



Department of Defense

INSTRUCTION

NUMBER 8510.01
November 28, 2007

ASD(NII)/DoD CIO

SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)

- References:**
- (a) Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002"
 - (b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
 - (c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
 - (d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
 - (e) through (ab), see Enclosure 1

1. PURPOSE

This Instruction:

1.1. Implements References (a), (b), (c), and (d) by establishing the DIACAP for authorizing the operation of DoD Information Systems (ISs).

1.2. Cancels DoD Instruction (DoDI) 5200.40; DoD 8510.1-M; and ASD(NII)/DoD CIO memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance" (References (e), (f), and (g)).

1.3. Establishes or continues the following positions, panels, and working groups to implement the DIACAP: the Senior Information Assurance Officer (SIAO), the Principal Accrediting Authority (PAA), the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel, the IA Senior Leadership (IASL), the Defense (previously DISN) IA Security Accreditation Working Group (DSAWG), and the DIACAP Technical Advisory Group (TAG).

1.4. Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.

1.5. Prescribes the DIACAP to satisfy the requirements of Reference (a) and requires the Department of Defense to meet or exceed the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to Reference (a) and section 11331 of title 40, United States Code (Reference (h)).

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General (IG) of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the “DoD Components”).

2.1.2. DoD-owned ISs and DoD-controlled ISs operated by a contractor or other entity on behalf of the Department of Defense that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, consistent with Reference (b).

2.2. Nothing in this Instruction shall alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (Reference (i)) and other laws and regulations. The application of the provisions and procedures of this Instruction to SCI or other intelligence ISs is encouraged where they may complement or discuss areas not otherwise specifically addressed.

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The Department of Defense shall certify and accredit ISs through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls as defined in Reference (d). IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the GIG architecture and risk assessments that are conducted at DoD-wide, mission area (MA), DoD Component, and IS levels consistent with Reference (a).

4.2. The Department of Defense shall establish and use an enterprise decision structure for IA C&A that includes and integrates GIG MAs pursuant to DoD Directive (DoDD) 8115.01 (Reference (j)) and the DIACAP governance process prescribed in this Instruction.

4.3. The DIACAP shall support the transition of DoD ISs to GIG standards and a net-centric environment while enabling assured information sharing by:

4.3.1. Providing a standard C&A approach.

4.3.2. Providing guidance on managing and disseminating enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting.

4.3.3. Accommodating diverse ISs in a dynamic environment.

4.4. All DoD-owned or -controlled ISs shall be under the governance of a DoD Component IA program in accordance with Reference (d). The DoD Component IA program shall be the primary mechanism for ensuring enterprise visibility and synchronization of the DIACAP.

4.5. All DoD ISs shall be implemented using the baseline DoD IA controls in accordance with Reference (d). The baseline DoD IA controls may be augmented if required to address localized threats or vulnerabilities.

4.6. A DIACAP Scorecard with a manual or DoD Public Key Infrastructure (PKI)-certified digital signature shall be visible to the DoD Chief Information Officer (CIO) and the DoD Component CIOs. The DIACAP Scorecard shall document the designated accrediting authority (DAA) accreditation decision as well as the results of the implementation of required baseline IA controls and additional IA controls that may be required by the DoD Component or local IS.

4.7. An Information Technology (IT) Security Plan of Action and Milestones (POA&M) shall be developed and maintained to record the status of any corrective actions directed in association with an accreditation decision.

4.8. The accreditation status and supporting DIACAP Package of DoD ISs shall be made available to interconnecting ISs, if requested, to support DAA accreditation decisions and to the Office of the IG DoD for audit and Federal Information Security Management Act (FISMA) assessment purposes.

4.9. All DoD ISs with an authorization to operate (ATO) shall be reviewed annually to confirm that the IA posture of the IS remains acceptable. Reviews will include validation of IA controls and be documented in writing.

4.10. Resources for implementing the DIACAP shall be identified and allocated as part of the Defense planning, programming, budgeting, and execution process.

4.11. Contracts for systems, services, and programs covered by this Instruction shall include clauses requiring compliance with the DIACAP. Failure to include such clauses is not justification for DIACAP non-compliance.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD CIO (ASD(NII)/DoD CIO) shall:

5.1.1. Oversee implementation of this Instruction, distribute DIACAP information standards and sharing requirements, and manage the transition from the previous DoD C&A process (Reference (e)) to the DIACAP.

5.1.2. Conduct an annual assessment of DoD Component IA programs for presentation in the annual report to Congress required by Reference (a).

5.1.3. Appoint a PAA for DoD ISs governed by the Enterprise Information Environment MA (EIEMA).

5.1.4. Appoint a DoD SIAO corresponding to a senior agency information security officer in Reference (a).

5.1.5. Provide annual certification to the Secretary of Defense and Director of OMB confirming that the DIACAP process is current and more stringent than the standards required by the OMB and the Secretary of Commerce pursuant to Reference (a).

5.2. The DoD SIAO, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall direct and coordinate the DoD IA Program (Reference (d)) and:

5.2.1. Ensure DoD ISs are assigned to and governed by a DoD Component IA program.

5.2.2. Advise, inform, and support the GIG PAAs and their representatives.

5.2.3. Establish and maintain a DIACAP CCM process, a DIACAP TAG, and an online DIACAP Knowledge Service (KS).

5.3. The Director, Defense Information Systems Agency (DISA), under the authority, direction, and control of the ASD(NII)/DoD CIO, shall:

5.3.1. Develop security technical configuration and implementation validation requirements and associated expected results for IT products and services and provide automated validation capabilities to the DoD Components for use in the DIACAP.

5.3.2. Develop and provide DIACAP training and awareness products and a distributive training capability to support the DoD Components according to Reference (b) and DoDD 8570.1 (Reference (k)) and post the training materials on the IA Support Environment Web site (<http://iase.disa.mil/>).

5.3.3. Appoint a flag-level representative to the DISN/GIG Flag Panel (previously the DISN Flag Panel).

5.4. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.4.1. Appoint a PAA for DoD ISs governed by the Business MA (BMA).

5.4.2. Participate in the DIACAP TAG to ensure that the DIACAP and execution of the responsibilities established in DoDI 5000.2 (Reference (l)) are mutually supportive.

5.5. The Under Secretary of Defense for Intelligence (USD(I)) shall appoint a PAA for all DoD ISs governed by the Defense Intelligence MA (DIMA).

5.6. The Director, Defense Intelligence Agency, under the authority, direction, and control of the USD(I), shall appoint a flag-level representative to the DISN/GIG Flag Panel.

5.7. The Director, National Security Agency, under the authority, direction, and control of the USD(I), shall:

5.7.1. Develop the IA component of the GIG architecture (Reference (c)) and publish supporting implementation material in the DIACAP KS.

5.7.2. Engage the GIG IA capability, services provider, and user communities -- to include commercial, defense, and other government agencies -- to foster development and evaluation of IA implementation and validation solutions that support the DIACAP.

5.7.3. Ensure that IA security engineering services provided to the DoD Components support the DIACAP.

5.7.4. Appoint a flag-level representative to the DISN/GIG Flag Panel.

5.8. The Heads of the DoD Components shall:

5.8.1. Ensure DoD ISs under their purview comply with the DIACAP.

5.8.2. Operate only accredited ISs (i.e., those with a current ATO, interim authorization to operate (IATO), or interim authorization to test (IATT)).

5.8.3. Comply with all accreditation decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATD).

5.8.4. Ensure that an annual assessment of the DoD Component IA program is conducted as required by Reference (a).

5.8.5. Appoint DAAs for DoD ISs under their purview.

5.8.6. Provide training and ensure appropriate professional certification for personnel engaged in or supporting the DIACAP is consistent with Reference (k) and supporting issuances.

5.8.7. Ensure that the information owner(s) appoints a user representative(s) (UR) for DoD ISs under the DoD Component's purview.

5.8.8. In the absence of a DoD Component CIO, appoint the SIAO.

5.9. The Chairman of the Joint Chiefs of Staff shall:

5.9.1. Appoint a PAA for DoD ISs governed by the Warfighting MA (WMA).

5.9.2. Ensure that Joint Capabilities Integration and Development System (JCIDS) implementation guidance requires DIACAP planning consistent with this Instruction.

5.10. The Commander, United States Strategic Command, shall:

5.10.1. Assign DAAs for space systems used by the Department of Defense in accordance with DoDD 8581.1 (Reference (m)).

5.10.2. Accredit IS processing, storing, or transmitting Nuclear Command and Control Extremely Sensitive Information (NC2-ESI) data.

5.10.3. Appoint a flag-level representative to the DISN/GIG Flag Panel.

5.11. The PAAs shall:

5.11.1. Represent the interests of the MA and, as required, issue accreditation guidance specific to the MA, consistent with this Instruction.

5.11.2. Appoint flag-level (e.g., general officer, senior executive) PAA Representatives to the DISN/GIG Flag Panel.

5.11.3. Resolve accreditation issues within their respective MAs and work with other PAAs to resolve issues among MAs, as needed.

5.11.4. Designate DAAs for MA ISs, if required, in coordination with appropriate DoD Components.

5.12. The PAA Representatives shall:

5.12.1. Serve as members of the DISN/GIG Flag Panel.

5.12.2. Provide MA-related guidance to DAAs, Milestone Decision Authorities (Reference (j)), the DSAWG, and the DIACAP TAG.

5.12.3. Advise the corresponding MA PAAs and assist the ASD(NII)/DoD CIO and SIAO in assessing the effectiveness of GIG IA capabilities.

5.13. The DoD Component CIOs shall:

5.13.1. Appoint a DoD Component SIAO in accordance with Reference (a) to direct and coordinate the DoD Component IA program consistent with the strategy and direction of the Defense-wide Information Assurance Program (DIAP).

5.13.2. Ensure that implementation and validation of IA controls through the DIACAP are incorporated as an element of the DoD Component IS life-cycle management processes.

5.13.3. Ensure that the C&A status of the DoD Component ISs is visible to the ASD(NII)/DoD CIO and PAAs.

5.13.4. Ensure collaboration and cooperation between the DoD Component IA program and the PAA and DAA structure.

5.13.5. Verify that a program or system manager is identified for each DoD Component IS.

5.13.6. Establish and manage an IT Security POA&M program.

5.14. The DoD Component SIAOs, under the authority, direction, and control of the DoD Component CIOs, shall:

5.14.1. Establish and enforce the C&A process within the DoD Component IA program.

5.14.2. Ensure DoD Component-level participation in the DIACAP TAG.

5.14.3. Track the C&A status of ISs that are governed by the DoD Component IA program.

5.14.4. Establish and manage a coordinated IA certification process for ISs governed by the DoD Component IA program. This includes but is not limited to:

5.14.4.1. Functioning as the certifying authority (CA) or formally delegating CA for governed ISs.

5.14.4.2. Ensuring and overseeing a qualified certification cadre (e.g., validators, analysts, CA representatives).

5.14.4.3. Identifying and recommending changes and improvements to certification and validation procedures to the TAG for inclusion in the DIACAP KS.

