Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance

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

References: (a) Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA)[1]
(b) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, (hereby canceled)
(e) through (bb), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Establishes the DoD information assurance (IA) certification and accreditation (C&A) process for authorizing the operation of DoD information systems consistent with the Federal Information Security Management Act (FISMA) (reference (a)), DoD Directive (DoDD) 8500.1 (reference (b)), and DoD Directive 8100.1 (reference(c)).

1.2. Supersedes DoD Instruction (DoDI) 5200.40 and DoD 8510.1-M, (references (d) and (e)).

1.3. Supports net-centricity [2] through an effective and dynamic IA C&A process.

1.4. Provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services (CES) and web services-enabled software systems and applications.

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 Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

[1] Available at http://iase.disa.mil/policy.html#PublicLaw
[2] See for example the *Department of Defense Net-Centric Data Strategy*, prepared by the DoD Chief Information Officer (CIO), (May 9, 2003).

organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Component(s)").

2.1.2. All DoD-owned or controlled information systems that receive, process, store, display or transmit DoD information, throughout the entire system life cycle (SLC) and regardless of classification or sensitivity, including but not limited to:

2.1.2.1. DoD information systems that support special environments, e.g., Special Access Requirements (SAR), as supplemented by the special needs of the program.

2.1.2.2. Information systems under contract to the Department of Defense.

2.1.2.3. Information systems of Non-appropriated Fund Instrumentalities.

2.1.2.4. Stand-alone information systems.

2.1.2.5. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

2.1.2.6. DoD information systems that are Prototypes or Advanced Concept Technology Demonstrations (ACTDs).

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

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

4. POLICY

This Instruction implements the policies established in DoDD 8500.1 (reference (b)) and described in DoDI 8500.2 (reference (g)). It is DoD policy that:

4.1. The Department of Defense shall certify and accredit information systems through an enterprise process for identifying, implementing, and managing IA capabilities and services. Information assurance capabilities and services shall be expressed as IA Controls as defined by DoDI 8500.2 (reference (g)) and maintained through a DoD-wide Configuration Control and Management (CCM) process that considers the Global Information Grid (GIG) architecture and risk assessments that are conducted at the Department, Mission Area (MA), DoD Component level, and information system (IS) level consistent with FISMA (reference (a)).

4.2. The Department of Defense shall establish and use an enterprise decision structure for IA certification and accreditation that includes and integrates GIG Mission Area (MA) Principal Accrediting Authorities (PAA) DoDD 8115.01 (reference (h)), the DoD IA Program (reference (g)), and a DIACAP CCM process.

4.3. The DIACAP shall support the transition of DoD information systems to GIG standards and a net-centric environment while enabling assured information sharing by: (1) providing a standard C&A approach; (2) managing and disseminating enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting; (3) accommodating diverse information systems; and (4) facilitating a dynamic environment.

4.4. All DoD-owned or -controlled information systems, to include outsourced Information Technology (IT)-based processes and platform IT interconnections, shall be under the governance of a DoD Component IA Program. The DoD Component IA Program shall be the primary mechanism for ensuring enterprise visibility and synchronization of the DIACAP.

4.5. All DoD information systems shall implement the baseline DoD IA Controls. The baseline DoD IA Controls address enterprise-wide threats and vulnerabilities and are augmented if required to address localized threats or vulnerabilities. The DIACAP Scorecard reflecting the results of the implementation of the required IA baseline controls is to be made visible at the DoD enterprise level, and additional IA controls that may have been required by the DoD Component or local information system are to be made visible to the DoD and Component CIO.

4.6. The C&A status of all DoD information systems shall be made available to support Designated Accrediting Authority (DAA) accreditation decisions.

4.7. Formal threat assessments at the individual DoD information system level are not required by DoDI 8500.2 (reference (g)), but may be required by other policy.

4.8. All DoD information systems with an Authorization to Operate (ATO) shall conduct reviews at least annually to validate the correct implementation of assigned IA Controls.

4.9. Resources for implementing the DIACAP shall be identified and allocated as part of the Defense Planning, Programming, Budgeting and Execution (PPBE) process.

4.10. Provisions for implementing the DIACAP shall be written into contracts of systems, services, and programs that are required to comply with the DIACAP. Failure to meet this requirement shall not be used as justification for DIACAP non-compliance.

5. RESPONSIBILITIES

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

5.1.1. Oversee implementation of this Instruction, promulgate DIACAP information standards and sharing requirements, and manage the transition from the previous DoD C&A process, DoDI 5200.40 (reference (d)), 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 FISMA (reference (a)) and based upon objective criteria outlined in Enclosure 3 of DoDI 8500.2 (reference (g)).

5.1.3. Appoint a Principal Accrediting Authority for DoD information systems governed by the Enterprise Information Environment Mission Area (EIEMA).

5.1.4. Appoint a DoD Senior Information Assurance Officer (SIAO) corresponding to a senior agency information security officer in FISMA (reference (a)) to direct and coordinate the DoD IA Program DoDI 8500.2 (reference (g)) and:

5.1.4.1. Ensure DoD information systems are assigned to and governed by a DoD Component IA Program.

5.1.4.2. Advise, inform and support the GIG PAAs and their Representatives.

5.1.4.3. Establish and maintain a DIACAP configuration control and management process, DIACAP Technical Advisory Group (TAG) and online DIACAP Knowledge Service (KS).

5.1.4.4. Conduct reviews of the certification determinations for DoD information systems requiring Office of the Secretary of Defense-level oversight (e.g., Acquisition Category (ACAT) ACAT I and ACAT IA programs DoDD 5000.1 (reference (i)).

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

5.2.1. Appoint a Principal Accrediting Authority for the Business Mission Area (BMA) for DoD information systems governed by the BMA.

5.2.2. Participate in the DIACAP TAG to ensure that the DIACAP and execution of responsibilities, as established by DoDD 5000.1 and DoDI 5000.2 (references (i) and(j)), are mutually supportive.

5.3. The Under Secretary of Defense for Intelligence shall appoint a Principal Accrediting Authority for all DoD information systems governed by the Defense Portion of the Intelligence Mission Area (DIMA).

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

5.4.1. Appoint a Principal Accrediting Authority for the Warfighting Mission Area (WMA) for DoD information systems governed by the WMA.

5.4.2. Ensure the Joint Capabilities Identification and Development System (JCIDS) CJCSI 3170.01D (reference (k)) requires DIACAP planning consistent with this Instruction.

5.5. The Director, Defense Information Systems Agency (DISA) shall:

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

5.5.2. Develop and provide DIACAP training and awareness products, and a distributive training capability to support the DoD Components according to DoDD 8500.1 (reference (b)) and DoDD 8570.1 (reference (l)) and post the training materials on the Information Assurance Support Environment (IASE) website (http://iase.disa.mil/).

5.6. The Director, National Security Agency (NSA) shall:

5.6.1. Develop the IA Component of the GIG Architecture and publish supporting implementation material in the DIACAP Knowledge Service.

5.6.2. Engage the GIG IA capability and 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.

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

5.7. The Heads of the DoD Components shall:

5.7.1. Ensure DoD information systems under their purview comply with the DIACAP.

5.7.2. Not operate unaccredited information systems (i.e., systems without a current ATO, IATO, or IATT).

5.7.3. Enforce accreditation decisions, including Denial of Authorization to Operate (DATO).

5.7.4. Support the annual assessment of DoD Component IA Programs as required by FISMA (reference (a)).

5.7.5. Consistent with PAA guidelines and authorities, appoint DAAs for DoD information systems under their purview.

5.7.6. Provide training for personnel engaged in or supporting the DIACAP consistent with DoDD 8570.1 (reference (l)) and supporting issuances.

5.7.7. Ensure that User Representatives (UR) are appointed for assigned DoD information systems according to guidelines established by the GIG PAAs.

5.8. The Principal Accrediting Authorities (PAAs) shall:

5.8.1. Ensure GIG MA data management strategies and processes include information assurance.

5.8.2. Establish criteria and authorization processes for information exchange between MA information systems and non-MA information systems, to include those external to the Department of Defense.

5.8.3. Ensure accreditation guidelines and decisions are consistent across, and recognized throughout, all impacted GIG MAs through formal establishment of an accreditation decision structure for all information systems that includes:

5.8.3.1. Direct designation of accrediting authorities for PAA designated GIG MA information systems, as appropriate.

5.8.3.2. Delegation of accrediting authority, as appropriate, to the Heads of Components.

5.8.3.3. Establishment of criteria and processes for the appointment of User Representatives.

5.8.3.4. Establishment or realignment of GIG MA or GIG-wide C&A review, support, or advisory bodies as required and integration with the DIACAP CCM.

5.8.4. Ensure the accreditation decision structure addresses special access and stand-alone information systems.

5.8.5. Identify a PAA Representative to the DoD SIAO for planning and coordination.

5.9. The PAA Representatives shall:

5.9.1. Work together to ensure the alignment of DoD information systems to MAs is clear and comprehensive.

5.9.2. Provide MA-related guidance to the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) and the DIACAP TAG.

5.10. The Defense IA/Security Accreditation Working Group (DSAWG) shall:

5.10.1. Serve as a community forum for reviewing and resolving C&A decisions related to the sharing of IA/security risk.

5.10.2. Take direction from the PAA Representatives and guidance from the DoD SIAO.

5.10.3. Inform and advise affected PAAs and DAAs on C&A decisions, to include but not limited to the DISN DAAs.

5.10.4. Interact with the DIACAP TAG to examine C&A issues and improve DIACAP Knowledge Service content.

5.11. The DIACAP Technical Advisory Group (TAG) shall:

5.11.1. Be chaired by an appointee of the DoD SIAO and take direction from the DoD SIAO and guidance from the PAA Representatives and ensure DoD Component level participation in the TAG.

5.11.2. Include membership from or interaction with the DoD Component IA Programs, the GIG Mission Areas, IA-related Communities of Interest (COI), and specialized entities within the IA Domain governance structure, e.g., the GIG IA Architecture Office and the DSAWG.

5.11.3. Provide detailed analysis and authoring support for the enterprise portion of the DIACAP Knowledge Service.

5.11.4. Provide configuration control for DIACAP related enterprise services, to include DIACAP Knowledge Service functionality.

5.11.5. Examine C&A related issues that are common across GIG entities and recommend changes to the baseline IA Controls or C&A process.

5.11.6. Review proposed MA or DoD Component IA Control sets for compatibility with the baseline DoD IA Controls and with other established IA Control sets.

5.11.7. Advise the Information Assurance Senior Leadership Group (IASL) or other IA advisory forums as identified by the DoD SIAO to resolve C&A priorities and cross-cutting issues.

