



DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

DoD PAAs

23 July 2009

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMBATANT COMMANDERS
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

Subject: DoD Information System Certification and Accreditation Reciprocity

- References: (a) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(c) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(e) through (j), see Attachment 3

The timely deployment of information systems (ISs) is critical to attaining the Department's strategic vision of Net-Centricity. Reciprocity of accreditation decisions and the artifacts contributing to the accreditation decision will advance information sharing, reduce rework and cycle time when establishing Combined/Joint ISs/networks, and support DoD mission accomplishment.

Attachments to this memorandum implement the security terms and conditions for certification and accreditation (C&A) reciprocity in accordance with (IAW) published DoD issuances (references a through h). When implemented within the DoD Information Assurance Certification and Accreditation Process (DIACAP) Enterprise Governance structure (Figure F1, reference e), they will deliver timely reciprocity.

This memorandum defines reciprocity as: "mutual agreement among participating enterprises to accept each other's security assessments in order

to reuse IS resources and/or accept each other's assessed security posture in order to share information.”

Each DoD IS has an assigned Designated Accrediting Authority (DAA) responsible for issuing an accreditation decision based on achieving an acceptable risk posture.

Reciprocity requires a level of trust based upon transparency, uniform processes and a common understanding of expected outcomes.

The DoD mission area Principal Accrediting Authorities (PAAs) endorse the security terms and conditions in attachments 1 and 2 to accelerate deployment of DOD ISs IAW their identified execution schedule. The guidance identified in attachment 1 support the Defense Information System Network/Global Information Grid (DISN/GIG) Flag Panel responsibilities to assess DoD Information Enterprise risk, authorize information exchanges and DoD Information Enterprise connections for ISs IAW DoD Instruction 8510.01 (paragraph 6.2.1.2., reference e). Attachment 1 establishes the security terms and conditions for fostering reciprocity when a DoD IS is deployed as an enterprise solution or Enterprise IS IAW DoD Chief Information Officer (CIO) memorandum (reference f). Under these conditions, the Defense IA Security Accreditation Working Group (DSAWG) will conduct the enterprise security reviews as described in Attachment 1. IS reciprocity decisions made by the DISN/GIG Flag Panel or the DoD PAAs are binding.

DoD Components deploying Non-Enterprise ISs shall follow the security terms and conditions in Attachment 2 to achieve reciprocity.

The connection and net-worthiness requirements for other than security are covered in DoD guidance for interoperability and supportability IAW DoD Directive 4630.05 (reference i). Because they impact a DoD Component's acceptance of a deployed IS, paragraph 2 of Attachment 1 and 2 outline connection and net-worthiness considerations. The guidance provides early visibility and involvement by appropriate DoD Component offices for connection and net-worthiness requirements for IS interoperability and supportability during review process.

ISs developed by and deployed within a single DoD Component are not subject to the reciprocity issue addressed in this memorandum. The developing/hosting component DAA solely establishes criteria, accepts the risk and grants access to those ISs.

Nothing in this document shall alter or supersede the authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for

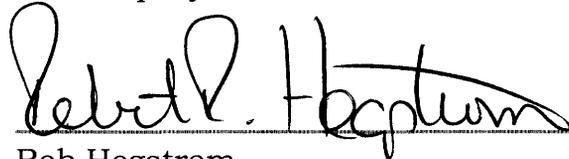
intelligence as directed by Executive Order 12333 and other laws and regulations.

This memorandum and attachments will be posted to the DIACAP Knowledge Service.

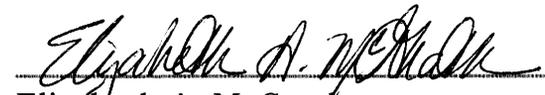
Signed:



David M. Wennergren
DoD Deputy Chief Information Officer



Rob Hegstrom
Director, Battlespace Awareness
Portfolio



Elizabeth A. McGrath
Assistant Deputy Chief Management
Officer



Nancy E. Brown
Vice Admiral, USN
Director for Command, Control,
Communications and Computer
Systems

Attachments:
As stated

ATTACHMENT 1

Attachment 1 describes the security terms and conditions to achieve reciprocity when a DoD Component deploys an Enterprise IS across the DoD Information Enterprise and receiving DoD Components.