5.14.4.4. Ensuring that DoD Component certification guidance is posted to the DoD Component portion of the KS.

5.14.5. Serve as the single IA coordination point for joint or Defense-wide programs that are deploying ISs to DoD Component enclaves.

5.15. The DAAs, in addition to the responsibilities established in Reference (d), shall:

5.15.1. Comply with DISN/GIG Flag Panel direction issued on behalf of the GIG MA PAAs.

5.15.2. Ensure a DIACAP package is initiated and completed for assigned ISs.

5.15.3. Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.

5.15.4. Ensure security classification guides are established according to DoD 5200.1-R (Reference (n)).

5.15.5. Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.

5.16. The Program Manager (PM) or System Manager (SM) for DoD ISs shall:

5.16.1. Ensure that each assigned DoD IS has a designated IA manager (IAM) with the support, authority, and resources to satisfy the responsibilities established in Reference (d) and this Instruction.

5.16.2. Implement the DIACAP for assigned DoD ISs.

5.16.3. Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

5.16.4. Ensure that information system security engineering is employed to implement or modify the IA component of the system architecture in compliance with the IA component of the GIG Architecture (Reference (c)) and to make maximum use of enterprise IA capabilities and services.

5.16.5. Enforce DAA accreditation decisions for hosted or interconnected DoD ISs.

5.16.6. Develop, track, resolve, and maintain the DIACAP Implementation Plan (DIP) for assigned DoD ISs.

5.16.7. Ensure IT Security POA&M development, tracking, and resolution.

5.16.8. Ensure annual reviews of assigned ISs required by FISMA are conducted.

5.17. The DoD IS URs shall:

5.17.1. Represent the operational interests of the user community in the DIACAP.

5.17.2. Support the IA controls assignment and validation process to ensure user community needs are met.

5.18. The IAMs, in addition to the responsibilities established in Reference (d), shall:

5.18.1. Support the PM or SM in implementing the DIACAP.

5.18.2. Advise and inform the governing DoD Component IA program on DoD ISs C&A status and issues.

5.18.3. Comply with the governing DoD Component IA program information and process requirements.

5.18.4. Provide direction to the IA Officer (IAO) in accordance with Reference (d).

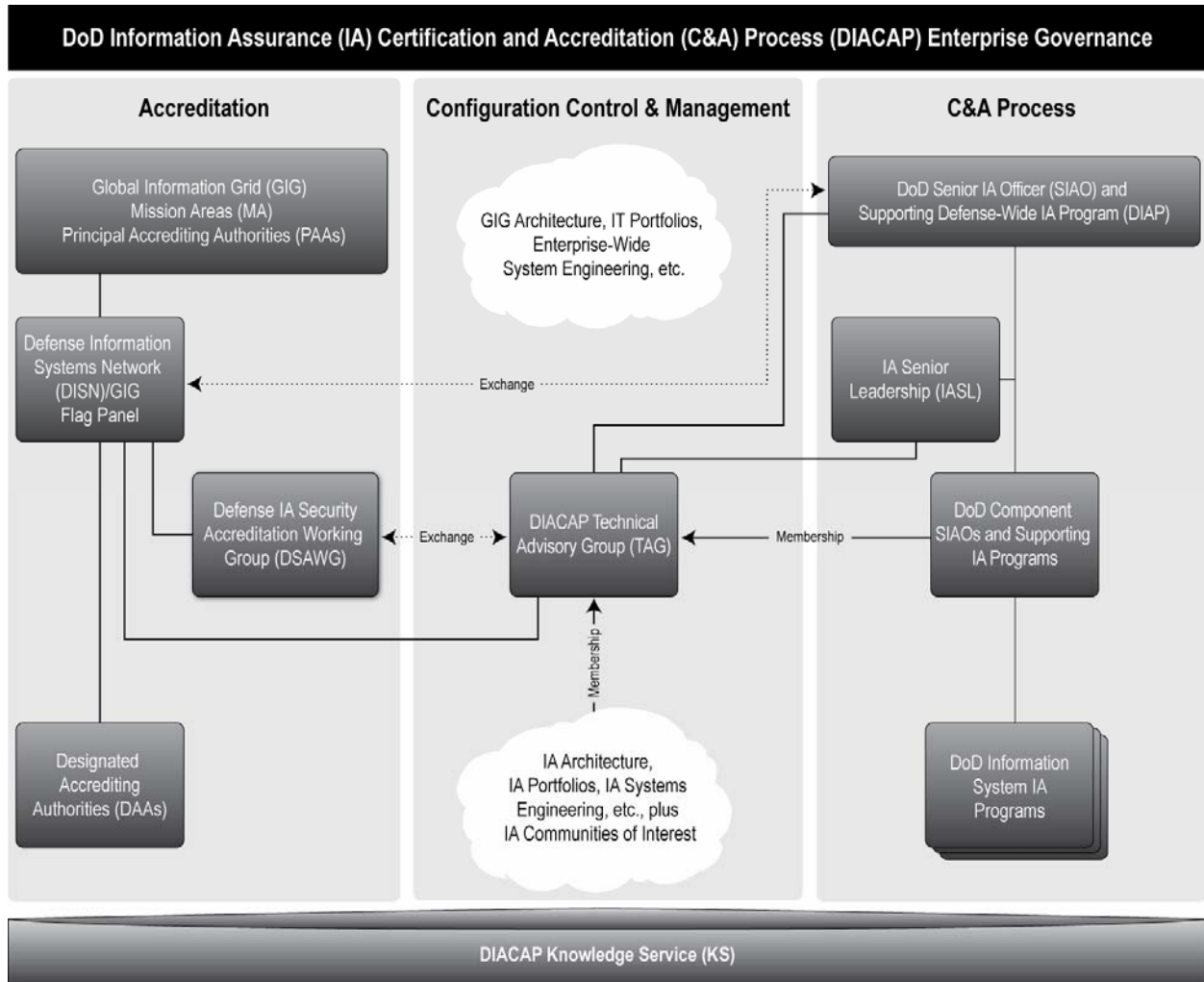
5.18.5. Coordinate with the organization's Security Manager to ensure issues affecting the organization's overall security are addressed appropriately.

6. PROCEDURES

6.1. Background. This section describes the DoD procedures for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISs. It also describes the processes for configuration management of DoD IA controls and supporting implementation materials. DIACAP activities and roles are distributed across all levels of the DoD and GIG governance structures, as well as all stages of the life cycle of both the IA Component of the GIG (Reference (c)) and of individual ISs. DIACAP implementation is supported by the DIACAP KS, a Web-based DoD resource that provides the most current requirements, guidance, and tools for implementing and executing the DIACAP, including IA control implementation procedures. Enclosure 4 provides additional information on the KS.

6.2. DIACAP Enterprise Governance. This structure is intended to synchronize and integrate DIACAP activities across all levels of the DoD and GIG MAs, all aspects of the IT life cycle, and logical and organizational entities. It comprises three major elements: an accreditation structure; a CCM structure; and a C&A process structure. These elements are illustrated in Figure F1. and described in subparagraphs 6.2.1. through 6.2.4.

Figure F1. DIACAP Enterprise Governance



6.2.1. Accreditation

6.2.1.1. PAAs are appointed for each of the GIG MAs (i.e., the EIEMA, BMA, WMA, and DIMA). PAAs may directly appoint DAAs for DoD ISs supporting an MA Community of Interest (COI) (DoD 8320.2-G (Reference (o))). DAAs have the authority and responsibility for accreditation decisions.

6.2.1.2. The DISN/GIG Flag Panel (charter under development), acting on behalf and in support of the PAAs, is responsible for advising PAAs; assessing enterprise risk; authorizing information exchanges and connections for enterprise IS, cross-MA IS, cross security domain connections, and non-DoD connections; and approving changes to the DoD IA control baseline.

6.2.1.3. The DSAWG (DoD CIO memorandum (Reference (p))), under the DISN/GIG Flag Panel, is the community forum for reviewing and resolving C&A decisions related to the sharing of community risk. The DSAWG develops and provides guidance to the DAAs for IS connections to the GIG.

6.2.2. CCM

6.2.2.1. The DIACAP TAG (ASD(NII) memorandum (Reference (q))) provides CCM of the DIACAP through interfacing with the DoD Component IA programs, IA COIs, and other entities (e.g., the GIG IA Program Office, DSAWG) to address issues that are common across all entities, by:

6.2.2.1.1. Providing detailed analysis and authoring support for the enterprise portion of the DIACAP KS content.

6.2.2.1.2. Recommending changes to the baseline IA controls to the DISN/GIG Flag Panel.

6.2.2.1.3. Recommending changes to the C&A process to the DoD SIAO.

6.2.2.1.4. Advising the IASL and other IA advisory forums identified by the DoD SIAO to resolve C&A priorities and cross-cutting issues.

6.2.2.1.5. Developing and managing DoD enterprise-level C&A automation requirements.

6.2.2.2. The TAG is supported by the DIACAP KS, described in Enclosure 4. The DIACAP KS enables TAG functions and activities, including maintenance of membership; voting, analysis, and authoring; and configuration control of KS enterprise content and functionality.

6.2.3. C&A Responsibilities. The DoD SIAO directs and coordinates the DoD IA Program. DoD Component SIAOs have authority and responsibility for certification. Each DoD Component SIAO serves as the CA for all DoD ISs assigned to or governed by the DoD Component CIO and supporting IA program. Each CA may task, organize, staff, and centralize or delegate certifying activities. Regardless of the adopted model, the SIAO is responsible for certification quality, capacity, visibility, and effectiveness. In addition, each CIO, supported by an appointed SIAO, is responsible for administration of the overall C&A process. This includes the integration of certification with other DIACAP activities, participation in the DIACAP CCM, visibility and sharing of the C&A status of assigned ISs, enforcement of training requirements

for persons participating in the DIACAP, support to DAAs, and responsiveness to the DoD CIO. The IASL (DoD CIO memorandum (Reference (r))) serves as an SIAO community forum for assessing and improving C&A process administration. The IASL provides strategic direction and guidance to ensure integrated Defense-wide IA. It provides for the integrated planning, coordination, and oversight of the Department’s IA programs.