5.12. DoD Component Chief Information Officers (CIO) shall:

5.12.1. Appoint a DoD Component Senior Information Assurance Officer (SIAO) corresponding to FISMA (reference (a)) to direct and coordinate the DoD Component IA Program consistent with the strategy and direction of the DoD IA Program.

5.12.2. Ensure that implementation and validation of IA Controls through the DIACAP is incorporated as an element of DoD Component information system life cycle management processes.

5.12.3. Ensure that the DIACAP status of DoD Component information systems is visible to the DoD CIO/SIAO and PAAs.

5.12.4. Ensure collaboration and cooperation between the DoD Component IA Program and the PAA/DAA structure.

5.12.5. Ensure a program or system manager is identified for each DoD Component information system.

5.12.6. Establish and manage a DIACAP Plan of Actions and Milestones (POA&M) program

5.13. DoD Component Senior Information Assurance Officers (SIAOs) shall:

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

5.13.2. Track the DIACAP status of information systems that are governed by the DoD Component IA Program.

5.13.3. Ensure the IA Controls assigned to each information system governed by the DoD Component IA Program address the assurance of the enterprise information environment.

5.13.4. Establish and manage a coordinated IA certification process for information systems governed by the DoD Component IA Program. This includes but is not limited to:

5.13.4.1. Functioning as the Certifying Authority (CA) for all governed information systems.

5.13.4.2. Ensuring and overseeing a qualified certification cadre, e.g., validators, analysts, certifying authority representatives.

5.13.4.3. Formally delegating certifying authority as necessary.

5.13.4.4. Implementing deliberate methods to incorporate validation and certification needs and lessons learned in the DIACAP Knowledge Service.

5.13.5. Establish and enforce the C&A process, roles and responsibilities, and review and approval thresholds and milestones within the DoD Component IA Program.

5.13.6. Serve as the single IA coordination point for Joint or Defense Programs that are deploying information systems to DoD Component enclaves.

5.14. Designated Accrediting Authorities, in addition to the responsibilities established in DoDI 8500.2 (reference (g)), shall:

5.14.1. Comply with GIG MA PAA(s) direction.

5.14.2. Ensure each DoD information system complies with applicable DoD baseline IA Controls in order to interconnect with the GIG.

5.14.3. Ensure assigned systems have appropriate data management and sharing policies according to DoDI 8500.2 (reference (g)) and implement security requirements for classified and controlled unclassified information, including establishing security classification guides according to DoD Regulation 5200.1-R (reference (m)).

5.14.4. Ensure that appropriate access policies are established for all information being produced by the assigned information systems, and that the established roles and privileges are consistent with defined enterprise roles and privileges.

5.14.5. Authorize or deny testing or operation of assigned DoD information systems.

5.15. Program or System Managers (PM or SM) for DoD information systems shall:

5.15.1. Ensure that each assigned DoD information system has a designated Information Assurance Manager (IAM) with the support, authority and resources to satisfy the responsibilities established in DoDI 8500.2 (reference (g)) and this Instruction.

5.15.2. Implement the DIACAP for assigned DoD information systems.

5.15.3. Plan and budget for IA Controls implementation, validation and sustainment throughout the system life cycle, to include timely and effective configuration and vulnerability management.

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

5.15.5. Identify and implement software quality controls and validation methods for assigned DoD information system programs that develop or integrate software.

5.15.6. Enforce accreditation decisions for hosted or interconnected DoD information systems.

5.15.7. Develop, track, and resolve the DIACAP Implementation Plan for assigned DoD information systems.

5.16. DoD Information System User Representatives shall:

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

5.16.2. Support the IA Controls assignment and validation process to ensure user community needs are met.

5.16.3. Work with information owners and Communities of Interest to ensure that data management and sharing policies and any required security classification guidelines are developed.

5.17. Information Assurance Managers (IAM), in addition to the responsibilities established in DoDI 8500.2 (reference (g)), shall:

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

5.17.2. Advise and inform the governing DoD Component IA Program on DoD information C&A status and issues.

5.17.3. Comply with information and process requirements of the governing DoD Component IA Program.

5.17.4. Provide direction to the Information Assurance Officer (IAO) according to reference (g).

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

6. PROCEDURES

Enclosures 3 and 4 provide an overview of the DIACAP and the DIACAP Package. DIACAP implementation procedures and baseline guidance are provided in the DIACAP Knowledge Service, a web-based resource that provides guidance and assistance for implementation of the DIACAP. The Knowledge Service provides the DoDI 8500.2 IA Controls (reference (g)) as well as the required, standardized DoD IA Controls implementation procedures, validation procedures and expected results for each IA Control. For further information on the DIACAP Knowledge Service, see Enclosure 5.

7. EFFECTIVE DATE

This Instruction is effective immediately. Specific DoD information system transition timelines and instructions are provided in Enclosure 6.

Enclosures – 6

E1. References, continued
E2. Definitions
E3. IA Certification and Accreditation Overview
E4. The DIACAP Package
E5. The DIACAP Knowledge Service Overview
E6. DoD Information System Transition Timeline and Instructions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000 (hereby canceled)

(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981 as amended

(g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(h) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005

(i) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003

(j) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003

(k) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01D, "Joint Capabilities Integration and Development System (JCIDS)," March 12, 2004

(l) DoD Directive 8570.1, "Information Assurance Training, Certification and Workforce Management," August 15, 2004

(m) DoD Regulation 5200.1-R , "DoD Information Security Program", January 1997

(n) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 28, 2000

(o) Clinger-Cohen Act of 1998 , Public Law 104-106

(p) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology, " February 27, 2002, incorporating Change 1, March 20, 2002

(q) Committee on National Security Systems Instruction (CNSSI) No. 4009, "National Information Assurance Glossary," May, 2003[3]

(r) DoD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004

(s) "Joint DODIIS/Crypotologic SCI Information Systems Security Standards", 31 March 2001, Revision 2

[3] Available at http://www.cnss.gov/instructions.html

(t) DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004

(u) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004

(v) DoD Instruction O-8530.2, "Support to Computer Network Defense," March 9, 2001

(w) "DoD Net-Centric Data Strategy", prepared by DoD Chief Information Officer (CIO), May 9, 2003

(x) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02B, "Defense Information Systems Network (DISN): Policy, Responsibilities, and Processes," July 31, 2003

(y) National Security Telecommunications and Information Systems Security Instruction (NSTISSP) No. 11, "National Information Assurance Acquisition Policy," July 2003

(z) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," 05 June 1999

(aa) OMB Circular A-11, Transmittal Memorandum #76, "Preparing, Submitting, and Executing a Budget,"(Revised 05/27/2003)[4]

(bb) Government Paperwork Elimination Act (GPEA) Public Law 105-277, October 1998

[4] Available at http://www.whitehouse.gov/omb/circulars/a11/02toc.html

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Accreditation Boundary. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged.

E2.1.2. Accreditation Decision. An official designation from a DAA, in writing or digitally signed and made visible to the DoD CIO, regarding acceptance of the risk associated with operating a DoD information system and expressed as an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO).

E2.1.3. Adequate Security. Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that DoD information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through implementation of assigned IA Controls. The DoD methodology for determining assigned IA Controls is defined in DoDD 8500.1 (reference (b)) and the baseline DoD management, personnel, operational, and technical IA Controls are established in DoDI 8500.2 (reference (g)).

E2.1.4. Artifacts. System policies, documentation, plans, test results and the like that express or enforce the IA posture of the DoD information system, make up the C&A information, and provide evidence of compliance with the assigned IA Controls.

E2.1.5. Assigned IA Controls. A list of IA Controls that a DoD information system must address to achieve an adequate IA posture. Assigned IA Controls include baseline DoD IA Controls, optional DoD IA Controls for special conditions or technologies, e.g., health information portability and privacy or cross security domain solutions, and DoD, Mission Area, Component and DoD information system supplements, if any. DoDI 8500.2 (reference (g)).

E2.1.6. Authorization Termination Date (ATD). The date assigned by the DAA that indicates the date upon which authorization to operate is terminated for an ATO, IATO, or IATT.

E2.1.7. Authorization to Operate (ATO). The authorization, granted by a DAA, for a DoD information system to process, store, or transmit information. Authorization is based on acceptability of the IA component, the system architecture and implementation of assigned IA Controls.

E2.1.8. Automated Information System (AIS) Application. See DoD Information System.

E2.1.9. Certification. A comprehensive validation of actual IA capabilities and services of a DoD information system, made as part of and in support of the DIACAP, to establish compliance with assigned IA Controls based on standardized procedures.

E2.1.10. Certification Determination. A CAs validation of the system's compliance with IA controls, identifying and assessing the risks with operating the system, and the cost to correct or mitigate the IA security weakness.

E2.1.11. Certifying Authority (CA). The senior official having the authority and responsibility for the certification of information systems governed by a DoD Component IA Program.

E2.1.12. Certifying Authority Representative. Official acting on behalf of the Certifying Authority

E2.1.13. Communities of Interest (COI). An inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. Communities of Interest in the DoD can be either institutional or expedient. Institutional COIs whether functional or cross-functional, tend to be continuing entities with responsibilities for ongoing operations. Expedient COIs are more transitory and ad hoc, focusing on contingency and crisis operations. DoD Net-Centric Data Strategy", (reference (n)) addresses institutional and expedient COIs.

E2.1.14. Confidentiality Level (CL). Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-share determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoDI 8500.2 (reference (g)) defines three confidentiality levels: classified, sensitive, and public.

E2.1.15. Core Enterprise Services (CES). A set of common services intended to provide or improve access, enable information sharing, and enhance interoperability among GIG entities. Core Enterprise Services enable service oriented architectures and may include web services. Examples of CES include enterprise management, messaging, discovery, mediation, collaboration, hosting, storage, IA/security, and user assistance.

E2.1.16. Defense and Intelligence Community Accreditation Support Team (DICAST). Facilitates the joint management of risk brought about by interconnecting the networks of the DoD and Intelligence Community Components.

E2.1.17. Defense IA/Security Accreditation Working Group (formerly DISN Security Accreditation Working Group). The DSAWG develops and provides accreditation recommendations to the PAAs, DoD SIAO and DISN DAAs for information system connections to the DISN. It is the DISN community forum for reviewing and resolving C&A decisions related to sharing of community risk. .

E2.1.18. Denial of Authorization to Operate (DATO). DAA determination that a DoD information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA Controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

E2.1.19. Designated Accrediting Authority (DAA). 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.

E2.1.20. DIACAP Implementation Plan. The Implementation Plan contains the information system'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.

E2.1.21. DIACAP Knowledge Service. A web-based repository of information and tools for implementing the DIACAP that is maintained through the DIACAP TAG.