1. C&A Supporting Security Terms and Conditions

a. Deploying DoD Component. The deploying DoD Component DAA shall ensure the following are accomplished by the Component's DIACAP Team:

(1) Prepare the system identification profile (SIP), DIACAP Implementation Plan (DIP) and list of deployment sites and dates.

(2) Reposit the IS's DIACAP package through use of or export¹ to the Enterprise Mission Assurance Support System (eMASS) SIPRNET instantiation to provide visibility to DSAWG.

(3) Conduct certification activities.

(a) Use the evaluation/validation procedures and expected outcomes published in the DIACAP Knowledge Service (<https://diacap.iaportal.navy.mil/>).

(b) Ensure security tests and evaluations address the additional receiving Component IA controls for the IS identified during the DSAWG enterprise security reviews.

(c) Document the compliance status of IA controls in the IS's DIACAP Scorecard and ensure an Information Technology (IT) Security Plan of Action and Milestones (POA&M) is generated IAW DoD Instruction 8510.01 (reference e).

(4) Resolve requested adjustments to the IS's assigned IA controls including planned inheritable controls identified during the DSAWG enterprise review process.

(5) Ensure the evaluation/validation of the IS's IA controls is performed by certified IA professionals IAW DoD Directive 8570.01 (reference h).

(6) Register the IS in the DoD Vulnerability Management System (VMS) for enterprise-level vulnerability management.

¹ DoD Components may have invested in other commercial capabilities to manage C&A activities within their components for ISs; however a copy of DIACAP package will be exported to the SIPRNET eMASS instantiation for DoD Enterprise visibility.

(7) Ensure the IS complies with the Information Assurance Vulnerability Management (IAVM) Program and operational orders (e.g., alerts, bulletins and Communication Tasking Orders (CTOs)).

(8) Provide installation and configuration requirements documentation prior to IS deployment including applicable DoD Security Technical Implementation Guides (STIGs) and IS compliance status.

(9) Register the IS in the DoD Ports, Protocols and Services Registry.

(10) Issue an accreditation decision for the IS and version being deployed.

b. Receiving DoD Component shall:

(1) Maintain situational awareness of the certification activities through the DSAWG security review process.

(2) Make available the receiving site's DIACAP package if requested by the DoD Component deploying the IS.

(3) Identify issues (e.g. requests for adjustments to the assigned IA controls) that will preclude the IS from connecting through their DSAWG representative.

(4) Upon Approval of an Enterprise IS take the following actions:

(a) Issue authorization to connect and operate the IS.

(b) Provide copy of implementing documentation (e.g., "authorization to connect") to deploying DoD Component DAA.

(c) Notify subordinate site(s) that the IS is authorized to operate and/or connect only in the accredited configuration.

(d) Update enclave accreditation and/or connection documentation to reflect the incorporation/connection of the Enterprise IS.

(4) Ensure IS installation guide and applicable DoD security configuration requirements are implemented.

(5) Implement IA controls (including inherited controls) and DoD Component-specific augmenting IA controls.

(6) Ensure that mitigations are maintained in accordance with the deploying IS IT Security POA&M.

c. DoD Enterprise IS Approval Process (Table 1)

(1) The DoD Component deploying the IS shall submit a request for a security review prior to beginning engineering and manufacturing development. For ISs under the Defense Acquisition Management Program this is Milestone A and for other ISs this is 9-12 months prior to planned deployment.

(a) The request will be forwarded to the DSAWG through the DoD Component DSAWG representative.²

(b) The DoD Component deploying the IS shall provide the DSAWG an electronic copy of the SIP, DIP, list of deployment sites and dates and initial overview briefing on IS.

(2) During the engineering and manufacturing development phase,³ the DoD Component deploying the IS shall:

(a) Reposit the DIACAP Package through use of or export⁴ to the eMASS SIPRNET instantiation to provide visibility to DSAWG.

(b) Provide a C&A status brief to the DSAWG. The DSAWG will identify any security issues requiring resolution before their recommendation is forwarded to the DISN/GIG Flag Panel for approval.