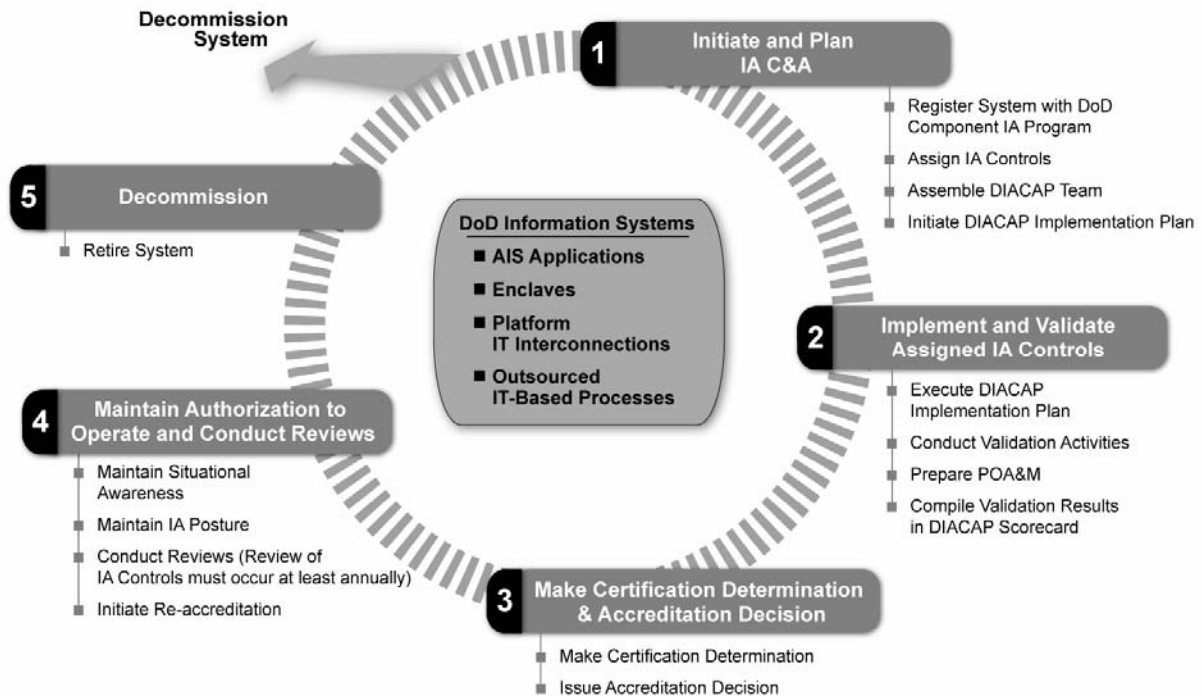
6.2.4. C&A Role Appointment. Table T1. identifies the appropriate authority for the appointment of C&A roles.

Table T1. Appointment of C&A Roles

| C&A Role | Appointed By |
|---------------------------------------|---|
| PAA | GIG MA Owner |
| PAA Representative | PAA |
| DAA | DoD Component Head or designee; PAA for MA-managed ISs |
| CIO | DoD Component Head |
| SIAO | DoD Component CIO or, in organizations in which the position of DoD Component CIO does not exist, the DoD Component Head Note: DoD SIAO appointed by DoD CIO |
| CA | SIAO is the Component CA, but may formally delegate the CA role as appropriate |
| CA Representative, Analyst, Validator | Component CA or CA delegates |
| IAM | PM or SM |
| IAO | IAM |
| UR | Information Owner |
| DIACAP TAG Representative | DoD Component SIAO or DoD Component CIO |

6.3. DIACAP Activities. The DIACAP consists of the activities and tasks depicted in Figure F2. The DIACAP parallels the system life cycle, and its activities should be initiated at inception (e.g., documented during capabilities identification or at the implementation of a major system modification). However, failure to initiate the DIACAP at system inception is not a justification for ignoring or not complying with the DIACAP. Unaccredited systems shall initiate the DIACAP immediately, regardless of the system life-cycle stage (e.g., acquisition, operation).

Figure F2. DIACAP Activities



6.3.1. Initiate and Plan IA C&A. This activity includes registering the system with the governing DoD Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS’s DIP.

6.3.1.1. Register the System with the DoD IA Program. System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. DIACAP registration is related to other DoD initiatives to collect IT-related information (e.g., the Defense Information Technology Portfolio Repository); however, specific registration instructions change over time and are therefore maintained through the DIACAP CCM and published in the DIACAP KS. The System Identification Profile (SIP) is generated during the registration process and becomes part of the DIACAP package for the IS. Attachment 1 to Enclosure 3 of this Instruction identifies the minimum data requirements and explanations for the SIP.

6.3.1.2. Assign IA Controls. Identifying applicable IA controls for an information system is a critical activity in the DIACAP. There are four basic steps in assigning the IA controls: determining the type of information system; determining the MAC and CL for the information system; identifying the baseline IA controls; and augmenting the baseline IA controls.

6.3.1.2.1. Baseline IA controls originate from Reference (d) control sets, are based on MAC and CL, and are implemented through procedures presented in the DIACAP KS.

6.3.1.2.2. Baseline IA control sets can be augmented with additional IA controls to address special security needs or unique requirements of the IS(s) to which they apply. Augmenting IA controls originate from an MA, a DoD Component, a COI, or a local system. Augmenting IA controls must neither contradict nor negate DoD baseline IA controls, must not degrade interoperability across the DoD Enterprise, and may not be used as a basis for denying connectivity of systems that have met the DoDI 8500.2 baseline IA controls for MAC and CLs of the gaining IS. Procedures for implementing augmenting IA controls are the responsibility of the originator.

6.3.1.2.3. Assigned IA controls may be inherited. Inheritance refers to situations where IA controls along with their validation results and compliance status are shared by two or more systems for the purposes of C&A. Through inheritance, an existing IA control and its compliance status extends from an originating IS to a receiving IS. Inheritance eliminates the need for the receiving systems to duplicate testing and documentation of inherited IA controls. The DIP specifically identifies IA controls inherited from other systems. The compliance status of IA controls inherited from the originating IS is reflected on the DIACAP Scorecard of the receiving IS.

6.3.1.3. Assemble the DIACAP Team

6.3.1.3.1. The members of the DIACAP Team are required to meet the trustworthiness investigative levels for users with IA management access to DoD unclassified ISs as established in Section E3.4.8. of Reference (d). SIAOs shall meet the same investigative requirements as those for DAA, and certification cadre members shall meet the same requirements as those established for monitoring and testing in Table E3.T1. of Reference (d).

6.3.1.3.2. DIACAP Team members will be trained and certified in accordance with Reference (k), as required.

6.3.1.3.3. Allowable relationships among DIACAP Team members are outlined in Table T2.

Table T2. Allowable Relationships Among DIACAP Team Members

| Relationships | Allowed (Y/N) |
|---|----------------------|
| PAA may be a DAA | Yes |
| DAA reports to the PM, SM, or Program Executive Officer (PEO) | No |
| DAA and CA for a DoD IS may be the same person | Yes |
| CIO may be a DAA | Yes |
| CA reports to a DAA | Yes |
| CA reports to the PM , SM, or PEO | No |
| PM or SM and CA both report to the DAA | Yes |
| PM or SM and CA for a DoD IS may be the same person | No |
| PM or SM and DAA for a DoD IS may be the same person | No |
| PM or SM and UR for a DoD IS may be the same person | No |
| PM or SM reports to CA | No |
| PM or SM reports to the CIO | Yes |
| PM or SM reports to the DAA | Yes |
| UR reports to the CIO | Yes |
| UR reports to the PM or SM | No |
| UR reports to the SIAO/CA | Yes |

6.3.1.4. Initiate the DIP. This plan contains the IS's assigned IA controls, including inherited IA controls. The plan also includes the IA control implementation status, responsible entities, resources, and the estimated completion date for each assigned IA control. The plan may reference applicable supporting implementation material and artifacts.

6.3.2. Implement and Validate Assigned IA Controls. This activity includes executing the DIP, conducting validation activities, preparing the IT Security POA&M, and compiling the validation results in the DIACAP Scorecard.

6.3.2.1. Execute the DIP. Each assigned IA control is implemented according to the applicable implementation guidelines described in the DIACAP KS.

6.3.2.2. Conduct Validation Activities. Validation procedures are maintained through the DIACAP CCM and published in the DIACAP KS. Each validation procedure describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results. Each procedure includes 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 and are made 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). For inherited IA controls, validation test results and supporting documentation are maintained by the originating IS and are made available to CAs of receiving ISs on request.

6.3.2.3. Record Compliance Status. The status of each assigned IA control is indicated on the DIACAP Scorecard. An example of a Scorecard and discussion of its fields are provided in Attachment 2 to Enclosure 3.

6.3.2.3.1. Compliant (C) IA controls are those for which the expected results for all associated validation procedures have been achieved.

6.3.2.3.2. Non-compliant (NC) IA controls are those for which one or more of the expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.

6.3.2.3.3. Not applicable (NA) IA controls are those that do not impact the IA posture of the IS as determined by the DAA.

6.3.2.4. Prepare an IT Security POA&M. An IT 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. IT 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 IT Security POA&Ms. IT 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 IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, 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 IT Security POA&M is also used to document DAA-accepted NC IA controls and baseline IA controls that are NA because of the nature of the system. A full discussion and templates for preparing an IT Security POA&M are provided in Attachment 3 to Enclosure 3.

6.3.3. Make Certification Determination and Accreditation Decision

6.3.3.1. The CA makes certification determinations.

6.3.3.1.1. A CA representative is an active member of the DIACAP Team from inception and continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts.

6.3.3.1.2. Certification considers:

6.3.3.1.2.1. The overall reliability and viability of the DoD IS plus the acceptability of the implementation and performance of IA mechanisms or safeguards inherent in the system.

6.3.3.1.2.2. The system behavior in the larger information environment, including consideration of vulnerabilities to the environment, correct and secure interactions with the information environment management and control services, and visibility into situational awareness and network defense services.

6.3.3.1.3. Impact codes are assigned by the TAG to IA controls at the time of authoring and are maintained through the DIACAP CCM. They indicate the TAG's assessment of the consequences of a failed IA control. Impact codes are expressed as high, medium, and low, with high indicating the greatest impact. In conjunction with the severity category, the impact code indicates the urgency with which corrective action should be taken. Within a severity category, non-compliant IA controls should be prioritized for correction or remediation according to their impact codes.

6.3.3.1.4. Severity categories are assigned to a system weakness or shortcoming by a CA or a designated representative as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as category (CAT) I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS in question. For instance, what may be a CAT I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves so that the overall risk to the system is reduced to a CAT II.

6.3.3.1.4.1. CAT I weaknesses shall be corrected before an ATO is granted.

6.3.3.1.4.2. CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.

6.3.3.1.4.3. CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.

6.3.3.1.5. The certification determination is based on the actual validation results. It considers impact codes associated with IA controls in a non-compliant status, associated severity categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). The weaknesses identified on the IT Security POA&M reflect residual risk to the system. See Attachment 3 to Enclosure 3 for further discussion on IT Security POA&M formulation.