E2.1.22 DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an information system. 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 package, the Comprehensive Package containing all information connected with the certification of the information system, and the Executive Package containing minimum information for an accreditation decision. The Comprehensive package contains the System Identification Profile (SIP), the DIACAP Implementation Plan, the Certification Documentation, the DIACAP Scorecard, and the POA&M if required. The Executive package contains the System Identification Profile, the DIACAP Scorecard, and the POA&M if required.

E2.1.23. DIACAP Scorecard. A summary report that shows the certified or accredited implementation status of a DoD information system's assigned IA Controls and supports or conveys a certification determination and/or accreditation decision. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD information system in a format that can be easily understood by managers and be easily exchanged electronically.

E2.1.24. DIACAP Team. The officials responsible for implementing the DIACAP for a DoD information system. At a minimum the DIACAP Team includes the DAA, the CA, the SIAO, the DoD information system PM or SM, the DoD information system IAM, IAO, and a User Representative.

E2.1.25. DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, Federal and DoD requirements..

E2.1.26. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. DoDD 8500.1 (reference (b)).

E2.1.26.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program,

such as those described in DoD Directive 5000.1 (reference (i)). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note: an AIS application is analogous to a "major application" as defined in OMB A-130 (reference (n)); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

E2.1.26.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130 (reference (n)). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.26.3. Outsourced IT-based process. For DoD information assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.26.4. Platform IT Interconnection. For DoD information assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration. Also see Platform IT.

E2.1.27. Enclave. See DoD Information System.

E2.1.28. Enterprise Information Environment (EIE). The common, integrated computing and communications environment of the Global Information Grid (GIG). The GIG EIE is composed of assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The GIG EIE is also composed of assets that operate as or in direct support of end user devices, workstations, and servers that provide local, organizational, regional, or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE

assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. DoDI 8115.01 (reference (h)).

E2.1.29. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (o)). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. DoDD 8100.1 (reference (c)).

E2.1.29.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.29.1.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.29.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.29.1.3. Processes data or information for use by other equipment, software, or services.

E2.1.29.2. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

E2.1.30. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. DoDD 8500.1 (reference (b)).

E2.1.31. Inheritance. Inheritance in the context of DIACAP refers to the state in which an IA Control along with the control's validation results and compliance status, is shared across two or more systems for the purposes of C&A. Through inheritance, an existing IA Control and its C&A status, would extend from an "originating" system to another "receiving" system in order to model a real-word scenario of shared security infrastructure or capability. Inheritance is intended to reduce the complexity of testing by allowing the unilateral application of validation test results to all systems sharing the security capability. The DIACAP Implementation Plan specifically identifies IA Controls inherited between systems.

E2.1.32. IA Capabilities and Services. Information technology (hardware, software, and firmware), data, facilities, and human activities designed and implemented to provide integrity, confidentiality, non-repudiation, identification and authentication, and availability of DoD information systems through the exercise of management, operational, technical, and personnel controls.

E2.1.33. IA Component of the GIG. The collective and interdependent IA capabilities and services of the information systems that comprise the GIG.

E2.1.34. IA Component of the GIG Architecture. An abstract expression of current and future instances of the IA Component of the GIG.

E2.1.35. IA Component of the System Architecture. An abstract expression of all current or future IA/security technical solutions employed within a DoD information system and all interfaces to core enterprise or COI services for IA/security. The IA/security architecture assigns and portrays the assigned IA roles and behavior of all inherent IA/security features and functions and all embedded IA or IA-enabled IT products, and prescribes rules for interaction and interconnection. The IA component of the system architecture must conform to the IA Component of the GIG Architecture.

E2.1.36. IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with DoDI 8500.2 (reference (g)).

E2.1.37. IA Control Set. Collection of IA Controls associated with a level of integrity, availability, and confidentiality.

E2.1.38. Information Assurance Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the title Information Systems Security Manager (ISSM). DoDI 8500.2 (reference (g)).

E2.1.39. Information Assurance Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. DoDI 8500.2 (reference (g)).

E2.1.40. Information Assurance Senior Leadership Group (IASL). This senior leadership group 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. In addition, the group will establish the relationships required to ensure IA is designed into the Global Information Grid (GIG) integrated architectures.

E2.1.41. Information Assurance Support Environment (IASE). A web based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation. DoDI 8500.2 (reference (g)).

E2.1.42. Impact Code. Indicates DoD's assessment of the likelihood that a failed IA control will have IA consequences that have system-wide consequences. It is an indicator of the impact associated with non-compliance or exploitation of the IA Control. May also indicate the urgency with which corrective action should be taken. Impact codes are expressed as High, Medium, Low where High is the indicator of greatest impact or urgency.

E2.1.42.1. High Impact Code. The absence or incorrect implementation of this IA Control may result in the loss of information resources, unauthorized disclosure of information, or failure to maintain information integrity. Such exploitation may severely disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.42.2. Medium Impact Code. The absence or incorrect implementation of this IA Control may moderately disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.42.3. Low Impact Code. The absence or incorrect implementation of this IA Control may minimally disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.43. Implementation Procedures. Describes the required steps and provides guidance for implementing DoD IA Controls.

E2.1.44. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.45. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology. DoDD 8000.1 (reference (p))

E2.1.46. Information System (IS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. CNSSI No. 4009 (reference (q)).

E2.1.47. Information Systems Security Engineering/Engineer (ISSE). An engineering process or individual that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration.

E2.1.48. Interim Authorization to Operate (IATO). Temporary authorization to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision.

E2.1.49. Interim Authorization to Test (IATT). Temporary authorization to test a DoD information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

E2.1.50. Mission Area (MA). A defined area of responsibility whose functions and processes contribute to accomplishment of the mission. Those mission areas are: The War

Fighting Mission Area (WMA), Business Mission Area, (BMA), DoD portion of the Intelligence Mission Area (DIMA), and Enterprise Information Environment Mission Area (EIEMA).

E2.1.51. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories.

E2.1.51.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.51.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

E2.1.51.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.52. Net-centricity. Net-centricity is a robust, globally connected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-centric capabilities enable network-centric operations and Net-Centric Warfare (NCW). DoDD 8320.2 (reference (r)).

E2.1.53. Outsourced IT-based Process. See DoD Information System.

E2.1.54. Platform IT. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.

E2.1.55. Platform IT Interconnection. See DoD Information System.

E2.1.56. Plan of Action and Milestones (POA&M). A plan of action and milestones is required for any accreditation decision that requires corrective actions. It is a tool identifying tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

E2.1.57. Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for information systems within a GIG Mission Area.

E2.1.58. Program or System Manager (PM or SM). Official responsible for the early and seamless integration of information assurance into and throughout the system life cycle of an assigned DoD information system.

E2.1.59. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.60. Residual Risk. Risk due to partial or unsatisfactory implementation of assigned IA Controls.

E2.1.61. Risk Management. Achieving and maintaining an acceptable IA posture (i.e., adequate security, interoperability, and visibility within IA situational awareness or command and control systems) through the implementation of assigned IA Controls. IA Controls are assigned based on the value of the information being processed and the extent of information environment being shared.

E2.1.62. Security Relevant Event. An event that would cause a harmful change in an information system or its environment, or that a competent IAM would consider to require noting, investigation, or prevention (e.g., the discovery of malicious code in an information system, the discovery of an attempt to connect an unapproved device to the network).

E2.1.63. Senior Information Assurance Officer (SIAO). Official responsible for directing an organization's information assurance program on behalf of the organization's CIO.

E2.1.64. Service. A unit of work or specific operation done by a service provider to achieve a desired end result for a service consumer.

E2.1.65. Service Oriented Architecture (SOA). An architectural style whose goal is to achieve loose coupling or minimal dependency among interacting proxies through a small set of simple and ubiquitous interfaces among all participating proxies and descriptive messages constrained by an extensible schema delivered through the interfaces. Also, a specific type of system in which each proxy is called a "service" because it performs some well-defined operation (i.e., "provides a service") that can be invoked outside of the context of a larger application. That is, a service might be implemented to expose a feature of a larger application (e.g., the purchase order processing capability of an enterprise resource planning system might be exposed as a discrete service), and the users of that service need be concerned only with the interface description of the service. Security requirements for interaction are addressed in design

and in the interface description, thus allowing proxies to dynamically interact with services outside the accreditation boundary.

E2.1.66. Severity Code. Indicates the CA's assessment of the likelihood of system-wide IA consequences, given a single or multiple findings. It is the Code assigned to a system IA security weakness by a CA as part of a certification analysis to indicate (1) the risk level associated with the IA security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III," where CAT I is the indicator of greatest risk and urgency.

E2.1.66.1. CAT I Severity Code. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges, and usually cannot be mitigated.

E2.1.66.2. CAT II Severity Code. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings can usually be mitigated and will not prevent an ATO from being granted.

E2.1.66.3. CAT III Severity Code. Assigned to recommendations that will improve IA posture but are not required for an authorization to operate.

E2.1.67. Stand-Alone Information System. An information system operating independently of any other information system within an environment physically secured commensurate with the highest classification of material processed or stored thereon. DoDI 8580.1 (reference (t)).

E2.1.68. System Identification Profile (SIP). An information base, i.e., a document, collection of documents, or collection of data objects within an automated information system, that uniquely identifies an information system within the DIACAP and contains established management indicators, e.g., DIACAP status.

E2.1.69. User Representative (UR). Individual or organization that represents the user community in the DIACAP.

E2.1.70. Validation. Activity applied throughout the system life cycle, to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD information system's assigned IA Controls are implemented correctly and are effective in their application.

E2.1.71. Validation Event. The execution of one or more Validation Procedures for a DoD information system.

E2.1.72. Validation Procedure. Describes the requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results, and may include associated supporting background material, sample results, or links to automated testing tools.

E2.1.73. Validator. Entity responsible for conducting a validation procedure.

E2.1.74. 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.