(3) No later than 60 working days prior to deployment the DoD Component deploying the IS shall brief the DISN GIG Flag Panel. The DISN/GIG Flag Panel shall approve or disapprove IS connection based on DSAWG recommendation(s) and a determination that the risk to the DoD Information Enterprise is acceptable and provide guidance to DoD Components.

(4) DISN/GIG Flag Panel approval. Approval will not be posted until actions (if any) directed by the DISN/GIG Flag Panel to mitigate remaining risk have been accomplished and documented in the IT Security POA&M.

d. Reciprocity Implementation Documentation. The DISN/GIG Flag Panel's risk decision is an authority to connect. The DISN/GIG Flag Panel decision:

² <http://iase.disa.smil.mil/dsawg/membership.html>. Combatant Commands will forward requests through the Joint Staff DSAWG representative. DoD agencies or activities without a DSAWG representative will forward requests through appropriate Principal Staff Assistant (e.g., OASD(NII), USD(I) etc.).

³ For ISs under the Defense Acquisition Management Program this is after entering Milestone B IAW the Milestone B fielding schedule and for other ISs this is 4-6 months prior to planned deployment.

⁴ DoD Components may have invested in other commercial capabilities to manage C&A activities within their components for ISs; however a copy of DIACAP package will be exported to the SIPRNET eMASS instantiation for DoD Enterprise visibility.

(1) Accepts/sanctions the originating DAA's accreditation decision.

(2) Accepts the residual risk for DoD Components receiving the IS and authorizes its connection to the DoD Information Enterprise.

(3) Means that a separate accreditation decision for the Enterprise IS will not be issued. The accreditation decision/documentation for the enclave(s) hosting the Enterprise IS (i.e., AIS application) shall be updated as required.

(4) Means that IA controls will not be tested for recertification.

2. Connection And Net-Worthiness Requirements

a. The timeliness of reciprocity is often influenced by connection and net-worthiness requirements of the entity hosting or providing a connection to the deploying IS. Connection and net-worthiness requirements include interoperability and supportability issues other than security which have an impact on network operations. These may include local connection approval processes, interconnection standards, infrastructure services compatibility, architecture compliance and validity, bandwidth, TEMPEST, and other issues bearing upon the operation of the IS in a local operating environment.

b. The following guidance is consistent with DoD Directive 4630.05 (reference i) and DoD Instruction 4630.8 (reference j) and are designed to complement the C&A supporting security terms and conditions in paragraph 1. The purpose is to provide early visibility on connection and net-worthiness requirements and eliminate unnecessary delays in accepting deploying systems due to unaddressed interoperability or supportability issues.

(1) Following an Enterprise IS request to the DSAWG, a list⁵ of DoD Component points of contact (POCs) for connection and net-worthiness requirements will be provided to the deploying DoD Component.

(2) The deploying DoD Component ensures that:

(a) The receiving DoD Component connection and net-worthiness POCs are contacted to identify connection and net-worthiness requirements and processes for interoperability and supportability.

(b) The information support plan⁶ developed IAW DOD Directive 4630.05 (reference i) and DOD Instruction 4630.8 (reference j) is available for

⁵ DSAWG representatives will provide Component POCs for connection and net-worthiness requirements.

⁶ Information on the ISP can be found at the following Defense Acquisition University link <https://acc.dau.mil/CommunityBrowser.aspx?id=28935>.

review by receiving DoD Component connection and net-worthiness offices and/or points of contact.

(c) The receiving DoD Component connection and net-worthiness requirements for other than security are managed and resolved IAW DoD Directive 4630.05 (reference i) and DoD Instruction 4630.8 (reference j).

(3) The receiving DoD Component DSAWG representative(s) will notify the DSAWG of unresolved connection and net-worthiness requirements upon receipt of the C&A status brief during the engineering and manufacturing development phase.

(4) Unresolved connection and net-worthiness issues attributed to IA control(s) will be immediately elevated to the DSAWG, the DISN/GIG Flag Panel when it becomes evident that resolution cannot be attained at the DAA level.

3. Disputes

a. DoD Component security issues related to C&A, IA controls, connection or operation will be resolved at lowest level possible. Unresolved connection and net-worthiness issues attributed to IA control(s) will be forwarded to the DSAWG by DoD Component DSAWG representatives.

b. Connection and Net-Worthiness Disputes. Non-Security connection or net-worthiness deficiencies or corrective actions that cannot be resolved shall be forwarded to the Assistant Secretary of Defense/DoD Chief Information Officer (ASD(NII)/DoD CIO) for review by the Interoperability Senior Review Panel (ISRP) IAW DoD Instruction 4630.8 (reference j).