6.3.3.1.6. A certification determination is always required before an accreditation decision. If a compelling mission or business need requires the rapid introduction of a new DoD IS into the GIG, validation activity and a certification determination are still required. If the operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

6.3.3.2. The DAA issues accreditation decisions.

6.3.3.2.1. An accreditation decision is communicated via the DIACAP Scorecard and accompanying IT Security POA&M, if required.

6.3.3.2.2. Documentation (e.g., artifacts, actual validation results) supporting an accreditation decision will be provided in electronic form if requested by DAAs of interconnecting systems.

6.3.3.2.3. An accreditation decision always applies to a specifically identified DoD IS and is based on a balance of mission or business need, protection of personal privacy, protection of the information being processed, and protection of the information environment and thus, by extension, protection of other missions or business functions reliant on the shared information environment.

6.3.3.2.4. An accreditation decision always requires a certification determination. If the validation is abbreviated as a result of mission urgency, the accreditation decision cannot exceed an IATO. If operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

6.3.3.2.5. When there is compelling operational necessity, DoD ISs may be allowed to operate despite IT security weaknesses that cannot be corrected or adequately mitigated within prescribed timeframes because of technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented.

6.3.3.2.6. An accreditation decision is expressed as an ATO, an IATO, an IATT, or a DATO. A system is considered unaccredited if an accreditation decision has not been made.

6.3.3.2.6.1. ATO

6.3.3.2.6.1.1. An ATO accreditation decision must specify an authorization termination date that is within 3 years of the authorization date.

6.3.3.2.6.1.2. A system with a CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. When requested by an affected military commander, the DoD Component CIO shall authorize operation of a system with a CAT I weakness through an IATO. This responsibility cannot be delegated below the DoD Component CIO, and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO and the system's DAA.

6.3.3.2.6.1.3. A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

6.3.3.2.6.1.4. An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA."

6.3.3.2.6.2. IATO

6.3.3.2.6.2.1. An IATO accreditation decision is intended to manage IA security weaknesses while allowing system operation. It is not intended to be a device for signaling an evolutionary acquisition. A version of a DoD IS acquired in one of a planned series of acquisition increments or development spirals should be granted an ATO, even if additional or enhanced capabilities and services are planned for future increments or spirals. The ATO accreditation decision should not be reserved for DoD ISs for which no change is planned or foreseen. Such thinking engenders an abuse of the IATO accreditation status and is an inaccurate portrayal of the DoD ISs' IA posture.

6.3.3.2.6.2.2. An IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days.

6.3.3.2.6.2.3. A request for an IATO must be accompanied by an IT Security POA&M that documents identified weaknesses and specifies corrective measures, as appropriate. Corrective actions specified in the IT Security POA&M must be achievable within the authorization period and resourced accordingly.

6.3.3.2.6.2.4. If CAT II weaknesses have not been corrected or satisfactorily mitigated after system operation under IATOs for a total of 360 days, the DAA will normally issue a DATO that will remain in effect until all corrective actions identified in the IT Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO.

6.3.3.2.6.2.5. The DoD Component CIO may authorize continuation of operation under IATO for systems with CAT II weaknesses that have operated for 360 consecutive days. This responsibility cannot be delegated below the DoD Component CIO. The DAA must certify in writing or through DoD PKI-certified digital signature that continued system operation is critical to mission accomplishment. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.

6.3.3.2.6.3. IATT

6.3.3.2.6.3.1. The IATT accreditation decision is a special case for authorizing testing in an operational information environment or with live data for a specified time period. IATTs should be granted only when operational environment/live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical).

6.3.3.2.6.3.2. All applicable IA controls should 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 SM, the DAA will determine which IA controls can only be tested in an operational environment.

6.3.3.2.6.3.3. An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate. Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).

6.3.3.2.6.4. DATO. A DATO will be issued if the DAA determines that a DoD IS should not operate because the IA design is inadequate, assigned IA controls are not adequately implemented, or because of a lack of other adequate security is revealed through certification activities and there are no compelling reasons to allow system operation under subparagraphs 6.3.3.2.6.1.2 or 6.3.3.2.6.2.5. If the system is already operational, the DAA will issue a DATO and halt operation of the system immediately.

6.3.4. Maintain Authorization to Operate and Conduct Reviews. Continued ATO is contingent on the sustainment of an acceptable IA posture. The DoD IS IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture.

6.3.4.1. Maintain Situational Awareness. Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM continuously monitors the system or 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 (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations. 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. Reference (a) requires revalidation of a select number of IA controls at least annually.

6.3.4.1.1. 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.

6.3.4.1.2. If a newly discovered CAT I weakness on a DoD IS operating with an ATO cannot be corrected within 30 days, the system can only continue operation under the terms prescribed in subparagraph 6.3.3.2.6.1.2.

6.3.4.1.3. If a newly discovered CAT II weakness on a DoD IS 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 subparagraph 6.3.3.2.6.2.5.

6.3.4.2. 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 IS itself.

6.3.4.3. Perform Reviews. The IAM shall annually provide a written or DoD PKI-certified digitally signed statement to the DAA and the CA that indicates the results of the security review of all IA controls and the testing of selected IA controls as required by Reference (a). The review will either confirm the effectiveness of assigned IA controls and their implementation, or it will recommend: changes such as those described in subparagraph 6.3.4.2.; a change in accreditation status (e.g., accreditation status is downgraded to IATO or DATO); or development of an IT Security POA&M. The CA and DAA shall review the IAM statement in light of mission and information environment indicators and determine a course of action that will be provided to the concerned CIO or SIAO for reporting requirements described in Reference (a). The date of the annual security review will be recorded in the SIP. A DAA may downgrade or revoke an accreditation decision at any time if risk conditions or concerns so warrant.

6.3.4.4. Initiate Reaccreditation. In accordance with OMB Circular A-130 (Reference (s)), an IS must be recertified and reaccredited once every 3 years. The results of an annual review or a major change in the IA posture at any time may also indicate the need for recertification and reaccreditation of the IS.

6.3.5. 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.

6.4. Transition to DIACAP. All DoD ISs are required to transition to the DIACAP in accordance with the timeline and instructions specified in Enclosure 5. The DoD Components are responsible for ensuring that all assigned DoD ISs meet the specified timelines.

6.5. IA Product Evaluation and DIACAP Evaluation. The DIACAP validation of a DoD IS that consists of a single IA -enabled product or solution (e.g., an IA-enabled database management system) may also serve as the IA-enabled product evaluation. These conditions are reiterated in Table T3.

Table T3. IA Product Evaluation and DIACAP Evaluation

| Condition | Acceptable Evaluation/Validation Approach |
|---|--|
| Accreditation boundary includes both IT products or services and IA or IA-enabled IT products. | <ol style="list-style-type: none"> 1. National Security Telecommunications and ISs Security Policy No.11 (Reference (t)) evaluation for IA and IA-enabled products; and 2. DIACAP for overall system design and configuration. |
| Proposed accreditation boundary includes ONLY a single IT product or service that is IA-enabled and nothing else. | DIACAP validation is sufficient; separate Reference (t) evaluation is not required. |

6.6. System Interconnection. Reference (s) requires “written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.” DoD ISs generally satisfy this requirement through compliance with connection management procedures established by the Chairman of the Joint Chiefs of Staff. Separately accredited ISs that communicate directly through tightly coupled mechanisms, such as shared memory or direct code invocation, are not subject to this requirement. In addition, for IA purposes, loosely coupled ISs (e.g., by proxy) communicating via Web services are not considered system interconnections and do not require connection approval, a security memorandum, or written management authorization. Dynamic interaction among accredited software systems that have been designed to interact is not considered a security-relevant event. This includes authorized messaging with non-DoD ISs (e.g., electronic commerce/electronic data interchange transactions with an IS belonging to another department or agency).

6.7. Type Accreditation. The type accreditation is the official authorization to employ identical copies of a system in specified environments. This form of C&A allows a single DIACAP package (i.e., SIP, DIP, supporting documentation for certification, DIACAP Scorecard, and IT Security POA&M (if required)) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. Automated Information System (AIS) applications accreditations are type accreditations. Stand-alone IS and demilitarized zone (DMZ) accreditations may also be type accreditations.

6.8. Stand-Alone IS Accreditation. Stand-alone ISs are treated as special types of enclaves that are not interconnected to any other network. Stand-alone systems do not transmit, receive, route, or interchange information outside of the system’s accreditation boundary. IA requirements for a stand-alone system are determined by its MAC and classification or sensitivity and need-to-know just as for other DoD ISs. Stand-alone systems must always be clearly identified as such on the IT Security POA&M, the SIP, and the DIACAP Scorecard. Because of the unique architecture of a stand-alone system, certain IA controls do not pose a risk to the system as a result of their non-implementation and thus are considered NA. NA IA controls are labeled as NA on the DIACAP Scorecard and addressed on the IT Security POA&M simply as a means to document and explain why the IA control is NA in the comments column. Refer to the KS for a discussion of IA controls that may be considered NA for stand-alone systems. Additionally, stand-alone systems that are deployed to multiple locations may be type accredited.

6.9. Outsourced IT-Based Processes. Outsourced IT-based processes supported by private sector ISs, outsourced ITs, and outsourced information services fall into two sub-categories that are treated differently for C&A purposes.

6.9.1. Outsourced IT-Based Processes Established for DoD Purposes Only. Outsourced IT-based processes that are dedicated to DoD processing and are effectively under DoD configuration control (e.g., the Navy Marine Corps Intranet) are certified and accredited as DoD enclaves. Typically, outsourced IT-based processes that are MAC I are in this sub-category and those that process classified information can only be in this sub-category.

6.9.2. Outsourced IT-Based Processes That Also Support Non-DoD Users. Outsourced IT-based processes that may also support non-DoD users or processes must still be certified and accredited by DoD entities. IA requirements for DoD information in an outsourced environment are determined by its MAC and classification or sensitivity and need-to-know just as for other DoD ISS. However, the following also applies.

6.9.2.1. Technical security of the outsourced environment is the responsibility of the service provider.

6.9.2.2. Outsourced applications that are accessed by DoD users from DoD enclaves (e.g., Powertrack) are subject to DoD enclave boundary defense IA controls for incoming traffic (e.g., ports and protocols and mobile code).

6.9.2.3. Responsibility for procedural and administrative security is shared between the service provider and the supported DoD entity contracting for the service.

6.9.2.4. Security responsibilities of the service provider down to the control level are made explicit in the contract, along with any other performance and service-level parameters by which the Department of Defense shall measure the IA profile of the outsourced IT-based process for the purpose of C&A.

6.9.2.5. Any baseline IA controls that are not explicit in the contract or otherwise covered by a service level agreement are categorized as NC. All such NC IA controls must be documented in an IT Security POA&M with an explanation as to why accepting the risk of operating the outsourced IT-based process with that control in an NC status is acceptable.