E2.A1. ATTACHMENT 1 TO ENCLOSURE 2

ACRONYMS

ACAT	Acquisition Category
ACTD	Advanced Concept Technology Demonstration
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
AIS	Automated Information System
ATD	Authorization Termination Date
ATO	Authorization to Operate
BMA	Business Mission Area
C&A	Certification and Accreditation
CA	Certifying Authority
CCA	Clinger Cohen Act
CCM	Configuration Control and Management
CDS	Cross Domain Solution
CES	Core Enterprise Services
CFO	Chief Financial Officer
CIO	Chief Information Officer
CJCS	Chairman Joint Chiefs of Staff
CJCSI	CJCS Instruction
CL	Confidentiality Level
C/NC	Compliant/Non-compliant
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COI	Communities of Interest
COTS	Commercially Owned Technology Services
DAA	Designated Accrediting Authority
DATO	Denial of Authorization to Operate
DCID	Director Central Intelligence Directive
DIACAP	DoD Information Assurance Certification and Accreditation Process
DICAST	Defense and Intelligence Community Accreditation Support Team
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DITPR	Defense Information Technology Portfolio Repository
DMS	Defense Messaging System
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DOT&E	Director, Operational Test and Evaluation
DSAWG	Defense IA/Security Accreditation Working Group (formerly DISN Security

	Accreditation Working Group)
EIE	Enterprise Information Environment
EIEMA	Enterprise Information Environment Mission Area
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GCCS	Global Command and Control System
GIG	Global Information Grid
GOGO	Government Owned Government Operated
GOTS	Government Owned Technology Services
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IASL	Information Assurance Senior Leadership Group
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IC	Intelligence Community
ICIS	Integrated Consumable Item Support
ID	Identification
IG	Inspector General
ISSE	Information Systems Security Engineer/Engineering
ISSM	Information Systems Security Manager
IT	Information Technology
JCIDS	Joint Capabilities Identification and Development System
KS	Knowledge Service
MA	Mission Area
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MC	Mission Critical
ME	Mission Essential
MS	Mission Support
MS-A, B or C	[Acquisition] Milestone A, B, or C
NCOW-RM	Net-Centric Operations and Warfare Reference Model
NIPRNet	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
NSS	National Security Systems
NSTISSP	National Security Telecommunications and Information Security Policy
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PAA	Principal Accrediting Authority
PM or SM	Program or System Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPBE	Planning, Programming, Budgeting and Execution
PPSM	Ports, Protocols and Services Management
RTM	Requirements Traceability Matrix

SAP	Special Access Program
SAR	Special Access Requirement
SCI	Sensitive Compartmented Information
SEP	System Engineering Plan
SIAO	Senior Information Assurance Officer
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SLC	System Life Cycle
SOA	Service Oriented Architecture
SSAA	System Security Authorization Agreement
TAG	Technical Advisory Group
TEMP	Test and Evaluation Master Plan
UR	User Representative
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USI	Universal System Identifier
WMA	Warfighting Mission Area

E3. ENCLOSURE 3

INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION OVERVIEW

E3.1 Background. This enclosure describes the DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, Federal and DoD requirements. It also describes the processes for configuration management of DoD IA Controls and supporting implementation materials. Within the Department of Defense, IA C&A is comprised of activities and roles that are distributed across all levels of the DoD organization and GIG governance structures, and across all stages of the life cycle of both the IA Component of the GIG and individual information systems.

E3.2. Statutory and Federal Requirements.

E3.2.1. E-Government Act. The E-Government Act (Public Law 107-347) of December 2002 recognized the criticality of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the "Federal Information Security Management Act (FISMA)" (reference (a)), requires Federal departments and agencies to develop, document, and implement an organization-wide program to provide information security for the information systems that support their operations and assets.

E3.2.2. FISMA. The FISMA requires Federal departments and agencies develop and implement an organization-wide information security program designed to safeguard IT assets and data. It lays out the Federal framework for annual IT security reviews, reporting, and remediation planning, and it requires that Federal departments and agencies evaluate their information system security programs and report the results on an annual basis. Under FISMA, the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information.

E3.2.3. OMB A-130. Office of Management and Budget (OMB) Circular No. A-130 (reference (n)), provides uniform government information resources management policies according to the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1998. Appendix III of OMB A-130 provides specific guidance on the security of federal automated information systems."

E3.3. DoD Requirements.

E3.3.1. The 8500 Series of DoD Directives and Other Issuances. DoD IA policy and processes are established in the 8500 series of DoD directives and other issuances. The DIACAP

is the IA process for implementing IA policy and integrating IA organizing principles and processes at the information system level. For example, DoDD 8500.1 (reference (b)) establishes four types of DoD information systems for the purposes of IA management. DoDI 8500.2 (reference (g)) establishes a controls-based approach for identifying and implementing IA capabilities and services and establishes the baseline DoD IA Controls for DoD information systems. The DIACAP defines the process for assigning, implementing and validating those IA Controls as well as an enterprise process for maintaining IA Controls and supporting implementation material. DoDI 8580.1 (reference (t)) establishes the process for integrating IA into the Defense Acquisition System. The DIACAP supports, complements, and enforces that process. DoDI 8551.1 (reference (u)) establishes the process for managing risk associated with network ports, protocols, and services management (PPSM). The DIACAP ensures that compliance with PPSM is a condition of the ATO or a risk consideration in an accreditation decision. DoDI O-8530.2 (reference (v)) establishes a requirement for operational DoD information systems to establish a service relationship with a Computer Network Defense Service Provider (CNDSP). The DIACAP ensures that association with a CNDSP is a condition of an ATO or a risk consideration in an accreditation decision.

E3.3.2. The GIG Information Assurance Domain. The GIG IA Domain, established by the "DoD Net-Centric Data Strategy" reference (w) as an element of the Enterprise Information Environment Mission Area, is the GIG governance entity responsible for establishing and maintaining a holistic view of IA and IA-enabled IT investments and initiatives across the GIG. It ensures that those investments and initiatives are aligned with GIG strategies and needs; and employ integrated strategic planning, integrated architectures, transition planning, and risk and performance management measures to ensure that suppliers and providers of IA capabilities and services operate as a logical whole and within an ordered framework to deliver the right IA capabilities and services to the right place and user, at the right time, at the right level and condition, and with the right support. The GIG IA Domain employs the DIACAP to link the implementation and performance of enterprise IA capabilities and services to individual systems.

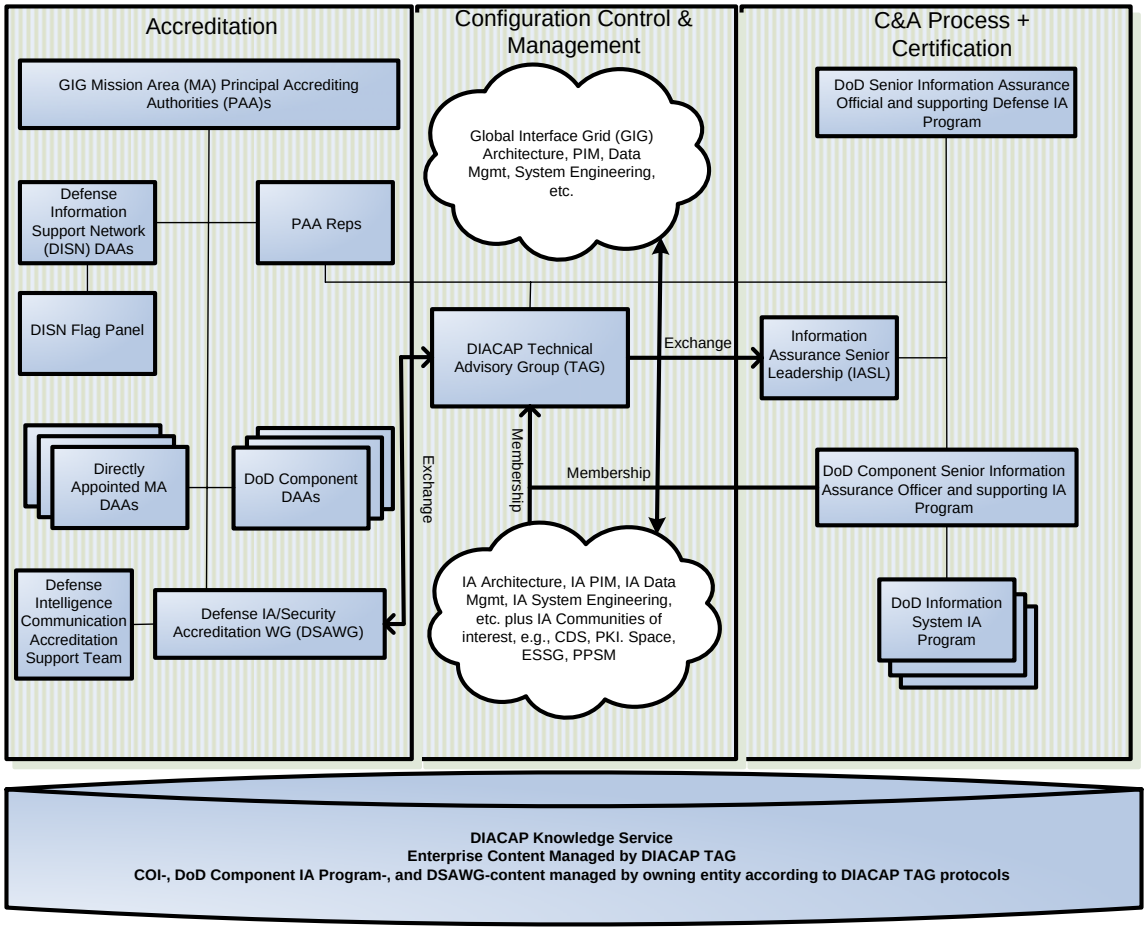
E3.3.3. The IA Component of the GIG Architecture is both a series of published documents and a dynamic process for understanding and transforming information assurance within the GIG. The IA Component of the GIG Architecture establishes target timeframes for enterprise capabilities and services that help drive GIG IA Domain investment strategies and baseline IA Controls, which are the basis for certification and accreditation decisions within the DIACAP.

E3.3.4. IA C&A and Net-Centricity. Traditionally, C&A decisions have not distinguished among the IA capabilities and services that are intrinsic to the set of information resources that comprise an information system, the information environment in which an information system operates, and the management and control information that is exchanged between the information system and enterprise services. In order to fully achieve the Department's vision of net-centric operations and warfare, the GIG must become increasingly service oriented, as described in the GIG Integrated Architecture and the Net-Centric Operations and Warfare Reference Model (NCOW-RM), DoDD 5000.1 (reference (i)). Specifically, the GIG must be increasingly populated with proxies that are designed to support interoperable machine-to-machine interaction over a network. This service-oriented transformation will

demand a very different IA C&A model – one that distinguishes between the IA features, functions and mechanisms that are intrinsic or "built in" to information systems, e.g., proxies, and the operational IA posture that emerges from the interaction of information systems. The DIACAP CCM, informed by the IA Component of the GIG Architecture and the GIG IA Domain, is the Department's vehicle for ensuring that its IA C&A model remains supportive of the GIG transformation.

E3.4. The DIACAP Enterprise Governance Structure is intended to synchronize and integrate DIACAP activities across all levels (Defense-wide, Mission Area, DoD Component, and DoD information system); across all aspects of the IT life cycle; and across both logical and organizational entities. To ensure appropriate separation of powers and checks and balances, it is comprised of three major elements: an accreditation structure; a C&A process certification structure; and a configuration control and management structure. These elements are illustrated in Figure E3.1 below and described in the succeeding paragraphs.