4. Post DoD Information Enterprise Connection Approval Life-Cycle Management

a. DSAWG. Following DISN/GIG Flag Panel connection approval, an IS shall only require further DSAWG security reviews if:

(1) DSAWG member requests review based on new security issues identified.

(2) Notification of “block release” or “version” of deployed IS, web services/ Service Oriented Architecture Capabilities. DSAWG may review and approve “block release” or “version” of the deployed IS, web services/ Service Oriented Architecture Capabilities as delegated by DISN/GIG Flag Panel.

b. DISN/GIG Flag Panel. Following the DISN/GIG Flag Panel connection approval, an IS shall only require further Enterprise IS security reviews at the request of the DSAWG.

Steps #	Timeframe	Deliverables Available	Expected Outcome
1 Enterprise IS Request and Overview Briefing	<ul style="list-style-type: none"> • Prior to end of Milestone A (For IS subject to DoD Directive 5000.01 reference a)) • For all other ISs 9-12 months before deployment 	<ul style="list-style-type: none"> • Draft/approved DIP w/ SIP. • DITPR Registration number • Proposed deployment sites & dates • Draft/approved Classification guide (if processing classified information) • Proposed IS architecture • Proposed Vulnerability Management Plan • Initial IS overview brief 	The DSAWG will provide a written summation of the review of the IS deliverables, overview brief, and any recommended actions to be completed prior to the DSAWG review.
2 DSAWG Review	<ul style="list-style-type: none"> • After entering Milestone B IAW Milestone B fielding schedule (for IS under DoD Directive 5000.01 (reference a)) • For all other ISs: 4-6 months before deployment 	<ul style="list-style-type: none"> • SIP • DIACAP Scorecard • IT Security Plan of Action with Milestones • Summary of certification results and Certification Recommendation signed by the Certification Authority • eMASS unique identifier to indicate completion of registration requirements • Information Support Plan (ISP) • Revised deployment sites & dates • Updated IS architecture • Confirmation of DoD Ports, Protocols and Services registration • Confirmation of registration in VMS • Brief to the DSAWG 	The DSAWG will provide a written summation of the DSAWG Review and any recommended actions to be completed prior to the DISN/GIG Flag Panel Review.
3 DISN/GIG Flag Panel Review & Decision	<ul style="list-style-type: none"> • 60 working days prior to initial deployment 	<ul style="list-style-type: none"> • Completed DIACAP Package • Statement of Accreditation Decision for the IS • Status of IT Security POA&M • Brief to the DISN/GIG Flag Panel 	The DISN/GIG Flag Panel Secretariat will provide a written summation of the DISN/GIG Flag Panel results to IS owner and DSAWG.
4 (As required by the DISN/GIG Flag Panel)	Timeframe will be identified by the DISN/GIG Flag Panel	Deliverables to the Flag Panel may consist of a revised Flag Panel brief and progress review of the IT Security POA&M. Initial Review to be conducted by the DSAWG.	The DSAWG will provide a written summation of the results to IS owner and the DISN/GIG Flag Panel Secretariat. The summary will include the recommendation to the DISN/GIG Flag Panel.

Table 1. Enterprise IS Security Reviews

ATTACHMENT 2

Attachment 2 describes the security terms and conditions to achieve reciprocity for Non-Enterprise IS.

1. C&A Supporting Security Terms and Conditions

a. Deploying DoD Component. The deploying DoD Component DAA shall ensure the following are accomplished by the Component's DIACAP Team:

(1) Prepare the SIP, DIP and list of deployment sites and dates.

(2) Provide access to the IS's DIACAP package as agreed to by DoD Components.

(3) Conduct certification activities.

(a) Use the evaluation/validation procedures and expected outcomes published in the DIACAP Knowledge Service (<https://diacap.iaportal.navy.mil/>).

(b) Ensure security tests and evaluations address the additional receiving Component IA controls for the IS identified during the Component level security reviews.