6.9.2.6. Security roles and responsibilities are to be made explicit in the acquisition along with the performance and service-level parameters by which the Department of Defense shall measure the IA profile of the outsourced IT-based process. The PM for an outsourced IT-based process will need to carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied in the acquisition in order to protect DoD information in the service provider's operating environment and interconnected DoD ISS.

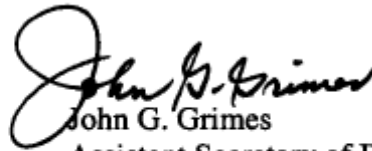
7. INFORMATION REQUIREMENTS

7.1. The annual assessment of the DoD Component IA programs for presentation in the annual report to Congress has been assigned Report Control Symbol (RCS) DD-NII(Q,A)2296 in accordance with DoD 8910.1-M (Reference (u)).

7.2. The DIACAP Package Contents and the review of proposed changes to the IA processes, procedures, and tools are exempt from licensing in accordance with paragraphs C4.4.2 and C4.4.3. of Reference (u).

8. EFFECTIVE DATE

This Instruction is effective immediately. Specific DoD IS transition timelines and instructions are provided in Enclosure 5.



John G. Grimes

Assistant Secretary of Defense for Networks
and Information Integration/
DoD Chief Information Officer

Enclosures – 5

- E1. References, continued
- E2. Definitions
- E3. The DIACAP Package
- E4. DIACAP KS Overview
- E5. DIACAP Transition Timeline and Instructions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (hereby canceled)
- (f) DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000 (hereby canceled)
- (g) Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer Memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006 (hereby canceled)
- (h) Section 11331 of title 40, United States Code
- (i) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (j) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005
- (k) DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004
- (l) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
- (m) DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 21, 2005
- (n) DoD 5200.1-R "Information Security Program," January 1997
- (o) DoD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006
- (p) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, Charter, "DISN Security Accreditation Working Group (DSAWG)," March 26, 2004¹
- (q) Assistant Secretary of Defense Networks and Information Integration Memorandum, "Charter of the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Technical Advisory Group (TAG)," July 26, 2007²
- (r) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum "Charter of IA Senior Leadership Group," March 5, 2004³
- (s) Appendix III to Office of Management and Budget Circular No. A-130, "Security of Federal Automated Information Resources," (Revised)
- (t) National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," June 2003
- (u) DoD 8910.1-M, "Procedures for Management of Information Requirements," June 1998
- (v) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," as revised June 2006
- (w) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended

¹ Available at <http://www.iase.disa.smil.mil/dsawg>

² Available at <https://diacap.iaportal.navy.mil/ks>

³ Available at <https://powhatan.iiie.disa.mil/iasl-iasg/charters.html>

- (x) DoD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense," April 23, 2007
- (y) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (z) OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003
- (aa) OMB Memorandum, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004
- (ab) OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," June 2006

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Accreditation Boundary. See Reference (v).

E2.2. Accreditation Decision. A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature.

E2.3. Adequate Security. See Reference (v).

E2.4. Artifacts. System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the information assurance (IA) posture of the DoD IS, make up the certification and accreditation (C&A) information, and provide evidence of compliance with the assigned IA controls.

E2.5. Assigned IA Controls. The set of IA controls that a given DoD IS must address to achieve an adequate IA posture. Consist of baseline IA controls plus any augmenting IA controls.

E2.6. Augmenting IA Controls. IA controls that augment baseline IA controls to address special security needs or unique requirements (e.g., cross security domain solutions, health information portability, privacy, etc.) of the IS(s) to which they apply. Augmenting IA controls may originate from a mission area (MA), a DoD Component, a Community of Interest (COI), or a local system. Augmenting IA controls must neither contradict nor negate DoD baseline IA controls and must not degrade interoperability across the DoD Enterprise.

E2.7. Authorization Termination Date (ATD). The date assigned by the DAA that indicates when an ATO, IATO, or IATT expires.

E2.8. Authorization to Operate (ATO). Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years.

E2.9. Baseline IA Controls. The minimum set of IA controls that must be addressed to achieve adequate security. Baseline IA controls are prescribed by DoDI 8500.2 (Reference (d)) based on mission assurance category (MAC) and confidentiality level (CL).

E2.10. Certification. For the purpose of this Instruction, a comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned IA controls based on standardized procedures.

E2.11. Certification Determination. A CA's determination of the degree to which a system complies with assigned IA controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA security weaknesses as documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M).

E2.12. Certifying Authority (CA). The senior official having the authority and responsibility for the certification of ISs governed by a DoD Component IA program.

E2.13. Certifying Authority Representative. An official appointed by and acting on behalf of the CA.

E2.14. Communities of Interest (COIs). For the purpose of this Instruction, the inclusive term used to describe groups of individuals who share information relative to common goals, interests, missions, or business processes.

E2.15. Community Risk. See Reference (b).

E2.16. Confidentiality Level (CL). See Reference (d).

E2.17. Core Enterprise Services (CESs). For the purpose of this Instruction, a set of common services intended to provide, enable, or improve access; enable information sharing; and enhance interoperability among Global Information Grid (GIG) entities. CESs enable service-oriented architectures and may include Web services. Examples of CESs include enterprise services management, messaging, discovery, mediation, collaboration, hosting, storage, IA/security, metadata services, and user assistance.

E2.18. Denial of Authorization to Operate (DATO). A DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

E2.19. Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (Reference (d) leads with the term designated approving authority, which was favored at the time of publication.)

E2.20. DIACAP Implementation Plan (DIP). Contains the IS's assigned IA controls. The plan also includes the implementation status, responsible entities, resources, and the estimated completion date for each assigned IA control. The plan may reference applicable supporting implementation material and artifacts.

E2.21. DIACAP Knowledge Service (KS). A Web-based repository of information and tools for implementing the DIACAP that is maintained through the DIACAP Technical Advisory Group (TAG).

E2.22. DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an IS. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. There are two types of DIACAP packages:

E2.22.1. The Comprehensive Package contains all of the information connected with the certification of the IS. It includes the System Identification Profile (SIP), the DIACAP Implementation Plan (DIP), the Supporting Certification Documentation, the DIACAP Scorecard, and the IT Security POA&M, if required.

E2.22.2. The Executive Package contains the minimum information for an accreditation decision. It contains the SIP, the DIACAP Scorecard, and the IT Security POA&M, if required.

E2.23. DIACAP Scorecard. A summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It shows the implementation status of a DoD IS's assigned IA controls (i.e., compliant (C), non compliant (NC), or not applicable (NA)) as well as the C&A status.

E2.24. DIACAP Technical Advisory Group (TAG). A formally chartered body established by Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer to examine and address common C&A issues, including changes to the baseline IA controls, across the DoD Component IA programs, IA COIs, and other GIG entities. The DIACAP TAG also maintains configuration control and management of the DIACAP and all its supporting content on the DIACAP KS.

E2.25. DIACAP Team. Comprised of the individuals responsible for implementing the DIACAP for a specific DoD IS. At a minimum the DIACAP Team includes the DAA, the CA, the DoD IS program manager (PM) or system manager (SM), the DoD IS IA manager (IAM), IA officer (IAO), and a user representative (UR) or their representatives.

E2.26. DoD-Controlled IS. An IS that is established only for DoD purposes, dedicated to DoD processing, and is effectively under DoD configuration control (e.g., the Navy Marine Corps Intranet).

E2.27. DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISs, including testing in a live environment, in accordance with statutory, Federal, and DoD requirements.

E2.28. DoD Information Systems. See Reference (b).

E2.29. Enterprise Information Environment. See Reference (j).

E2.30. Global Information Grid (GIG). See Reference (c).

E2.31. Impact Code. For the purpose of this Instruction, a code indicating the consequences of a non-compliant IA control. It is an indicator of the impact associated with exploitation of the IA control. In conjunction with the severity category, it also indicates the urgency with which corrective action should be taken. Impact codes are expressed as high, medium, and low, with high indicating the greatest impact.

E2.31.1. High Impact Code. The absence or incorrect implementation of the IA control may have a severe or catastrophic effect on system operations, management, or information sharing. Exploitation of the weakness may result in the destruction of information resources and/or the complete loss of mission capability.

E2.31.2. Medium Impact Code. The absence or incorrect implementation of the IA control may have a serious adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in loss of information resources and/or the significant degradation of mission capability.

E2.31.3. Low Impact Code. The absence or incorrect implementation of the IA control may have a limited adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in temporary loss of information resources and/or limit the effectiveness of mission capability.

E2.32. Implementation Procedures. Procedures describing the required steps and providing guidance for implementing DoD IA controls. Implementation procedures are found in the DIACAP KS.

E2.33. Information Assurance (IA). See Joint Publication 1-02 (Reference (w)).

E2.34. Information Assurance Control. See Reference (b).

E2.35. Information Assurance Manager (IAM). See Reference (d).

E2.36. Information Assurance Officer (IAO). See Reference (d).

E2.37. Information Assurance Support Environment. See Reference (d).

E2.38. Information Owner. See Reference (v).

E2.39. Information Resources. See Reference (w).

E2.40. Information System (IS). See Reference (d).

E2.41. Information System Security Engineering. See Reference (d).

E2.42. Interim Authorization to Operate (IATO). A temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.

E2.43. Interim Authorization to Test (IATT). A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

E2.44. IT Security Plan of Action and Milestones (POA&M). A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses. Required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks. Also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

E2.45. Mission Area (MA). See Reference (j).

E2.46. Mission Assurance Category (MAC). See Reference (b).

E2.47. Net-centric. See DoDD 8320.2 (Reference (x)).

E2.48. Platform IT Interconnection. See Reference (d).

E2.49. Principal Accrediting Authority (PAA). The senior official representing the interests of a GIG MA regarding C&A. Also issues C&A guidance specific to a GIG MA as required.

E2.50. Program Manager or System Manager (PM or SM). For the purpose of this Instruction, the individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.

E2.51. Proxy. See Reference (b).

E2.52. Residual Risk. See Reference (v).

E2.53. Security Relevant Event. For the purpose of this Instruction, an event that could cause a harmful change in an IS or its environment, or that an IAM would consider worthy of notation, investigation, or prevention (e.g., the discovery of malicious code in an IS, the discovery of an attempt to connect an unapproved device to the network).

E2.54. Senior Information Assurance Officer (SIAO). The official responsible for directing an organization's IA program on behalf of the organization's chief information officer.

E2.55. Service-Oriented Architecture. For the purpose of this Instruction, a paradigm for defining, organizing, and using distributed capabilities in the form of loosely coupled software services that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations.

E2.56. Severity Category. The category a CA assigns to a system security weakness or shortcoming as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as “Category (CAT) I, CAT II, or CAT III,” with CAT I indicating the greatest risk and urgency. Severity categories are assigned after consideration of all possible mitigation measures that have been taken within system design/architecture limitations for the DoD IS in question.

E2.56.1. CAT I Severity Category. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. An ATO will not be granted while CAT I weaknesses are present.