Figure E3.1. DIACAP Enterprise Governance



E3.4.1. Accreditation. The Principal Accrediting Authorities are aligned to the GIG MA's, i.e.., the Enterprise Information Environment, Business, Warfighting, and Intelligence. Each PAA has a Representative who works with the DoD SIAO to oversee the DIACAP TAG and DSAWG. The DSAWG is expanded from Defense Information Systems Network (DISN) to

Defense-wide, and supports the GIG PAAs and all DAAs, to include the DISN DAAs. The GIG PAAs may realign the DISN DAA structure and appointments as needed. The DSAWG coordinates cross-cutting issues and workload with the Defense and Intelligence Community Accreditation Support Team (DICAST). DoD Component DAAs are responsive to authority from the GIG PAAs, and support and enforce PAA guidelines. Additionally, PAAs may directly appoint DAAs for major initiatives or COIs.

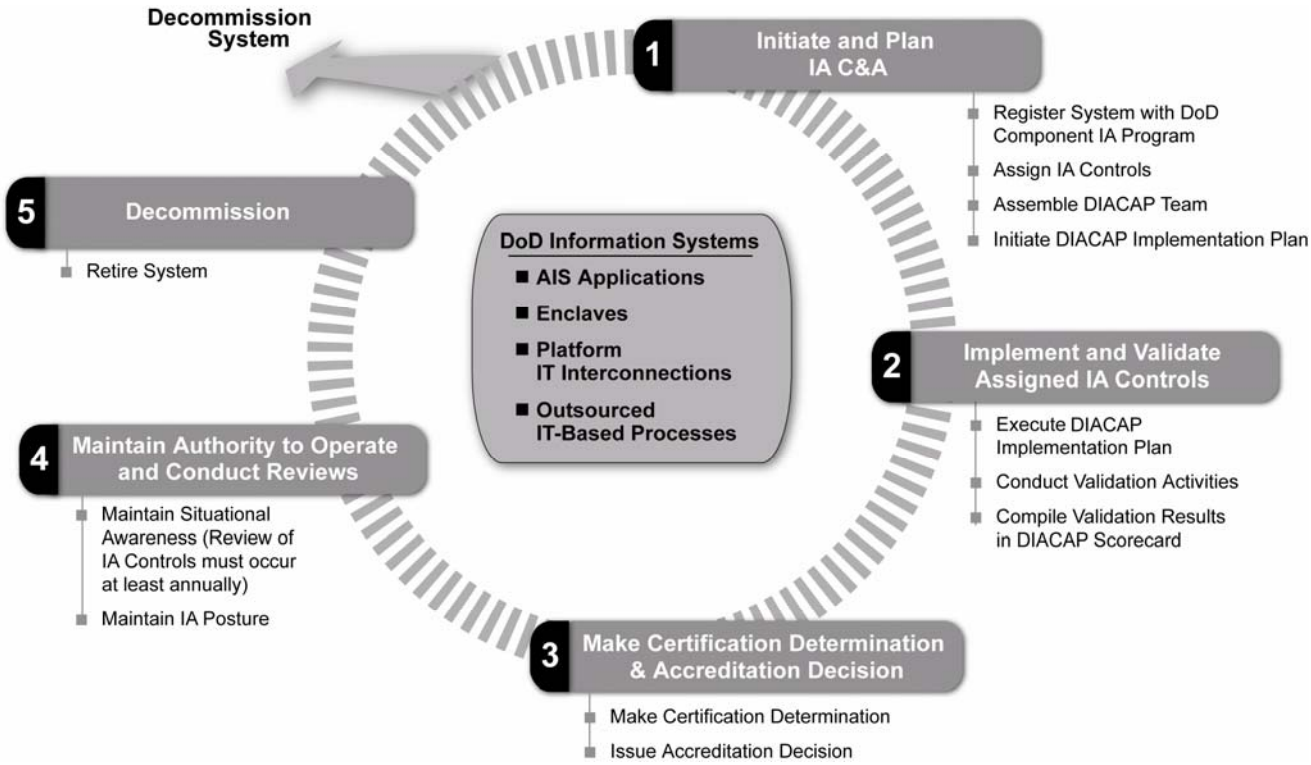
E3.4.2. Configuration Control and Management (CCM). The DIACAP TAG provides detailed analysis and authoring support for the enterprise portion of the DIACAP Knowledge Service content. The TAG interfaces with DoD Component IA Programs, the MAs, IA COIs, and specialized entities within the IA Domain Governance Structure (e.g., the IA Architecture Office or the DSAWG); addresses issues that are common across entities; and recommends changes to the baseline IA Controls and C&A process. The Information Assurance Senior Leadership (IASL) group serves as an SIAO community forum for establishing priorities and resolving cross-cutting issues.

E3.4.3. C&A Process Administration and Certification. Authority and responsibility for certification are vested in DoD Component SIAO. Each SIAO serves as the CA for all DoD information systems assigned to or governed by the DoD Component CIO[5] and supporting IA Program. Each CA may task organize, staff and centralize/delegate certifying activities as he/she sees fit. Regardless of the adopted model, the SIAO is responsible for certification quality, capacity, visibility, and effectiveness. Additionally, each CIO, supported by his/her 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 DIACAP status of assigned information systems, enforcement of training requirements for persons participating in the DIACAP, support to DAAs, and responsiveness to the DoD CIO. The IASL serves as an SIAO community forum for assessing and improving C&A process administration.

E3.5. DIACAP Activities. The DIACAP is comprised of the following activities, Figure E3.2., and tasks, which may occur concurrently or at different frequencies for different IA Controls. 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 non-complying with the DIACAP. Regardless of system life cycle stage (e.g., acquisition, operation), unaccredited systems shall initiate the DIACAP immediately. The earlier in the system life cycle the DIACAP is initiated, the less expensive and problematic is the implementation of IA and services.

[5] All DoD information systems must be aligned to/governed by a DoD Component CIO.

Figure E3.2. DIACAP Activities



E3.5.1. Initiate and Plan IA C&A. This activity includes registering the system with the governing DoD Component IA Program, assigning IA Controls, assembling the DIACAP Team, and initiating the information system's DIACAP Implementation Plan.

E3.5.1.1. The members of the DIACAP Team are required to meet the investigative levels for users with IA management access to DoD unclassified information systems as established in paragraph E3.4.8. of DoDI 8500.2 (reference (g)). 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.T.1of DoDI 8500.2 (reference (g)). Allowable relationships among DIACAP Team members are outlined in Table E3.1 below.

Table E3.1. Allowable Relationships Among DIACAP Team Members

Organizational Condition or Status	**Allowed (Y/N)**
CA reports to a DAA	Yes
CA reports to the PM or SM	No
CIO is a DAA	Yes
DAA and CA for a DoD information system are the same person	Yes
DAA reports to the PM or SM	No
PAA is a DAA	Yes
PM or SM and CA both report to the DAA	Yes
PM or SM and CA for a DoD information system are the same person	No
PM or SM and DAA for a DoD information system are the same person	No
PM or SM and User Representative for a DoD information system are 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
User Representative reports to the CIO	Yes
User Representative reports to the PM or SM	No
User Representative reports to the SIAO/CA	Yes

E3.5.1.2. System registration establishes the relationship between the DoD information system and the governing DoD Component IA Program that continues until the DoD information system is decommissioned. DIACAP registration is related to other DoD initiatives to collect IT-related information, e.g., the DITPR; however, specific registration instructions change over time and are therefore maintained through the DIACAP CCM and published in the

DIACAP Knowledge Service. Attachment 1 to Enclosure 4 of this Instruction identifies the minimum data requirements, plus explanations, for registration. The System Identification Profile (SIP) becomes part of the DIACAP package for the information system. The DIACAP package is a collection of documents or collection of data objects generated through DIACAP implementation for an information system and maintained throughout the system's life cycle. It has an executive and comprehensive version

E3.5.1.3. Regarding system interconnection, OMB A-130 (reference (n)) requires "written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems." DoD information systems generally satisfy this requirement through compliance with the connection management procedures established in CJCSI 6211.02 (reference (x)). Exceptions are (1) a network connection as described in DoD Regulation 5200.1-R (reference (m)) with a non-DoD network, and (2) separately accredited information systems that communicate directly through tightly coupled mechanisms such as shared memory or direct code invocation. For IA purposes, loosely coupled proxies communicating via web-services, is not considered a system interconnection, i.e., does 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 information systems, e.g., electronic commerce/electronic data interchange transactions with an information system belonging to another department or agency.

E3.5.1.4. A DIACAP Implementation Plan contains the information system'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.

E3.5.2. Implement and Validate Assigned IA Controls. This activity includes all tasks related to the execution of the DIACAP Implementation Plan. Each assigned IA Control is implemented according to the applicable implementation and validation requirements and expected results described in the DIACAP Knowledge Service. IA Controls may be individually validated as they are completed, or they may be validated by sub-entity of the DoD information system, Subject Area, or other organizing scheme established by the DIACAP Team; therefore, implementation and validation activities may be occurring in parallel. Validation includes all tasks related to the execution of the Validation Procedures that are associated with assigned IA Controls. Validation Procedures are maintained through the DIACAP CCM and published in the DIACAP Knowledge Service. Each Validation Procedure describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results, and may include associated supporting background material, sample results, or links to automated testing tools. Actual results are recorded according to the criteria and protocols specified in the Validation Procedure 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. The status of actual results for all assigned Validation Procedures is compiled into a DIACAP Scorecard, further discussed and illustrated in Enclosure 4 of this Instruction.

E3.5.3. Make Certification Determination and Accreditation Decision.

E3.5.3.1. 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. Certification considers: (1) the IA posture of the DoD information system itself, that is, the overall reliability and viability of the information system plus the acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself; and (2) how the system behaves in the larger information environment, that is, does it introduce vulnerabilities to the environment; does it correctly and securely interact with information environment management and control services; is its visibility to situational awareness and network defense services adequate? Two indicator codes aid in this consideration: Impact Codes and Severity Codes. Impact Codes are assigned by DoD to IA Controls at the time of their authoring and maintained through the DIACAP CCM. Within an IA Control Set, they indicate each IA Control's relative contribution to the approved target IA posture, and are expressed as High, Medium, or Low. Severity Codes are assigned by an approved CA representative to specific findings or IA security weaknesses during certification.

E3.5.3.2. The certification determination is based on the validation actual results. It considers Impact Codes associated with IA Controls in a non-compliant status, associated Severity Codes, 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). Certification aids in POA&M development and characterizes residual risk. See Attachment 3 to Enclosure 4 of this Instruction for further discussion on POA&M formulation.

E3.5.3.3. The accreditation decision always applies to an operationally ready instance of a DoD information system and is 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 upon the shared information environment. An accreditation decision is expressed as Authorization to Operate (ATO), Interim Authorization to Operate (IATO), Interim Authorization to Test (IATT), or Denial of Authorization to Operate (DATO). Absent an accreditation decision, a system is considered Unaccredited.

