

(6) WMA ISs that are subject to the requirements of DODI 5000.02, "Operation of the Defense Acquisition System," (reference f) are required to prepare an Acquisition IA Strategy and an Information Support Plan.

h. Criteria for Authorization (i.e., Accreditation) Decisions. WMA IS Authorizing Officials (i.e., DAAs) must adhere to guidance in reference a pertaining to conditions and timelines for granting authorization (i.e., accreditation) decisions.

(1) An ATO granted to a WMA IS can be for a period no longer than 3 years from the date signed. Any WMA IS granted an ATO cannot operate with Category (CAT) I weaknesses unless the DOD component CIO responsible for the WMA IS grants an ATO based upon mission criticality.

(2) A WMA IS granted an ATO can only have CAT II weaknesses if there is an IT Security POA&M documenting the mitigation strategy for correcting each CAT II weakness. If necessary, funds must be allocated to support the mitigation of the weaknesses.

(a) The Authorizing Official (i.e., DAA) must receive periodic updates on the status of correcting the weaknesses.

(b) CAT II weaknesses must be corrected or mitigated to a CAT III within180 days of the date the accreditation decision is granted.

(c) Failure to mitigate the findings in the allotted time period will result in a review of the authorization (i.e., accreditation) decision by the Authorizing Official (i.e. DAA).

(d) If a CAT I finding is discovered after granting an ATO to a WMA IS and cannot be mitigated within 30-days, the Authorizing Official (i.e., DAA) should rescind the ATO and grant either an IATO or DATO based upon the severity of the weakness. If an IATO is granted, an IT POA&M will be developed and maintained to track the status of corrective actions taken in association with mitigating the weakness.

i. Authorization (i.e., Accreditation) Decision Review

(1) An authorization (i.e., accreditation) decision review will be conducted when a WMA IS fails to meet the deadline for correcting weaknesses identified in an IT Security POA&M.

(2) In this review, the WMA IS PM will have the opportunity to provide justification for failing to meet the deadline.

(3) The Authorizing Official (i.e., DAA) will determine whether to grant an IATO or DATO based upon the justification, and the acceptability of the risks associated with the unmitigated weaknesses.

(4) The Authorizing Official (DAA) will provide the results of the authorization (accreditation) decision review to the WMA IS PM in a new authorization (accreditation) decision memorandum.

j. Enterprise Mission Assurance Support Service (eMASS)

(1) To ensure authorization (i.e., accreditation) evidence is available to Authorizing Officials (i.e., DAAs) of interconnecting ISs and the WMA PAA, WMA IS accreditation data (i.e., SIP, DIP, certification determination, accreditation memorandum, DIACAP scorecard, and IT Security POA&M) shall be loaded or exported into eMASS.

(2) If the Authorizing Official (i.e., DAA) of the interconnecting system does not have eMASS access, the Authorizing Official (i.e., DAA) must provide access to the DIACAP package through an alternate method.

5. Compliance with DISN/GIG Flag Panel Guidance. WMA ISs must comply with DISN/GIG Flag Panel Guidance. WMA IS Authorizing Officials (i.e., DAAs) will submit statements of compliance to the WMA PAA or DISN/GIG Flag Panel, when required.

6. Compliance with DOD Baseline Security Controls. WMA ISs must comply with applicable DOD baseline security controls. Each WMA IS must have a plan and budget for the implementation, validation, and sustainment of security controls.

7. Training

a. WMA IA workforce personnel must be adequately trained and certified in accordance with DODD 8570.01, “DOD Information Assurance Training, Certification, and Workforce Management” (reference g) in order to perform the tasks associated with their IA responsibilities.

b. WMA Authorizing Officials (i.e., DAAs) must complete computer-based training or Web-based training within 30 days of assignment to their position.

(1) Authorizing Official (i.e., DAA) training is located on the DOD IA Portal (http://iase.disa.mil). WMA Authorizing Officials (i.e., DAAs) must maintain a copy of the course completion certificate for the record.

(2) A copy of the course completion certificate should be retained for the duration of the appointment as the WMA IS Authorizing Official (i.e., DAA).

c. Additional IA training is highly recommended for all WMA IA personnel.

8. Certification and Accreditation Reciprocity

a. WMA IS Authorizing Officials (i.e., DAAs) will implement reciprocity, based on the security control assessment (i.e., certification) and authorization (i.e., accreditation) documentation in accordance with the DOD memorandum titled, "DOD Information System Certification and Accreditation Reciprocity" (reference e).

b. Any issues concerning reciprocity between WMA ISs or with ISs of other mission areas should be brought to the attention of the WMA PAA for resolution.

c. Each WMA IS is required to have an Executive Package consisting of a SIP, a DIACAP Scorecard, and an IT Security POA&M to support reciprocity efforts.