E2.56.2. CAT II Severity Category. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.

E2.56.3. CAT III Severity Category. Assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.

E2.57. Stand-Alone Information System. An information system operating independently of and without interconnection to any other information system.

E2.58. System Identification Profile (SIP). A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component IA program.

E2.59. User Representative (UR). An individual or organization that represents the user community for a particular system for DIACAP purposes.

E2.60. Validation. Activity applied throughout the system’s life cycle to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD IS’s assigned IA controls are implemented correctly and are effective in their application.

E2.61. Validation Procedure. Preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results that are used for validating IA controls. May include associated supporting background material, sample results, or links to automated testing tools.

E2.62. Validator. Entity responsible for conducting a validation procedure.

E2.63. Web Services. Self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of Web services support messaging, service descriptions, registries, and loosely coupled interoperability.

E3. ENCLOSURE 3

THE DIACAP PACKAGE

E3.1. The DIACAP package is developed through DIACAP activity and maintained throughout a system’s life cycle. Implementing the activities of the DIACAP generates the results listed in the “Comprehensive Package” column of Table E3.T1. The “Executive Package” column lists the minimum information necessary for an accreditation decision. Note that Table E3.T1. is not meant to describe a single fixed document format. Each DAA will determine what information is necessary to make an accreditation decision.

Table E3.T1. DIACAP Package Contents

| Comprehensive Package | Executive Package |
|---|--|
| System Identification Profile (SIP) | SIP |
| DIACAP Implementation Plan (DIP) <ul style="list-style-type: none"> • IA controls – inherited and implemented • Implementation status • Responsible entities • Resources • Estimated completion date for each IA control | |
| Supporting Certification Documentation <ul style="list-style-type: none"> • Actual validation results • Artifacts associated with implementation of IA controls • Other | |
| DIACAP Scorecard <ul style="list-style-type: none"> • Certification determination • Accreditation decision | DIACAP Scorecard <ul style="list-style-type: none"> • Certification determination • Accreditation decision |
| IT Security POA&M (If required) | IT Security POA&M (If required) |

E3.2. The SIP is compiled during the DIACAP registration and maintained throughout the system life cycle. An overview of the SIP is provided in Attachment 1 to Enclosure 3.

E3.3. The DIACAP Scorecard is a summary report that conveys information on the IA posture of a DoD IS succinctly in a format that can be exchanged electronically. A notional scorecard is provided in Attachment 2 to Enclosure 3. Additional data elements may be specified by CIOs, DAAs, or other enterprise users of the DIACAP Scorecard.

E3.4. An IT Security POA&M is required for any accreditation decision that requires corrective action and is also used to document NC or NA IA controls that have been accepted by the responsible DAA. The IT Security POA&M addresses:

E3.4.1. Why the system needs to operate.

E3.4.2. Any operational restrictions imposed to lessen the risk during an interim authorization.

E3.4.3. The DAA's rationale for accepting certain IA controls that are categorized as NC or NA.

E3.4.4. Specific corrective actions necessary to ensure that assigned IA controls have been implemented correctly and are effective.

E3.4.5. The agreed-upon timeline for completing and validating corrective actions.

E3.4.6. The resources necessary and available to properly complete the corrective actions. Attachment 3 to Enclosure 4 provides instructions for understanding and developing an IT Security POA&M.

Attachments – 3

- E3.A1. System Identification Profile
- E3.A2. Notional DIACAP Scorecard
- E3.A3. IT Security POA&M Instructions

E3.A1. ATTACHMENT 1 TO ENCLOSURE 3SYSTEM IDENTIFICATION PROFILE

E3.A1.1. The SIP identifies the data requirements for registering an IS with the governing DoD Component IA program. Information requirements for the SIP are described in Table E3.A1.T1.

Table E3.A1.T1. System Identification Profile

| ID | Data Element Descriptor | Example, Acceptable Values or Comment | Required/Conditional¹ |
|-----------|------------------------------------|---|---|
| 1 | System Identification | The System Identification Number or Code used by the DoD Component to uniquely identify the system. | Required/System Generated |
| 2 | System Owner | List the element or organization within the DoD Component that owns, controls, or manages the IS. | Required |
| 3 | Governing DoD Component IA Program | List the DoD Component that owns the IS. | Required |
| 4 | System Name | Provide the full descriptive name, e.g., Agency Billing System. | Required |
| 5 | Acronym | Provide a shortened or commonly used name or abbreviation (upper case) for this entry (e.g., ABS). | Required |
| 6 | System Version or Release Number | List the version or release number for the IS (e.g., 1.0). | Required |
| 7 | System Description | Provide a narrative description of the system, its function, and uses. Indicate if the system is stand-alone. | Required |
| 8 | DIACAP Activity | Identify the current DIACAP Activity: <ol style="list-style-type: none"> 1. Initiate and plan IA C&A 2. Implement and validate assigned IA controls 3. Make certification determination and accreditation decision 4. Maintain ATO and conduct reviews 5. Decommission | Required |

Table E3.A1.T1. System Identification Profile, (cont'd)

| ID | Data Element Descriptor | Example, Acceptable Values or Comment | Required/Conditional ¹ |
|----|---------------------------------------|---|-----------------------------------|
| 9 | System Life Cycle Phase | Identify the current life-cycle phase of the information system: <ol style="list-style-type: none"> 1. Concept Refinement 2. Technology Development 3. System Development and Demonstration 4. Production and Deployment 5. Operations and Support 6. Disposal or Decommissioning | Required |
| 10 | System Acquisition Phase | For programs of record, identify the current System Acquisition Phase: <ol style="list-style-type: none"> 1. Pre-Milestone A (Concept Refinement) 2. Post-Milestone A (Technology Development) 3. Post-Milestone B (System Development and Demonstration) 4. Post-Milestone C (Production and Deployment) 5. Post-Full Rate Production/Deployment Decision (FRPD/FRDD) | Conditional |
| 11 | IA Record Type | Identify the type of DoD information system (i.e., AIS Application, Enclave*, Outsourced IT-Based Process** or Platform IT Interconnection). *Indicate if stand-alone or DMZ. ** Indicate if DoD-controlled or control shared with service provider. | Required |
| 12 | Mission Criticality | Identify the mission criticality of this system (i.e., mission critical (MC), mission essential (ME), or mission support (MS) if neither MC or ME. (Reference (1)). | Required |
| 13 | Accreditation Vehicle | Identify the C&A process that was or is being used to C&A the IS (e.g., DIACAP, DCID 6/3, NIST 800-37). | Required |
| 14 | Additional Accreditation Requirements | Identify any additional accreditation requirements beyond the IA C&A process (e.g., privacy, special access requirements (SAR), cross security domain solutions, Non Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or GIG CAP identifier, ports, protocols, and services management.) | Conditional |

Table E3.A1.T1. System Identification Profile, (cont'd)

| ID | Data Element Descriptor | Example, Acceptable Values or Comment | Required/ Conditional¹ |
|-----------|--|---|--|
| 15 | ACAT Category | Identify the acquisition category if applicable according to Reference (1) (e.g., ACAT I). | Conditional |
| 16 | Governing Mission Area | Enterprise Information Environment MA (EIEMA), Business MA (BMA), Warfighting MA (WMA), or Defense Intelligence MA (DIMA) | Required |
| 17 | Software Category | Identify whether the system software is commercial off-the-shelf (COTS) or Government off-the-shelf (GOTS). | Required |
| 18 | MAC Level | List the information system's MAC level (i.e., MAC I, MAC II, or MAC III). | Required |
| 19 | Confidentiality Level | List the information system's CL (i.e., public, sensitive, or classified). | Required |
| 20 | Accreditation Status | Identify the accreditation status of the IS (i.e., unaccredited, ATO, IATO, IATT, DATO). | Required (default is unaccredited) |
| 21 | Certification Date | List the date the IS was certified by the CA. | Conditional |
| 22 | Accreditation Documentation | Are there documentation and artifacts that support the accreditation status? Answer Yes or No. | Conditional |
| 23 | Accreditation Date | List the date of the current accreditation decision (ATO, IATO, IATT, DATO). If the IS has no accreditation determination, enter "NONE" and the projected accreditation date. | Required |
| 24 | Authorization Termination Date | List the date that the current accreditation (ATO, IATO, IATT) is set to expire. | Conditional |
| 25 | DIACAP Team Roles, Member Names, and Contact Information | Identify the DIACAP Team (e.g., DAA, the CA, the DoD IS PM or SM, the DoD IS IAM, IAO, and UR). | Required |

Table E3.A1.T1. System Identification Profile, (cont'd)

| ID | Data Element Descriptor | Example, Acceptable Values or Comment | Required/ Conditional¹ |
|-----------|---|--|--|
| 26 | Privacy Impact Assessment Required | Indicate whether a privacy impact assessment is required for a new or previously existing IT system. Reference DoD 5400.11-R (Reference (y)). Answer Yes or No. | Required |
| 27 | Privacy Act System of Records Notice Required | Indicate whether a Privacy Act System of Record Notice is required by Reference (y). Answer Yes or No. | Required |
| 28 | E-Authentication Risk Assessment Required | Indicate whether an E-Authentication Risk Assessment has been performed for the system according to OMB M-04-04 (Reference (z)). Answer Yes or No. | Required |
| 29 | Date of Annual Security Review | List the date of the last annual security review for systems with an ATO. Required by Reference (a) and by the DIACAP for ISs with an ATO in effect for more than 1 year. | Required |
| 30 | System Operation | Identify whether the system operation is: <ol style="list-style-type: none"> 1. Government (DoD) Owned, Government Operated (GOGO) 2. Government (DoD) Owned, Contractor Operated (GOCO) 3. Contractor Owned, Contractor Operated (COCO) – includes outsourced IT services 4. Contractor Owned, Government (DoD) Operated (COGO) 5. Non-DoD – includes Federal, State, and local governments, grantees, industry partners, etc. | Required |
| 31 | Contingency Plan Required | Indicate whether a contingency plan addressing disruptions in operations of the IS is in place. Answer Yes or No. | Required |
| 32 | Contingency Plan Tested | Indicate whether the contingency plan that is in place has been tested. Answer Yes or No. | Required |

¹ Required entries are mandatory for completing the SIP. Conditional entries must be completed if they apply to the system being profiled. If the entry does not apply, the box is left blank.

E3.A2. ATTACHMENT 2 TO ENCLOSURE 3

DIACAP SCORECARD

E3.A2.1. The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD PKI-certified digital signature. The DIACAP Scorecard contains a listing of all IA controls and their status of either C, NC, or NA. An example of a DIACAP Scorecard is shown in Figure E3.A2.F1. Table E3.A2.T1. explains the fields contained in Figure E3.A2.F1.