E3.5.3.4. The ATO accreditation decision must specify an Authorization Termination Date (ATD) that is within three years of the authorization date. See paragraph E3.5.4.4. below for guidelines on re-accreditation.

E3.5.3.5. The IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DoD information system may not be granted more than two consecutive 180 day IATOs. A request for IATO must be accompanied by a POA&M for correcting or satisfactorily mitigating the weaknesses. Corrective actions specified in the POA&M must be achievable within the authorization period and must be resourced accordingly. If, at the end of a second consecutive IATO, a DoD information system weaknesses have not

been corrected or satisfactorily mitigated, the DAA shall issue a DATO. The DATO shall remain in effect until all corrective actions identified in the POA&M are implemented satisfactorily and the DAA is able to grant an ATO. CAT II weaknesses are those that can lead to unauthorized system access or activity but can usually be corrected or mitigated to a point where any residual risk is acceptable. An ATO can be granted with a CAT II weaknesses only when there is clear evidence that the CAT II weaknesses can be corrected or satisfactorily mitigated within six months of the accreditation decision If CAT II weaknesses cannot be corrected or satisfactorily mitigated within the time limitation imposed in the IATO, the DAA must certify in writing that continued system operation is critical to mission accomplishment or terminate system operation. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD Component CIO..

E3.5.3.6. An accreditation decision always requires a certification determination. If a compelling mission or business need requires the rapid introduction of a new DoD information system into the GIG, validation activity and a certification determination are still required. If the validation is abbreviated in the interest of time, the accreditation decision cannot exceed IATO. If operation will be required beyond the time period of the IATO, a complete validation should be initiated immediately.

E3.5.3.7. An IATO accreditation decision is intended to manage IA security weaknesses. It is not intended to be a device for signaling an evolutionary acquisition. If IA/security is adequate for the intended processing time, the version of an DoD information system acquired in one of a planned series of acquisition increments or development spirals may (and should) be granted ATO, even if additional or enhanced IA capabilities and services are planned for future increments or spirals. The ATO accreditation decision should not be reserved for DoD information systems for which no change is planned or foreseen. Such thinking engenders an abuse of the IATO accreditation status and an inaccurate portrayal of the DoD information system's IA posture.

E3.5.3.8. 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. An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate.

E3.5.4. Maintain Authorization to Operate and Conduct Reviews. Continued authorization to operate is contingent upon the sustainment of an acceptable IA posture. The DoD information system IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture.

E3.5.4.1. Situational Awareness. Included in the IA Controls assigned to all DoD information systems are IA Controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations, e.g., penetration testing. The IAM monitors for security relevant events and configuration changes to the system or information environment that negatively impact IA posture, and both continuously and periodically assesses the quality of IA Controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., Inspector General,

Government Accountability Office), exercises, operational evaluations, and the like. Additionally, the IAM, independently or at the direction of the CA or DAA, may schedule a re-validation of any or all IA Controls at any time. FISMA (reference (a)), requires revalidation of a select number of controls not less than annually.

E3.5.4.2. 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 information system itself.

E3.5.4.3. Reviews. Not less than annually, the IAM provides a written statement to the DAA and the CA, based on the review of all IA Controls and testing of selected IA Controls as required by FISMA (reference (a)), that either confirms the effectiveness of assigned IA Controls and their implementation or recommends changes such as those described in paragraph E3.5.4.2 above. The CA and DAA review the IAM statement in light of mission and information environment indicators and determine a course of action. The review and determination, expressed according to Table E3.2 below, is recorded in the System Identification Profile, described in Attachment 1 of Enclosure 4 of this Instruction, and made visible to the DoD CIO/SIAO for FISMA reporting. In addition to potential changes in accreditation status that are triggered by annual reviews and the scheduled termination of accreditation decisions, changes may be event-driven. A DAA may downgrade or revoke an accreditation decision any time risk conditions or concerns so warrant.

Table E3.2. Annual Review Determinations

Number	Determination
1	No change in accreditation status, no corrective action required, and no change in ATD
2	No change in accreditation status, PM or SM is directed to initiate precautionary IA improvements, no change in ATD.
3	Accreditation status is downgraded to IATO, PM or SM is directed to prepare a POA&M, ATD is reset to 180 days or less.
4	Accreditation status is downgraded to DATO, and operation is halted.

E3.5.4.4. Re-accreditation. An information system must be recertified and reaccredited once every three years. The results of validation tests of IA Controls conducted during an annual review may be used in the recertification and re-accreditation of the information system.

E3.5.5. Decommission the DoD Information System. When a DoD information system is removed from operation, a number of IA-related events are required relative to the disposition

of DIACAP registration information and system–related data or objects in GIG supporting IA infrastructures and core enterprise services such as key management, identity management, service management, privilege management, policy management, and discovery. Requirements and procedures change over time as the GIG EIE changes and these changes are maintained through the DIACAP CCM and published in the DIACAP Knowledge Service.

E3.6. IA Product Evaluation and DIACAP Evaluation. The DoDI 8500.2 (reference (g)) requires the evaluation of IA and IA-enabled IT products that are incorporated into DoD information systems. DoD information systems that are comprised of both IT products and IA or IA-enabled products shall ensure that their IA and IA-enabled products are evaluated according to DoDD 8500.1 (reference (b)), and shall be subject to the DIACAP. Any DoD information system that is comprised of a single IA-enabled product or solution shall be subject to the DIACAP, however, the DIACAP validation may also serve as the IA-enabled product evaluation. For ease of readership, this condition is restated in Table E3.3, below:

Table E3.3. IA Product Evaluation and DIACAP Validation

Condition	Acceptable Evaluation / Validation Approach
Accreditation Boundary includes both IT products or services and IA or IA-Enabled IT Products	1. NSTISSP 11 (reference (y)) evaluation for IA and IA-Enabled Products, plus 2. DIACAP for overall system design and configuration
Proposed Accreditation Boundary includes a single IT product or service that is IA-enabled AND nothing else	DIACAP validation is sufficient; separate NSTISSP 11 evaluation is not required.

E3.7. Software Quality. New DoD information systems developing or integrating software must specify software quality controls and validation methods. These may be references to plans or activities required by the Defense Acquisition System, e.g., a Test and Evaluation Master Plan (TEMP) or System Engineering Plan (SEP), or they may be adjuncts that detail the specific security-related requirements for validation of software quality. Software quality controls shall include, but not be limited to software practices aimed at making software resistant to compromise and denial of service, such as avoiding buffer overflows, avoiding cross-site scripting, validating input, authenticating inter-process communications, protecting application configuration data, making the software resistant to internal failure (e.g., preventing deadlocks and sequence conditions, managing time-outs, load level limits, unresponsive output, managing error and exception handling and recovery), and preparing software for deployment (e.g., removing debugger hooks and developer backdoors, default accounts, sensitive comments, and developer/maintenance passwords).

E4. ENCLOSURE 4

THE DIACAP PACKAGE

E4.1. The DIACAP Package. 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 E4.1 below. The Executive Package column lists the information that may be necessry for an accreditation decision. Note, Table E4.1. is not meant to describe a single fixed document format. Each DAA will determine what information is necessary to make an accreditation decision. Acquisition contracts must specify information assurance C&A deliverables.

Table E4.1. DIACAP Package Contents

Comprehensive Package	**Executive Package**
System Identification Profile	System Identification Profile
Implementation Plan • IA Controls – Inherited and implemented • Implementation Status • Responsible entities • Resources • Estimated completion date for each IA Control	
Supporting Documentation for Certification • Actual Validation Results • Artifacts associated with implementation of IA Controls • Other	
DIACAP Scorecard • Certification determination • Accreditation Determination	DIACAP Scorecard • Certification Determination • Accreditation Determination
POA&M (If required)	POA&M (If required)

E4.2. System Identification Profile (SIP). The SIP is compiled during the DIACAP registration and maintained throughout the system life cycle. An overview of the System Identification Profile is provided at Attachment 1 to Enclosure 4.

E4.3. The DIACAP Scorecard. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD information system in a format that can be easily understood by managers and be easily exchanged electronically. A notional scorecard is provided in Attachment 2 to Enclosure 4 of this Instruction. Additional data elements may be specified by CIOs, DAAs, or other enterprise users of the DIACAP Scorecard.

E4.4. Plan of Action and Milestones (POA&M). A plan of action and milestones is required for any accreditation decision that requires corrective actions. The POA&M addresses: (1) why the system needs to operate; (2) any operational restrictions imposed to lessen the risk during the interim authorization; (3) specific corrective actions necessary to demonstrate that all assigned IA Controls have been implemented correctly and are effective; (4) the agreed upon timeline for completing and validating corrective actions; and (5) the resources necessary and available to properly complete the corrective actions. Attachment 3 to Enclosure 4 provides instructions for understanding and developing a POA&M.

Attachments – 3

E4.A1. System Identification Profile
E4.A2. Notional DIACAP Scorecard
E4.A3. Plan of Action and Milestones (POA&M) Instructions

E4.A1 ATTACHMENT 1 TO ENCLOSURE 4

SYSTEM IDENTIFICATION PROFILE (SIP)

ID	Data Element Descriptor	Example, Acceptable Values or Comment	Required/ Conditional
1	System ID	Unique, system generated ID for each individual system.	
2	System Component	The organization that owns or controls the DoD information system	Required
3	Governing DoD Component IA Program		Required
4	System name		Required
5	Acronym		
6	System Version or Release Number		Required
7	System Description	A narrative description of the system, its function, and uses	Required
8	DIACAP Activity	Initiate and Plan IA C&A, Implement and Validate Assigned IA Controls , Make Certification Determination and Accreditation Decision, Maintain Authorization to Operate and Conduct Reviews.,	
9	System Life Cycle or Acquisition Phase	1. Concept Refinement 2. Milestone A (MS-A) Technology Development, 3. MS-B System Development and Demonstration 4. MS-C Production and Deployment Demonstration 5. Operations and Support 6. Disposal or Decommissioning	Required
10	Information Assurance Record Type	Enclave, AIS application, Outsourced IT-Based Process, Platform IT Interconnection	Required
11	MAC	I, II, III	Required
12	Confidentiality Level		Required
13	Mission Criticality	Mission Critical (MC) Mission Essential (ME) based or Mission Support (MS)	Required
14	Accreditation Vehicle	8500.2 , (DCID) 6/3	Required