9. Post-Accreditation Activities

a. WMA ISs must be continuously monitored, including periodic independent evaluations (e.g., penetration testing) for security-relevant events and configuration changes that negatively impact the IA posture.

b. Reviews must be conducted annually to ensure the effectiveness of IA controls and meet Federal Information Security Management Act (FISMA) requirements. The reviews should include analysis of modifications and/or deviations from the original security controls for the WMA IS that may lead to a requirement for reauthorization (i.e., accreditation). A WMA IS being removed from operation must also adhere to guidance in reference (a) for decommissioning a system.

c. Newly Discovered Weaknesses. WMA ISs must adhere to guidance in reference a concerning the discovery of new weaknesses (CAT 1 or CAT 2) after the Authorizing Official (i.e., DAA) has granted an authorization (i.e., accreditation) decision.

d. Monitoring Security Controls. The assigned security controls of WMA ISs should be monitored for opportunities to make changes or improvements to their implementation.

e. Contingency Plans. Every WMA IS will have a contingency plan in place that addresses disruptions in operations. The contingency plan will be tested semiannually.

10. Conflict Resolution. Submit unresolved issues between the stakeholders of WMA ISs to the WMA PAA for resolution.

a. Each WMA Authorizing Official (i.e., DAA) involved in the issue must submit a memorandum to the WMA PAA detailing their position on the issue along with any supporting documentation and recommendations that will assist the WMA PAA in making a decision.

b. If necessary, the WMA PAA will schedule a formal meeting to discuss the issue. The WMA PAA will respond, in writing, to all unresolved issues submitted for resolution. Issues between WMA ISs and ISs of other mission areas must be submitted to the DISN/GIG Flag Panel for resolution.

## ENCLOSURE B

## RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff (CJCS) shall appoint a PAA for the DOD ISs governed by the WMA.

2. DISN/GIG Flag Panel shall:

a. Advise the mission area PAAs.

b. Assess enterprise risk.

c. Authorize information exchanges and connections for enterprise ISs, cross mission area ISs, cross security domain connections, and non-DOD connections.

d. Approve changes to the DOD security control baseline.

e. Adjudicate disagreements relating to security for ISs crossing mission area boundaries.

3. DSAWG shall:

a. Review and resolve risk decisions related to assessing and sharing community risk.

b. Develop and provide guidance to Authorizing Officials (i.e., DAAs) for IS connections to the GIG.

4. WMA PAA shall perform the duties below in addition to the PAA duties defined in reference h:

a. Appoint, in writing, a flag-level (e.g., general officer, senior executive) PAA Representative to the DISN/GIG Flag Panel.

b. Resolve authorization (i.e., accreditation) issues within the WMA and work with other PAAs to resolve issues among mission areas, as needed.

c. Appoint Authorizing Officials (i.e., DAAs) for WMA ISs in accordance with the conditions and process in Enclosure A.

d. Provide confirmation to the WMA Portfolio Lead that the required IA and information security objectives are being achieved.

5. WMA PAA Representative shall:

a. Represent the mission requirements and accrediting interests of the IS owners within the WMA.

b. Develop an annual report on the authorization (i.e., accreditation) status of WMA ISs for the WMA PAA and other mission area PAAs.

c. Resolve issues concerning the appointment of Authorizing Officials (i.e., DAAs) for WMA ISs.

d. Serve as a voting member on the DISN/GIG Flag Panel.

6. Heads of DOD components shall:

a. Appoint Authorizing Officials (i.e., DAAs) for WMA ISs under their purview.

b. Solicit assistance from the WMA PAA Representative in determining the Authorizing Official (i.e., DAA) appointment if the head of the DOD component is providing an acquisition service and the IS owner/executive agent falls outside of the component's purview.

c. Implement WMA PAA and DISN/GIG Flag Panel decisions on enterprise deployment, operation, and connection of WMA ISs.

7. DOD Component Chief Information Officers (CIOs) shall engage the WMA PAA in matters of appointing an Authorizing Official (i.e., DAA) when the determination of an Authorizing Official (i.e.m DAA) is disputed or cannot be determined.