Figure E3.A2.F1. Example of a DIACAP Scorecard

DIACAP SCORECARD

| | | | | | |
|--|--|--|---|---|--|
| System Name Enterprise Mission Assurance Support Service | | System Owner ASD(NII) | | IS Type AIS Application | |
| Designated Accrediting Authority (DAA) Nathan Gray | | Accreditation Status ATO | Accreditation Date 23-Sep-05 | Period Covered ATD 23-Sep-07 | Last Update 24-Dec-05 |
| Certifying Authority (CA) Matthew Summers | | Certification Date 10-Sep-05 | Mission Assurance Category (MAC) MAC II | | Confidentiality Level (CL) Sensitive |

- MAC I, Classified
- MAC II, Classified
- MAC III, Classified
- MAC I, Sensitive
- MAC II, Sensitive
- MAC III, Sensitive
- MAC I, Public
- MAC II, Public
- MAC III, Public

| IA Control Subject Area | IA Control Number | IA Control Name | Inherited? | C/NC/NA | Impact Code | Last Update |
|-------------------------|-------------------|---|------------|---------|-------------|-------------|
| Continuity | COAS-2 | Alternate Site Designation | No | C | Medium | 02-Nov-05 |
| Continuity | COBR-1 | Protection of Backup and Restoration Assets | No | C | High | 02-Nov-05 |
| Continuity | CODB-2 | Data Back-up Procedures | Yes | C | Low | 30-Sep-05 |
| Continuity | CODP-2 | Disaster and Recovery Planning | No | NC | Medium | 08-Nov-05 |
| Continuity | COEB-1 | Enclave Boundary Defense | Yes | C | High | 02-Nov-05 |
| Continuity | COED-1 | Scheduled Exercises and Drills | No | C | Medium | 24-Dec-05 |

Table E3.A2.T1. Scorecard Instructions

| Reference | Description |
|--------------|--|
| System Name | The name of the system being certified. |
| System Owner | The organization within the DoD Component that owns, controls, or manages the IS. |
| IS Type | The IS type (i.e., AIS application, enclave, outsourced IT-based process, and platform IT interconnection). Indicate if the enclave is stand-alone or a DMZ. |
| DAA | The name and signature of the DAA for the system. Manual or DoD PKI-certified digital signatures are acceptable. |

Table E3.A2.T1. Scorecard Instructions, (cont'd)

| Reference | Description |
|-------------------------|--|
| Accreditation Status | The accreditation decision for the system (i.e., unaccredited, ATO, IATO, IATT, DATO). |
| Period Covered | Includes the date of the accreditation (if the system has a decision other than unaccredited), and the ATD. |
| Last Update | The date of the last change that occurred on the scorecard. This is primarily driven by updates to the IA controls and their associated status. |
| CA | The name of the individual serving as the CA for the system. |
| Certification Date | The date of the certification. |
| MAC | The MAC applied to the system. |
| CL | The CL applied to the system. |
| IA Control Subject Area | The subject area associated with the IA control. |
| IA Control Number | The reference number associated with the IA control. |
| IA Control Name | The name associated with the IA control. |
| Inherited | An indication (Yes or No) of whether or not the IA control is inherited. |
| C/NC/NA | An indication of the compliance status of the IA control (i.e., C, NC, NA). An IT Security POA&M is required if NC or NA. Note: NC may indicate either non-implementation or complete failure of the control under testing; it also may indicate a partial failure of a control under testing (e.g., three of four testing points pass). |
| Impact Code | The impact code associated with the IA control. |
| Last Update | The date of the last change of the IA control's compliance status (C/NC/NA). |

E3.A3. ATTACHMENT 3 TO ENCLOSURE 3

IT SECURITY POA&M INSTRUCTIONS

E3.A3.1. The primary purpose of an IT Security POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities. OMB requires agencies to prepare IT Security POA&Ms for all programs and systems in which an IT security weakness has been found. OMB guidance (Reference (aa)) directs CIOs and the DoD Component program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (for program officials this includes all systems that support their operations and assets, including those operated by contractors). In addition, program officials are required to update the agency CIO on their progress on at least a quarterly basis and at the direction of the CIO. This enables the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB. Under the DIACAP, the IT Security POA&M is also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable because of the nature of the system (e.g., stand-alone systems).

E3.A3.2. The IT Security POA&M is designed to be a management tool to assist: agencies in closing their security performance gaps; IGs in their evaluation work of agency security performance; and OMB with oversight responsibilities. The Department of Defense is responsible for maintaining the confidentiality of IT Security POA&Ms because they may contain pre-decisional budget information. There are three types of IT Security POA&Ms, as reflected in Table E4.A3.T1. DoD IT Security POA&Ms shall:

E3.A3.2.1. Be tied to the agency's budget submission when required through the project identifier(s) of the system. This links the security costs with security performance. OMB Circular No. A-11 (Reference (ab)) requires that agencies develop and submit to OMB business cases (Exhibits 300) for major IT investments. Additionally, each agency submits an Exhibit 53, a list of both major and non-major IT investments. The agency assigns project identifier(s) to each investment and includes it with these exhibits.

E3.A3.2.2. Address all IT security weaknesses, including but not limited to those found during GAO audits, financial system audits, official security tests and evaluations or compliance reviews, and critical infrastructure vulnerability assessments.

E3.A3.2.3. Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

E3.A3.2.4. Follow the format detailed below that is consistent with the examples provided by OMB.

E3.A3.2.5. Be submitted to the DoD SIAO when directed.

Table E3.A3.T1. Types of DoD IT Security POA&Ms

| Report | Responsibility | Submit To | Dates Due |
|--|-------------------|--|--|
| System-level IT Security POA&Ms (Table E4.A3.T2) | PMs/IAMs | DoD Component CIO (Also to DoD SIAO for all systems with a CAT I weakness or on the OMB Watch List (Exhibit 300s) for security) | 1 Dec, 1 Mar, 1 Jun, 1 Sep |
| DoD Component-level IT Security POA&M (Table E4.A3.T3) | DoD Component CIO | ASD(NII)/DoD CIO | Due with the DoD Component's annual FISMA report and as directed |
| DoD Enterprise IT Security POA&M | ASD(NII)/DoD CIO | OMB | As directed |

E3.A3.3. The subparagraphs below describe the System Level IT Security POA&M.

E3.A3.3.1. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA, the SIAO, and the governing DoD Component CIO.

E3.A3.3.2. Table E3.A3.T2. is an example of a completed system-level IT Security POA&M, illustrating the appropriate level of detail required. Included in the heading of the system-level IT Security POA&M template is a field for OMB Project ID and Security Costs, which must be filled in from Exhibits 300 and 53, where applicable.

E3.A3.3.3. Once an initial system-level IT Security POA&M weakness has been opened, changes cannot be made to the data in columns 1 (“Weakness”), 6 (“Scheduled Completion Date”), 7 (“Milestones with Completion Dates”), and 9 (“Source Identifying Weakness”).

E3.A3.3.4. IT Security POA&Ms listing CAT I or CAT II weaknesses shall be assessed for classification. For instance, the fact that a MAC I or MAC II IS has a CAT I weakness that has not been mitigated to a degree that will preclude immediate unauthorized access dictates a minimum classification of CONFIDENTIAL. Other factors that would influence a classification decision include the number of CAT II weaknesses identified for a single system and whether the system itself is classified. At a minimum an IT Security POA&M will be protected as Sensitive. Classified IT Security POA&Ms for unclassified systems must be maintained in an appropriate environment separate from the unclassified DIACAP Package.

E3.A3.4. The following sections explain how to complete the system-level IT Security POA&M fields. Note: NA IA controls will have entries only in columns 1, 3, and 11.

E3.A3.4.1. Column 1: Type of Security Weakness. Describe security weaknesses identified during certification or by the annual program review, independent evaluations by IGs, or any other work done by or on behalf of the program office or the DoD Component. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. When it is necessary to provide more sensitive data, the IT Security POA&M should note the fact of its special sensitivity and it should be protected accordingly. When more than one weakness has been identified, number each individual security weakness as shown in the examples. Indicate “NA” in this column as required.

E3.A3.4.2. Column 2: CAT (Severity Category). Category assigned to a system IA security weakness by a CA as part of certification analysis to indicate the risk level associated with the IA security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as CAT I, CAT II, or CAT III, with CAT I indicating the greatest risk and urgency.

E3.A3.4.3. Column 3: IA Control and Impact Code. An IA control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA control are assignable and thus accountable. IA controls are assigned according to MAC (for integrity and availability) and CL in accordance with Reference (d). Impact codes indicate the consequences of a non-compliant IA control and are expressed as high, medium, or low, with high indicating the greatest impact.

E3.A3.4.4. Column 4: Point of Contact (POC). Identity the office or organization that the DoD Component will hold responsible for resolving the security weakness.

E3.A3.4.5. Column 5: Resources Required. Estimated funding or manpower (i.e., full-time equivalents) resources required to resolve the security weakness. Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.6. Column 6: Scheduled Completion Date. Scheduled completion date for resolving the security weakness. Please note that the initial date entered should not be changed. If a security weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in column 10 (“Status”). Enter “NA” if risk is accepted for a satisfactorily mitigated CAT II or a CAT III weakness.

E3.A3.4.7. Column 7: Milestones with Completion Dates. A milestone will identify specific requirements for correcting an identified weakness. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones, the agency should note them in column 8 (“Milestone Changes”). Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.8. Column 8: Milestone Changes. This column includes changes to completion dates and reasons for the changes. Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.9. Column 9: Source Identifying the Weakness. Identify the source (e.g., program review, test and evaluation program findings, IG DoD audit, GAO audit) of the security weakness.

E3.A3.4.10. Column 10: Status. The DoD Component should use one of the following terms to report status of corrective actions: ongoing, completed, or risk accepted for a CAT II or CAT III weakness that has been accepted by the DAA. “Completed” should be used only when a security weakness has been fully resolved and the corrective action has been tested. Include the date of completion or risk acceptance for a CAT III weakness. Enter “Risk Accepted by DAA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.11. Column 11: Comments. If the IA control is inherited, cite the originating IS. For NA IA controls, provide the reason the control is not applicable. Additional information may include anticipated source of funding and other obstacles and challenges to resolving the security weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system).