ID	Data Element Descriptor	Example, Acceptable Values or Comment	Required/ Conditional
15	Additional Accreditation Vehicles	e.g., Privacy Requirements, Special Access Requirements, Cross Domain Solution (CDS) Ticket Number, Non Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or GIG CAP Identifier, Ports, Protocols and Services Management (PPSM) Identifier	As specified
16	Certification Date	Date certified by designated approval authority	
17	Approval Date	Date approved by designated approval authority	
18	Accreditation Status	Unaccredited, ATO, IATO, IATT, DATO	Required (default is Unaccredited)
19	Accreditation Document	Do you have formal documentation that indicates the specifics of the certification and accreditation (C&A) process?	
20	Accreditation Date	For ATO, IATO, IATT	Required
21	Authorization Expiration Date	For ATO, IATO, IATT	Conditional
22	DIACAP Team Roles, Member Names and Contact Information	e.g., PM or SM, IAM, User Representative, CA, DAA, SIAO, CIO	Required
23	ACAT Category	Categorization of Project/Program relative to ACAT designations	
24	Type of IT Investment	What type of IT investment is this (Business System, Infrastructure, NSS, Initiative, Not Applicable)?	
25	System Life cycle Phase	Identifies the phase of its lifecycle in which the system is, or will 1. Concept Refinement: 2. Technology Development: 3. System Development & Demonstration	
26	Software Category	COTS, GOTS or Custom business system	
27	Privacy Impact Assessment	Yes/No	
28	E-	Yes/No	

ID	Data Element Descriptor	Example, Acceptable Values or Comment	Required/ Conditional
	Authentication Risk Assessment		
29	Date Annual Security Review	What was the date of the annual security review required by FISMA and DoD?	
30	System Operation	Government (DoD) Owned Government Operated (GOGO)	
31	Contingency Plan	Yes/No	
32	Contingency Plan Tested	Yes/No	
33	Information Assurance Record Type	• Automated Information System Application • Enclave (8500.2) • Outsourced IT-based Process (8500.2)	
34	Security Controls Tested Date	Indicate the last date system security controls were tested.	

E4.A2. ATTACHMENT 2 TO ENCLOSURE 4

NOTIONAL DIACAP SCORECARD

DIACAP SCORECARD

System Name	Accreditation	Period Covered From	Period Covered To	Last Update
Enterprise Mission Assurance Support Service	**IATO**	**17-May-05**	**17-Nov-05**	**11-Oct-05**

Designated Accrediting Authority (DAA)		
Nathan Gray		
Certifying Authority (CA)	Certified?	Cert. Date
Matthew Summers	Yes	17-May-05

Mission Assurance Category (MAC)	Confidentiality Level (CL)
MAC II	Sensitive

IA Control Subject Area	Number	IA Control Name	C/NC	Impact Code	Last Update
Continuity	COAS-2	Alternate Site Designation	NC	High	11-Oct-05
Continuity	COBR-1	Protection of Backup and Restoration Assets	C	High	27-Sep-05
Continuity	CODB-2	Data Backup Procedures	C	Basic	11-Oct-05
Continuity	CODP-2	Disastery and Recovery Planning	C	Medium	11-Oct-05
Continuity	COEB-1	Enclave Boundary Defense	NC	High	1-Oct-05
Continuity	COED-1	Scheduled Exercises and Drills	NC	Medium	1-Oct-05
Continuity	COEF-2	Identification of Essential Functions	NC	Medium	11-Oct-05

E4.A2.1. Table E4.A2.1 below provides explanations for the fields contained in the notional scorecard.

Table E4.A2.1. Scorecard Instructions

Reference	Description
System Name	The identifying name for the system being certified.
Accreditation	The accreditation decision for the system (i.e., Unaccredited, ATO, IATO, IATT, DATO)
Period Covered	The period covered describes the date of the accreditation (if the system has a decision other than Unaccredited), and the Authorization Termination Date (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.
Designated Accrediting Authority	The name of the individual serving as the DAA for the system.
Certifying Authority	The name of the individual serving as the CA for the system.
Certified?	An indication (Yes or No) of whether or not the system has been

Reference	Description
	certified.
Cert. Date	The date of the certification.
Mission Assurance Category (MAC)	The Mission Assurance Category applied to the system.
Confidentiality Level (CL)	The Confidentiality Level applied to the system.
IA Control Subject Area	A listing of the Subject Area associated with the IA Control.
Number	A listing of the reference number associated with the IA Control.
IA Control Name	A listing of the name associated with the IA Control.
C/NC	An indication of the compliance status of the IA Control (Compliant or Non-Compliant). A POA&M is required if N/C. Note: N/C may indicate either non-implementation or complete failure of the control under testing; it also may indicate that partial failure of a control under testing, (i.e. three of four testing points pass)
Impact Code	A listing of 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).

E4.A3. ATTACHMENT 3 TO ENCLOSURE 4

PLAN of ACTION and MILESTONES (POA&M) INSTRUCTIONS

E4.A3.1. A plan of action and milestones (POA&M) is a tool identifying tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

E4.A3.2. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The Office of Management and Budget (OMB) requires agencies to prepare POA&Ms for all programs and systems where an information technology (IT) security weakness has been found and OMB guidance directs chief information officers (CIOs) and agency program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets, including those operated by contractors). Additionally, program officials are required to regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

E4.A3.3. The POA&M is designed to be a management tool to assist agencies in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. They may contain pre-decisional budget information and the Department of Defense (DoD) has a responsibility to maintain the confidentiality of this type of information. DoD IT Security POA&Ms shall:

E4.A3.3.1. Be tied to the agency's budget submission when required through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.[6]

E4.A3.3.2. Include all IT security weaknesses found during any other review done by, for, or on behalf of the agency, including but not limited to Government Accountability Office (GAO) audits, financial system audits, official security test and evaluation or compliance review and critical infrastructure vulnerability assessments.

E4.A3.3.3. Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

E4.A3.3.4. Follow the format detailed in the examples provided by the OMB and shown below.

[6] OMB Circular A-11 (reference (aa)) requires that agencies develop and submit to OMB business cases (exhibit 300) for major IT projects. Additionally, each agency submits an exhibit 53, a list of both major and non-major IT systems. The agency assigns a unique identifier to each system and includes it with these exhibits.

E4.A3.3.5. Be submitted to the DoD Senior Information Assurance Officer (SIAO) (i.e. the OASD(NII) DCIO IA Director) as directed.

E4.A3.4. When there is compelling operational necessity DoD information systems 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 as described below.

E4.A3.5. Types of DoD IT Security POA&Ms and Severity Codes

E4.A3.5.1. There are three types of DoD IT Security POA&Ms as reflected in Table E4.A3.1 and further described in paragraphs below.

Table E4.A3.1. Types of DoD IT Security POA&Ms

Report	Responsibility	Submit To	Dates
System Level POA&Ms (Table 2)	Program Managers (PM)/Information Assurance Managers	DoD Component CIO and; DoD SIAO: All systems with a CAT I weakness or on OMB Watch List (Exhibit 300s) for security and others on request	1 Dec, 1 Mar, 1 Jun, 1 Sep
DoD Component level Significant IA Security Weaknesses POA&M (Table 3)	DoD Component CIO	OSD (NII)	1 Dec, 1 Mar, 1 Jun, 1 Sep
DoD Enterprise POA&M	OSD (NII)	OMB	Included in the Oct FISMA Report

E4.A3.5.2. Severity Codes are assigned to a system weakness or shortcoming by a Certification Authority (CA) or his designated representative as part of a certification analysis to indicate (1) the risk level associated with the security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III" where CAT I is the indicator of greatest risk and urgency. CAT I weaknesses shall receive the highest priority for correction or mitigation. Severity codes are assigned after consideration of all possible mitigation measures have been taken within system design/architecture limitations for the DoD information system 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 off-set or mitigated by other protections within hosting enclaves such that the overall risk to the system is reduced to a CAT II.

E4.A3.5.2.1. CAT I weaknesses allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges, and cannot be satisfactorily mitigated. CAT I weaknesses shall be corrected before an Authorization to Operate (ATO) is granted. A system can operate with a CAT I weakness only when the system is critical to military operations and failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. Only the Component CIO shall authorize operation of a system with a CAT I weakness and this can only be done through an Interim Authorization to Operate (IATO). This responsibility cannot be delegated below the Component CIO and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO

E4.A3.5.2.2. CAT II weaknesses are those that can lead to unauthorized system access or activity but can usually be corrected or mitigated to a point where any residual risk is acceptable. CAT II weaknesses must be corrected or satisfactorily mitigated before an ATO can be granted If CAT II weaknesses cannot be corrected or satisfactorily mitigated within the time limitation imposed in the IATO, the DAA must certify in writing that continued system operation is critical to mission accomplishment or terminate system operation. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD Component CIO.

E4.A3.5.2.3. CAT III weaknesses, if corrected, will improve the system's IA posture but do not preclude an authorization to operate. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will show scheduled completion date as N/A, note acceptance by DAA in the milestone column, and risk accepted in the status column.

E4.A3.6. A POA&M shall be prepared for DoD information systems with a current ATO that are found to be operating in an unacceptable IA posture through Government Accountability Office (GAO) audits, IG audits, or other reviews or events, such as an annual security review or compliance validation. An unacceptable IA posture results when the IA Controls compliance posture does not match that authorized by the Accreditation Decision. For example an IA Control is found to be non-compliant or a satisfactory mitigation is not in place, leading to a newly identified weakness. If the DoD information system already has an IT Security POA&M, the newly identified weakness will be added to that documentation.

E4.A3.6.1. If a newly discovered CAT I weakness on a DoD information system operating with an ATO cannot be corrected within 30 days, the system can only continue operation under the terms prescribed in paragraph E4.A3.5.2.1. above.

E4.A3.6.2. If a newly discovered CAT II weakness on a DoD information system 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 paragraph E4.A3.5.2.2. above.

E4.A3.7. 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 PM 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.

E4.A3.7.1. IT Security POA&Ms are permanent records. Weaknesses posted become part of that record and will be updated, but not removed after correction or mitigation actions are completed. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

E4.A3.7.2. Table E4.A3.2. below 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 Identification (ID) and Security Costs which must be filled in from Exhibits 300 and 53, where applicable.

E4.A3.7.3. Once an initial system level IT Security POA&M weakness has been opened, no changes may be made to the data in columns 1 (Weakness), 6 (Scheduled Completion Data), 7 (Milestones with Completion Dates), and 9 (Identified in Chief Financial Officer (CFO) Audit or other Review).

E4.A3.7.4. IT Security POA&Ms listing CAT I or CAT II weaknesses shall be assessed for classification. For instance, the fact that a Mission Assurance Category (MAC) I or II information system 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.

E4.A3.7.5. The following instructions explain how a system level IT Security POA&M should be completed.

E4.A3.7.5.1. Column 1. Type of security weakness. Describe security weaknesses identified during certification or by the annual program review, IG independent evaluation or any other work done by or on behalf of the program office or Component. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the IT Security POA&M should note the fact of its special sensitivity and should be classified accordingly. Where more than one weakness has been identified, number each individual security weakness as shown in the examples.