8. WMA IS Authorizing Official (i.e., DAA) shall:

a. Complete DOD Authorizing Official (i.e., DAA) training within 30 days of appointment, maintain a copy of the course completion certificate, and recertify every 3 years.

b. Ensure compliance with all DISN/GIG Flag Panel guidance and PAA-directed actions and submit statements of compliance to the WMA PAA, when required.

c. Establish and direct goals, policies, and procedures relating to IA of WMA ISs under their control.

d. Approve and submit IT security POA&Ms with mitigation actions if unable to comply with directed guidance.

e. Monitor compliance and status of assets under their control.

f. Complete compliance checks to validate mitigations and/or completion of compliance actions.

g. Authorize or deny operation or testing of WMA ISs under their control.

h. Review WMA IS authorization (i.e., accreditation) documentation to determine if the level of risk is acceptable for operations.

i. Make authorization (i.e., accreditation) decisions for WMA ISs under their control in accordance with reference a and assume responsibility for operating a WMA IS at an acceptable level of risk.

j. Implement security reciprocity between WMA ISs and with ISs of other mission areas and departments.

k. Ensure accreditation documentation is made available to interconnecting ISs, if requested, to support authorization (i.e., accreditation) decisions and FISMA assessments.

l. Conduct authorization (i.e., accreditation) decision reviews, when necessary.

9. Program Manager for a WMA IS shall:

a. Appoint, in writing, a WMA Information System Security Manager (ISSM, i.e., IAM) responsible for the life cycle selection, integration, management, and oversight of security requirements/security controls for WMA ISs under the Program Manager's purview.

b. Appoint, in writing, an Information Systems Security Engineer (ISSE) for each assigned WMA IS.

c. Implement the DIACAP and complete a SIP and DIP for each assigned WMA IS.

d. Plan and budget for implementation, validation, and sustainment of security controls throughout the WMA IS life cycle.

e. Develop, track, and resolve IT security POA&Ms for WMA ISs under their control.

f. Ensure that required information is provided to acquisition managers to properly address and fund IA requirements for WMA ISs.

g. Allocate resources to achieve and maintain an acceptable level of security and to remedy security weaknesses.

h. Develop and test contingency plans for WMA ISs under their control.

i. Ensure a mission assurance category (MAC) to WMA ISs under their control in coordination with the User Representative.

j. Implement configuration control of all WMA ISs and/or assets under their control.

k. Provide requested information to the WMA PAA for inclusion in the annual report on the accreditation status of WMA ISs.

l. Ensure WMA ISs under their control comply with applicable DOD baseline security controls.

m. Ensure the authorization (i.e., accreditation) status of WMA ISs under their control is visible via eMASS for instances where reciprocity of certification decisions and understanding of the accreditation decisions are required.

n. Validate completion of the DIACAP package, including an authorization (i.e., accreditation) decision memorandum, for assigned WMA ISs.

10. CA testing and evaluating an IS registered in the WMA Portfolio shall:

a. Conduct a comprehensive security control assessment (i.e., certification) of the WMA IS to establish the degree it complies with assigned security controls based upon standardized procedures.

b. Provide a certification determination for the assigned WMA IS.

c. Compile the results of the security control assessment (i.e., certification) process on the DIACAP Scorecard.

d. Submit an authorization (i.e., accreditation) recommendation to the WMA IS Authorizing Official (i.e., DAA).

e. Assist the ISSM with defining IA requirements and the annual life cycle security review of security controls and testing of selected security controls to confirm their effectiveness.

11. User Representative shall act as a representative for the WMA user community on security control assessment (i.e., certification) and authorization (i.e., accreditation) activities and issues.

a. Lead development of SCGs for WMA ISs under their control in coordination with the WMA Authorizing Official (i.e., DAA).

b. Ensure a mission assurance category (MAC) to WMA ISs under their control in coordination with the Program Manager.

12. ISSM (i.e., WMA IAM) overseeing the lifecycle security of an IS in the WMA Portfolio shall:

a. Support implementation of the DIACAP for the assigned WMA IS and establish an IA program to ensure synchronization with the DIACAP.

b. Maintain accurate authorization (i.e., accreditation) documentation and information in eMass for the assigned WMA IS.

c. Provide direction to appointed WMA ISSOs (i.e., WMA IAOs) for supporting the implementation of the DIACAP.

d. Manage WMA ISSOs (i.e., WMA IAOs) and assign responsibilities to IA personnel reporting to the WMA Authorizing Official (i.e., DAA).

e. Maintain situational awareness and initiate actions to improve or restore the IA posture of the assigned WMA IS.

f. Notify the WMA Authorizing Official (i.e., DAA) of any CAT 1 weaknesses discovered after an accreditation decision is granted to a WMA IS.

g. Define IA requirements for the WMA IS.

h. Conduct the life cycle security reviews of security controls and test selected security controls to confirm their effectiveness. Submit a signed report on the results of the annual security review to the WMA Authorizing Official (i.e., DAA).

i. Review and approve the security requirements identified for IT products, services, and contract support required to develop the WMA IS.

j. Assist in developing SCGs for assigned WMA ISs.

k. Enter and maintain data in the DITPR or SIPRNET IT Registry and eMASS (when required) for assigned WMA ISs.