Table E3.A3.T2. System-Level IT Security POA&M Example

| System Level IT Security POA&M Example | | | | | | | | | | | |
|--|------------------|---------------------------------------|----------------|-------------------------------|--|--|---|---|------------------------------|--------------------------------------|--|
| Date Initiated: | October 1, 2005 | | | IS Type: | Enclave | | | OMB Project ID: | 009-222334-55874 | | |
| Date Last Updated: | January 10, 2006 | | | <i>(See Note 1)</i> | | | | <i>(See Note 2)</i> | | | |
| Component Name | OSD | | | POC Name: | James Avery | | | | | | |
| System / Project Name: | DoD Network | | | POC Phone: | 703-698-7753 | | | Security Costs: | <i>(See Note 3)</i> \$62,500 | | |
| DoD IT Registration No: | 86753 | | | POC E-Mail: | james.avery@dod.ctr.mil | | | | | | |
| Weakness (1) <i>(See Note 4)</i> | CAT (2) | IA Control and Impact Code (3) | POC (4) | Resources Required (5) | Scheduled Completion Date (6) | Milestones with Completion Dates (7) | Milestone Changes (8) | Source Identifying Weakness (9) | Status (10) | Comments (11) | |
| 1 An account management process has not been implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. | I | IAAC-1 Impact High | IAO | \$50,000 | 5/30/2005 | Develop an account Management Process - 1/15/2005; Management Review of account management process 3/15/2005; Implement/Test account management process - 4/15/2005 | Implementing and Testing the account management process delayed till 10/15/2005 due to inadequate funding | 8500.2 IA Controls Test Conducted 5/15/2005 | Ongoing | Funding will be available in FY 2006 | |
| 2 Security plan is out of date, more than one year since last update despite new interconnections | II | DCSD-1 Impact High | IAO | \$5,000 | 11/30/2005 | Update plan and obtain independent review - 11/30/2005 | | 8500.2 IA Controls Test Conducted 5/15/2005 | Ongoing | | |
| 3 Lack of accurate systems hardware and software baseline hampers implementation of Configuration Management processes. | II | DCHW-1/DCSW-1 Impact High | IAO | \$0 | 8/31/2005 | Establish baseline inventory of the hardware and software and utilize revision control system - 6/15/2005. Implement a software revision control program - 8/31/2005 | | Security Test and Evaluation - 4/15/2005 | Completed - 10/30/2005 | | |
| 4 Encryption is not certified FIPS 140-2 compliant. | III | DCNR-1 Impact Medium | IAO | \$5,000 | 10/21/2005 | Upgrade encryption software to FIPS 140-2 certified version 10/21/2005 | | IG Audit 3/21/2005 | Ongoing | May slip due to delay in funding | |
| 5 | | | | | | | | | | | |
| 6 | | | | | | | | | | | |
| 7 | | | | | | | | | | | |
| 8 | | | | | | | | | | | |
| 9 | | | | | | | | | | | |
| 10 | | | | | | | | | | | |
| 11 | | | | | | | | | | | |

- Note 1 – Indicate if the enclave is stand-alone or a DMZ.
- Note 2 – Cite project identifier(s) from OMB Exhibit 300, if applicable.
- Note 3 – Security costs from OMB Exhibit 53, if applicable.
- Note 4 – NA IA controls will have entries only in columns 1, 3, and 11.

E3.A3.5. The subparagraphs below describe the DoD Component-Level IT Security POA&M.

E3.A3.5.1. DoD Components are required to complete and submit a DoD Component-level IT Security POA&M as indicated in Table E3.A3.T1. A DoD Component-level IT Security POA&M is required for the following:

E3.A3.5.1.1. Systemic weaknesses (significant IA security weaknesses) identified across the DoD Component.

E3.A3.5.1.2. Systemic weaknesses (significant IA security weaknesses) identified by GAO and IG DoD audits and reviews.

E3.A3.5.2. Table E3.A3.T3. contains an example of a completed DoD Component-level IT Security POA&M, illustrating the appropriate level of detail required. Once a DoD Component has completed the initial DoD Component-level IT Security POA&M, no changes should be made to the data in columns 1 (“Weakness”), 4 (“Scheduled Completion Date”), 6 (“Milestones with Completion Dates”), and 8 (“Identified in GAO Audit or Other Review”).

E3.A3.5.3. Refer to the instructions for the system-level IT Security POA&M in section E3.A3.4. for guidance in filling out applicable items on the DoD Component-level POA&M.

Table E3.A3.T3. The DoD Component-Level IT Security POA&M Example

| Component Level IT Security POA&M Example | | | | | | | |
|--|---------------|------------------------|-------------------------------|---|-----------------------|--|------------|
| Date: | | March 1, 2005 | | POC Name: | | Mr. Navy CIO | |
| Component Name: | | DON | | POC Phone: | | 555-555-5555 | |
| | | | | POC E-mail: | | doncio@nav.mil | |
| Weakness (1) | POC (2) | Resources Required (3) | Scheduled Completion Date (4) | Milestones with Completion Dates (5) | Milestone Changes (6) | Source Identifying Weakness (7) | Status (8) |
| 1 Annual testing of contingency plans not being conducted | Component CIO | 700K | 3/1/2006 | Verify and test contingency plans for 98% of systems C&A 12/30/05 | | Annual Review | Ongoing |
| 2 Security Awareness, Training, and Education – no process for tracking completion of specialized training | Component CIO | 200K | 10/1/2005 | Implement and test training database 6/1/05 Enter personnel requiring specialized training into database 10/1/05 | | OIG Audit | Ongoing |
| 3 Inconsistent and inadequate personal computer inventory afloat | Component CIO | 500K | 10/1/2006 | Implement and test afloat computer inventory system 10/1/05 Enter 50% afloat inventory into database 3/1/06 | | Naval Audit Service | Ongoing |

E3.A3.6. The subparagraphs below describe the DoD Enterprise-Level IT Security POA&M.

E3.A3.6.1. The DoD CIO is responsible for completing and submitting a DoD Enterprise-level IT Security POA&M as indicated in Table E3.A3.T1.

E3.A3.6.2. Systemic IA security weaknesses reported on the DoD Enterprise-level IT Security POA&M are derived from the DoD Component-level IT Security POA&Ms, GAO and IG DoD audits, and other reviews and events.

E4. ENCLOSURE 4

DIACAP KNOWLEDGE SERVICE (KS)¹ OVERVIEW

E4.1. DoD IA practitioners and developers need ready access to current DIACAP implementation guidance in order to uniformly apply the methods, standards, and practices required to successfully certify and accredit the DoD ISs comprising the GIG. Because the GIG is an ever-changing entity, DoD IA practitioners tasked with GIG certification and accreditation responsibilities require implementation guidance, access, and content suitable to accomplishing C&A in this dynamic DoD-wide environment. Implementation guidance must reflect the most up-to-date DoD intent regarding evolving IA security objectives and risk conditions. Written manuals that must be formally and laboriously coordinated lack the timeliness and versatility required to adequately meet the access, distribution, and relevancy challenges posed. To address this enterprise challenge, the DIACAP KS, developed and owned by the Department of Defense, has been established as the on-line, Web-based resource that provides requirements, guidance, and tools for implementing and executing the DIACAP. The KS is available to all individuals with C&A responsibilities, provides convenient access to Reference (d) IA controls and required standardized IA control implementation and validation procedures, and assists members of the IA community in fulfilling the requirements of the DIACAP. It is accessible by individuals with a DoD PKI certificate (Common Access Card (CAC)), or External Certification Authority (ECA) certificate in conjunction with DoD sponsorship (e.g., for DoD contractors without a CAC and working off-site). The KS is the DoD official resource for implementing and executing the DIACAP.

E4.2. The purpose of the DIACAP KS is to provide IA practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in DIACAP. The DIACAP KS supports both automated and non-automated implementation of the DIACAP.

E4.3. The KS is a library of tools, diagrams, process maps, documents, etc., to support and aid in the execution of the DIACAP. It is a collaboration workspace for the DIACAP user community to develop, share, and post lessons learned and best practices and a source for IA news and events and other IA-related information resources.

E4.4. The DIACAP TAG is responsible for maintaining CCM of the online KS content. The TAG:

E4.4.1. Provides detailed analysis and authoring support for the enterprise portion of the DIACAP KS content.

¹ <https://diacap.iaportal.navy.mil/>

E4.4.2. Provides configuration control for DIACAP-related enterprise services, including DIACAP KS functionality.

E4.4.3. Interfaces with the DoD Component IA programs, GIG MAs, IA COIs, and specialized entities within the IA domain governance structure. (See Figure F1.)

E4.4.4. Addresses issues that are common across entities and recommends changes to the baseline IA controls and C&A process.

E5. ENCLOSURE 5

DIACAP TRANSITION TIMELINE AND INSTRUCTIONS

E5.1. The DIACAP Transition Timeline and Instructions provide guidance and direction for all systems transitioning to DIACAP from the DITSCAP environment.

Table E5.T1. DIACAP Transition Timeline and Instructions

| DoD IS C&A STATUS | | TRANSITION TIMELINE and INSTRUCTIONS |
|------------------------------|---|--|
| 1 | Unaccredited new start or operational DoD IS (No DITSCAP activity). | Initiate DIACAP. |
| 2 | DoD IS has initiated DITSCAP, but does not yet have a signed Phase One System Security Authorization Agreement (SSAA). | Transition to DIACAP immediately. |
| 3 | DoD IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA Requirements Traceability Matrix (RTM) incorporates all DoD baseline IA controls as specified in Reference (d). | Continue under DITSCAP. The DITSCAP SSAA section addressing re-accreditation requirements (section 5.7 in the SSAA outline of Reference (e)) should have been modified as directed by Reference (g) to identify the governing DoD Component IA program and describe the system’s strategy and schedule for transitioning to DIACAP, satisfying the DIACAP Annual Review and meeting the reporting requirements of FISMA (Reference (a)). The schedule for transitioning from DITSCAP to DIACAP shall not exceed the system re-accreditation timeline. |
| 4 | DoD IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA RTM does not incorporate all DoD baseline IA controls as specified in Reference (d). | Comply with guidance at #3 above and continue under DITSCAP. The DITSCAP RTM to incorporate all DoD baseline IA controls as specified in Reference (d) and a plan for implementing them should have been modified as directed by Reference (g). IA controls implementation timelines |

Table E5.T1. DIACAP Transition Timeline and Instructions, (cont'd)

| DoD IS C&A STATUS | | TRANSITION TIMELINE and INSTRUCTIONS |
|------------------------------|---|---|
| | | may extend beyond the DITSCAP accreditation decision, that is, the DITSCAP accreditation decision is not contingent upon full compliance with the baseline IA controls, but the system must provide information/visibility of its compliance status and have a viable plan for achieving compliance in order to be granted an accreditation decision under DITSCAP. |
| 5 | DoD IS has a DITSCAP accreditation decision that is current within 3 years. | <p>A strategy and schedule for transitioning to DIACAP, achieving compliance with Reference (d) baseline IA controls, satisfying the DIACAP Annual Review, and meeting the reporting requirements of Reference (a) should be completed as directed by Reference (g).</p> <p>If the DITSCAP RTM does not incorporate the baseline DoD IA controls as specified in Reference (d), the DoD IS shall provide the DAA with an assessment of compliance.</p> <p>If the accreditation decision is IATO and the system is on a path toward full authorization, continue under DITSCAP as modified by the guidelines of this table to achieve authorization.</p> |
| 6 | DoD IS has a DITSCAP ATO that is more than 3 years old. | Initiate DIACAP. |