E4.A3.7.5. Column 2. CAT (Severity Code). Code assigned to a system IA security weakness by a CA as part of certification analysis to indicate (1) the risk level associated with the IA security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III" where CAT I is the indicator of greatest risk and urgency. POA&Ms with CAT I weaknesses will normally be classified.

E4.A3.7.5.3. Column 3. Security Control. An IA Security 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 Security Control are assignable and thus accountable. IA Security Controls are assigned according to MAC (for Integrity and Availability) and Confidentiality Level in accordance with DoDI 8500.2 (reference (g)).

E4.A3.7.5.4. Column 4. POC. Identity of the office or organization that the DoD Component will hold responsible for resolving the security weakness.

E4.A3.7.5.5. Column 5. Resources Required. Estimated funding or manpower (i.e., full time equivalents (FTE)) resources required to resolve the security weakness. Include the anticipated source of funding (i.e., within the system or as a part of a cross-cutting security infrastructure program). Include whether a reallocation of base resources or a request for new funding is anticipated. This column should also identify other, non-funding, obstacles and challenges to resolving the security weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc).

E4.A3.7.5.6. 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." If risk is accepted for a CAT II or CAT III weakness, enter N/A.

E4.A3.7.5.7. Column 7. Milestones with Completion Dates. A milestone will identify specific requirements to correct 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 the Column 8, "Milestone Changes."

E4.A3.7.5.8. Column 8. Milestone Changes. This column would include new completion dates for the particular milestone.

E4.A3.7.5.8. Column 9. Identified in GAO Audit or Other Review. The agency should identify the source (e.g., program review, IG audit, GAO audit, etc.) of the security weakness. Security weaknesses that have been identified as a significant IA security weakness or other reportable condition in the latest agency IG audit under other applicable law (e.g., financial system audit under the Financial Management Integrity Act, etc). If yes is reported, also identify and cite the language from the pertinent audit report.

E4.A3.7.5.10. 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 accepted for a CAT III weakness.

Table E4.A3.2.

Date:	January 17, 2005			**POC Name:**	John Smith		**OMB Project ID:***			
Component Name:	OSD			**POC Phone:**	703-555-5555		009-222334-55874			
System/Project Name:	DoD Network			**POC E-mail:**	john.smith@dod.ctr.mil		**Security Costs:**			
DoD IT Registration No.:							$57,500			
Weakness	**CAT**	**Security Control**	**POC**	**Resources Required**	**Scheduled Completion Date**	**Milestones with Completion Dates**	**Milestone Changes**	**Identified in CFO Audit or other Review**	**Status**	**Comments**
A 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 7/15/2005 due to inadequate funding.	8500.2 Controls Test Conducted 5/15/2005	Ongoing	
Security plan is out of date, more than one year since last update despite new interconnections	II - Security Plan Exists but not up to date.	DCSD-1 Impact High	IAO	$5,000	11/30/2005	Update plan and obtain independent review 11/30/2005		8500.2 Controls Test Conducted 5/15/2005	Ongoing	
Lack of accurate system 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	Completed 10/30/2005
Encryption is not certified FIPS 140-2 compliant.	III	DCNR-1 Impact Medium	IAO	$5,000	5/21/2005	Upgrade encryption software to FIPS 140-2 certified version 5/21/2005		IG Audit 3/21/2005	Ongoing	
Developers have privileged roles on the production system	III	ECPA-1 Impact High	IAO	N/A		Reduce the number of developers having access .		IG Audit 3/21/2005	Risk Accepted	DAA has approved the provided justification for approved developers having access for
Audit application does not audit certain actions.	II	ECAR-2 Impact Medium	IAO	$2,500	9/30/2005	(1) prohibit simultaneous log-ons of SAs and ISSOs, (2) ensure physical logs are maintained, 6/15/2005(3) provide instructions for configuring additional required audits, 7/15/2005and (4) require periodic review of the local authorized users list to ensure its accuracy and currency.9/15/2005		8500.2 Controls Test Conducted 5/15/2006	Ongoing	

SAMPLE

System Level POA&M

*Cite unique project ID and name shown on exhibit 300 and security costs from exhibit 53, if applicable

E4.A3.8. DoD Components are required to complete and submit a DoD Component level IT Security POA&M as indicated in Table E4.A3.3.

E4.A3.8.1. A Component level IT Security POA&M is required for the following:

E4.A3.8.1.1. Systemic weaknesses (significant IA security weaknesses) identified across the Component.

E4.A3.8.1.2. Systemic weaknesses (significant IA security weaknesses) identified by GAO and IG audits and reviews.

E4.A3.8.2. Table E4.A3.3 below contains an example of a completed Component level IT Security POA&M, illustrating the appropriate level of detail required. Once a DoD Component has completed the initial 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).

E4.A3.8.3. The Component level IT Security POA&M should be filled out using the instructions in section E4.A3.7.5 for a system level IT Security POA&M, however, the Security Control column does not apply for a Component level IT Security POA&M.

Date:	March 1, 2005	POC Name:	Mr. Navy CIO				
Component Name:	DON	POC Phone:	555-555-1234				
		POC E-mail:	doncio@nav.mil				
Weakness	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Milestone Changes	Identified in CFO Audit or other Review	Status
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
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
Inconsistent and inadequate personal computer Inventory afloat	Component CIO	500K	10/1/2006	Implement and test afloat computer inventory system 10/1/05		Naval Audit Service	Ongoing
				Enter 50% afloat inventory into database 3/1/06			
				Enter 100% afloat inventory into database 10/1/06			

SAMPLE

Table E4.A3.3
Component Level POA&M

E4.A3.9. The DoD CIO is responsible for completing and submitting a DoD Enterprise IT Security POA&M that will be included in the October FISMA report as indicated in Table E4.A3.1. above. It identifies DoD significant IA security weaknesses that are systemic across the Department. Systemic IA security weaknesses reported on the Enterprise IT Security POA&M are derived from the DoD Component level quarterly significant IA security weakness IT Security POA&Ms, GAO and IG audits, and other reviews and events.

E5. ENCLOSURE 5

DIACAP KNOWLEDGE SERVICE OVERVIEW

E5.1. Introduction. Department of Defense 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 information systems comprising the Global Information Grid (GIG). Because the GIG is an ever-changing entity, DoD IA practitioners tasked with GIG certification 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 Knowledge Service (KS), developed and owned by DoD, 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 and provides convenient access to the DoDI 8500.2 (reference (g)) 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 accessed 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 DoD's official resource for implementing and executing the DIACAP.

E5.2. Purpose. The purpose of the DIACAP Knowledge Service is to provide the 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 Knowledge Service supports both automated and non-automated implementation of the DIACAP.

E5.3. KS Overview. The KS is a library of tools, diagrams, process maps, documents, etc., to support and aid in execution of the DIACAP. It is a collaboration workspace for the DIACAP user community to develop, share and post lessons learned & best practices and a source for IA news and events and other IA-related information resources.

E5.4. DIACAP Technical Advisory Group (TAG). The DIACAP TAG is responsible for maintaining configuration control and management of the online Knowledge Service content. The TAG:

E5.4.1. Provides detailed analysis and authoring support for the enterprise portion of the DIACAP Knowledge Service content.

E5.4.2. Provides configuration control for DIACAP related enterprise services, to include DIACAP Knowledge Service functionality.

E5.4.3. Interfaces with DoD Component IA Programs, GIG Mission Areas, IA COIs, and specialized entities within the IA Domain Governance Structure, see Figure E3.1. DIACAP Enterprise Governance.

E5.4.4. Addresses issues that are common across entities; and recommends changes to the baseline IA Controls and C&A process.

E5.5 Supports the C&A Community. The DIACAP Knowledge Service supports the C&A end user by helping the user to find the most current GIG IA Certification and Accreditation (C&A) guidelines, determine which enterprise level IA Controls apply to a given information system, find implementation guidance and validation procedures and expected results for each IA Control, read about real-world experiences implementing DIACAP, get access to forms, templates and collaborative workspace, and find the latest IA news.

E6. ENCLOSURE 6

DIACAP TRANSITION TIMELINE AND INSTRUCTIONS

DoD INFORMATION SYSTEM C&A STATUS		TRANSITION TIMELINE and INSTRUCTIONS
1	Unaccredited new start or operational DoD Information System (No DITSCAP activity).	Initiate DIACAP.
2	DoD information system has initiated DITSCAP, but does not yet have a signed Phase One System Security Authorization Agreement (SSAA).	Transition to DIACAP immediately.
3	DoD information system 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 DoDI 8500.2 (reference (g)).	Continue under DITSCAP. Within 180 days of this Instruction, modify the DITSCAP SSAA paragraph addressing Re-accreditation Requirements (Paragraph 5.7 in the DoDI 5200.40 SSAA Outline (reference (d)) 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 FISMA reporting requirements. The schedule for transitioning from DITSCAP to DIACAP shall not exceed the system re-accreditation timeline.
4	DoD information system 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 does not incorporate all DoD baseline IA Controls as specified in DoDI 8500.2 (reference (g)).	Continue under DITSCAP. Within 180 days of this Instruction, modify the DITSCAP RTM to incorporate all DoD baseline IA Controls as specified in DoDI 8500.2 (reference (g)) and develop a plan for implementing them. IA Controls implementation timelines 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. Additionally, modify the DITSCAP SSAA paragraph addressing Re-accreditation Requirements (Paragraph 5.7 in the DoDI

DoD INFORMATION SYSTEM C&A STATUS		TRANSITION TIMELINE and INSTRUCTIONS
		5200.40 SSAA outline (reference (d)) to identify the governing DoD Component IA Program and describe the system's strategy and schedule for transitioning to DIACAP, achieving compliance with the DoDI 8500.2 (reference (g)) baseline IA Controls, satisfying the DIACAP Annual Review and meeting FISMA reporting requirements. The schedule for transitioning from DITSCAP to DIACAP shall not exceed the system re-accreditation timeline.
5	DoD information system has a DITSCAP accreditation decision that is current within three years.	Within 180 days of this Instruction, establish a strategy and schedule for transitioning to DIACAP, achieving compliance with the DoDI 8500.2 (reference (g)) baseline IA Controls, satisfying the DIACAP Annual Review and meeting FISMA reporting requirements. If the DITSCAP RTM <u>does not incorporate</u> the baseline DoD IA Controls as specified in DoDI 8500.2 (reference (g)) the DoD information system shall provide the DAA with an assessment of compliance. If the accreditation decision is interim and the system is on a path toward full authorization, continue under DITSCAP as modified by the guidelines of this Table to achieve authorization.
6	DoD information system has a DITSCAP authorization to operate that is more than three years old.	Initiate DIACAP.