(c) Document the compliance status of IA controls in the IS's DIACAP Scorecard; and ensure an IT Security POA&M is generated IAW DoD Instruction 8510.01 (reference e).

(4) Resolve requested adjustments to the IS's assigned IA controls including planned inheritable controls identified during DoD Component security reviews.

(5) Ensure the evaluation/validation of IS's IA controls is performed by certified IA professionals IAW DoD Directive 8570.01 (reference h).

(6) Register IS in the DoD VMS for enterprise-level vulnerability management.

(7) Ensure the IS complies with IAVM Program and operational orders (e.g., alerts, bulletins and CTOs).

(8) Provide installation and configuration requirements documentation prior to IS deployment including applicable DoD STIGs and IS compliance status.

(9) Register the IS in the DoD Ports, Protocols and Services Registry.

(10) Issue an accreditation decision for the IS and version being deployed.

b. Receiving DoD Component shall:

(1) Maintain situational awareness of the certification activities through the DoD Component POCs.

(2) Make available the receiving sites' DIACAP package if requested by the DoD Component deploying the IS.

(3) Identify issues (e.g. requests for adjustments to the assigned IA controls) that will preclude the IS connecting through their Component POC.

(4) Upon receipt of accreditation decision take the following actions:

(a) Issue authorization to connect and operate the IS.

(b) Provide copy of implementing documentation (e.g. "authorization to connect") to deploying DoD Component DAA.

(c) Notify subordinate site(s) that IS is authorized to operate and/or connect only in the accredited configuration.

(d) Update enclave accreditation and/or connection documentation to reflect the incorporation/connection of the IS.

(5) Ensure IS installation guide and applicable DoD security configuration requirements are implemented.

(6) Implement IA controls (including inherited controls) and DoD Component-specific augmenting IA controls.

(7) Ensure that mitigations are maintained in accordance with the deploying IS IT Security POA&M.

c. Non-Enterprise IS Approval Process (Table 2)

(1) The DoD Component deploying the IS shall submit a request for a security review prior to beginning engineering and manufacturing development. For ISs under the Defense Acquisition Management Program this is Milestone A and for other ISs this is 9-12 months prior to planned deployment.

(a) The request will be forwarded to the receiving DoD Component(s) single point of contact.

(b) The DoD Component deploying the IS shall provide the receiving DoD Component(s) single point of contact an electronic copy of the SIP, DIP and deployment sites/schedule.

(2) During the engineering and manufacturing development phase,⁷ the DoD Component deploying the IS shall:

(a) Provide visibility of the DIACAP Package as agreed to by DoD Components.

(b) Provide C&A status to the receiving DoD Component. The receiving DoD Component single point of contact will identify any security issues requiring resolution before recommendation is forwarded to the DoD Component DAA.

(3) No later than 60 working days prior to deployment the DoD Component deploying the IS shall provide status to the receiving DoD Component single point of contact. The receiving DoD Component DAA shall approve or disapprove the IS's connection based on determination that the risk to the DoD Component's networks is acceptable and provide guidance to DoD Component sites.

d. Reciprocity Implementation Documentation. The receiving DoD Component's DAA risk decision is an authority to connect. The Receiving DAA decision:

(1) Accepts/sanctions the originating DAA's accreditation decision.

(2) Assesses and accepts the residual risk for the DoD Component enclaves receiving the IS and authorizes its connection to the Component network.

(3) Means the accreditation decision/documentation for the enclave(s) hosting the Non-Enterprise IS (i.e., AIS application) shall be updated as required.

(4) Means that IA controls will not be tested for recertification.

2. Connection And Net-Worthiness Requirements

a. The timeliness of reciprocity is often influenced by connection and net-worthiness requirements of the entity hosting or providing a connection to the deploying IS. Connection and net-worthiness requirements include interoperability and supportability issues other than security which have an

⁷ For ISs under the Defense Acquisition Management Program this is after entering Milestone B IAW the Milestone B fielding schedule and for other ISs this is 4-6 months prior to planned deployment.

impact on network operations. These may include local connection approval processes, interconnection standards, infrastructure services compatibility, architecture compliance and validity, bandwidth, TEMPEST, and other issues bearing upon the operation of the IS in a local operating environment.

b. The following guidance is consistent with DoD Directive 4630.05 (reference i) and DoD Instruction 4630.8 (reference j) and are designed to complement the C&A supporting security terms and conditions in paragraph 1. The purpose is to provide early visibility on connection and net-worthiness requirements and eliminate unnecessary delays in accepting deploying ISs due to unaddressed interoperability or supportability issues.