13. ISSE shall:

a. Implement and modify the IA component of the WMA IS architecture in compliance with the GIG architecture.

b. Maximize the use of enterprise IA capabilities and services in the WMA IS.

14. WMA ISSOs (i.e., WMA IAOs) shall perform duties as defined in reference i.

## ENCLOSURE C

## REFERENCES

a. DODI 8510.01, 28 November 2007, “Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)”

b. DODI 8115.02, 30 October 2006, “Information Technology Portfolio Management Implementation”

c. CNSSI No. 4009, 26 April 2010, “National Information Assurance (IA) Glossary”

d. DODD 8500.01E, 24 October 2002 (current as of 21 April 2007), “Information Assurance (IA)”

e. DOD memorandum, 23 July 2009, “DOD Information System Certification and Accreditation Reciprocity”

f. DODI 5000.02, 8 December 2008, “Operation of the Defense Acquisition System”

g. DODD 8570.01, 15 August 2004, Information Assurance Training, Certification, and Workforce Management

h. CJCSI 6211.02C Series, “Defense Information System Network (DISN): Policy and Responsibilities”

i. DODI 8500.2, 6 February 2003, “Information Assurance (IA) Implementation”

j. DOD 8570.01-M, 20 April 2010, “Information Assurance Workforce Improvement Program”

k. CJCSI 6510.01 Series, “Information Assurance (IA) and Computer Network Defense (CND)”

l. CJCSI 8410.01A Series, “WarFighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing”

(INTENTIONALLY BLANK)

# GLOSSARY

## PART 1 -- ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| | A |
| ATO | Authorization to Operate |
| | C |
| C&A | Certification and Accreditation |
| CA | Certification Authority |
| CAT | category |
| CC/S/A | combatant command, Service, Defense agency |
| CIO | Chief Information Officer |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CNSSI | Committee on National Security Systems instruction |
| CTO | Critical Tasking Order |
| CT&E | certification, test, and evaluation |
| | D |
| DAA | Designated Accrediting Authority |
| DATO | Denial of Authorization to Operate |
| DDC4 | Deputy Director for Command, Control, Communications, and Computer Systems |
| DIACAP | DOD Information Assurance Certification and Process |
| DIP | DIACAP Implementation Plan |
| DISN | Defense Information Systems Network |
| DITPR | DOD Information Technology Portfolio Registry |
| DOD | Department of Defense |
| DODD | DOD directive |
| DODI | DOD instruction |
| DSAWG | Defense Information Assurance Security Accreditation Working Group |
| | E |
| eMASS | Enterprise Mission Assurance Support Service |
| | F |
| FISMA | Federal Information Security Management Act |
| FRAGO | Fragmentary Order |
| | G |
| GIG | Global Information Grid |

I

| | |
|---|---|
| IA | information assurance |
| IAM | Information Assurance Manager |
| IAO | Information Assurance Officer |
| IATO | Interim Authorization to Operate |
| IATT | Interim Authorization to Test |
| IAVA | Information Assurance Vulnerability Alert |
| IS | information system |
| ISSE | Information Systems Security Engineer |
| ISSM | Information Systems Security Manager |
| ISSO | Information System Security Officer |
| IT | information technology |

M

| | |
|---|---|
| MAC | Mission Assurance Category |

N

| | |
|---|---|
| NSA | National Security Agency |

P

| | |
|---|---|
| PAA | Principal Accrediting Authority |
| POA&M | Plan of Action and Milestones |
| PM | Program Manager |

S

| | |
|---|---|
| SCG | Security Classification Guide |
| SIP | System Identification Profile |
| SIPRNET | Secret Internet Routing Protocol Network |
| SRRs | Security Readiness Review Scripts |
| STIG | Security Technical Implementation guide |

U

| | |
|---|---|
| UCP | Unified Command Plan |
| USCYBERCOM | United States Cyber Command |
| USSTRATCOM | United States Strategic Command |

W

| | |
|---|---|
| WMA | Warfighting Mission Area |

## PART II -- DEFINITIONS

See reference a for the definitions of IA terms used in this instruction.

(INTENTIONALLY BLANK)