(1) The receiving DoD Component POC will notify the deploying DoD Component of connection and net-worthiness requirements for interoperability and supportability upon receipt of initial reciprocity request.

(2) The deploying DoD component ensures that:

(a) The receiving DoD Component connection and net-worthiness POCs are contacted to identify connection and net-worthiness requirements and processes for interoperability and supportability.

(b) The information support plan⁸ developed IAW DOD Directive 4630.05 (reference i) and DOD Instruction 4630.8 (reference j) is available for review by the receiving DoD Component connection and net-worthiness offices and/or points of contact.

(c) The receiving DoD Component connection and net-worthiness requirements for other than security are managed and resolved IAW DoD Directive 4630.05 (reference i) and DoD Instruction 4630.8 (reference j).

(3) Unresolved connection and net-worthiness issues attributed to IA control(s) will be immediately elevated to the DSAWG or DISN/GIG Flag Panel, when it becomes evident that resolution is not attainable at the DAA level.

3. Disputes

a. DoD Component security issues related to C&A and IS connection or operation for deployment will be resolved at the lowest level possible as part of the receiving DoD Component review process. Unresolved connection and net-worthiness issues attributed to IA control(s) will be forwarded to the DSAWG for review.

⁸ Information on the ISP can be found at the following Defense Acquisition University link <https://acc.dau.mil/CommunityBrowser.aspx?id=28935>.

b. Connection and Net-Worthiness Disputes. Non-security connection or net-worthiness deficiencies or corrective actions that cannot be resolved shall be forwarded to the Assistant Secretary of Defense/DoD Chief Information Officer (ASD(NII)/DoD CIO) for review by the Interoperability Senior Review Panel (ISRP) IAW DoD Instruction 4630.8 (reference j).

4. Post Non-Enterprise Connection Approval Life-Cycle Management. Following DoD Component connection approval, an IS's shall only require further reciprocity security reviews, if a DoD Component single point of contact requests review based on new security issues.

Step #	Timeframe	Deliverables for Review	Expected Outcome
1 Request	<ul style="list-style-type: none"> • Prior to end of Milestone A (For IS subject to DoD Directive 5000.01 (reference a)) • For all other ISs 9-12 months before deployment 	<ul style="list-style-type: none"> • Draft/approved DIP w/ SIP. • DITPR Registration number • Proposed deployment sites and dates • Draft/approved classification guide (if processing classified information) • Proposed IS architecture • Proposed Vulnerability Management Plan 	The receiving DoD Component(s) will acknowledge receipt of reciprocity request and identify any requirements (e.g., net-worthiness or connection) to be completed prior to step review.
2 Review	<ul style="list-style-type: none"> • After entering Milestone B IAW Milestone B fielding schedule (for IS under DoD Directive 5000.01 (reference a)) • For all other ISs: 4-6 months before Deployment 	<ul style="list-style-type: none"> • SIP • DIACAP Scorecard • IT Security Plan of Action with Milestones • Summary of certification Results and Certification Recommendation signed by the Certification Authority • ISP • Revised deployment sites and dates • Updated IS architecture • Confirmation of DoD Ports, Protocols and Services registration • Confirmation of registration in VMS 	The receiving DoD Component(s) will identify any remaining security and/or deployment issues, constraints, or limitations to be completed prior to approval.
3 Approval	<ul style="list-style-type: none"> • 60 working days prior to initial Deployment 	<ul style="list-style-type: none"> • Completed DIACAP Package • Statement of Accreditation Decision for the IS • Status of IT Security POA&M 	The receiving DoD Component(s) will provide written approval based on review to IS owner and to the DoD Component DAA.

Table 2. DoD Component Non-Enterprise Security Review

ATTACHMENT 3

References

(e) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007

(f) DoD CIO Memorandum, "DoD Enterprise Services Designation – Collaboration, Content Discovery, and Content Delivery," February 2, 2009

(g) Chairman, Joint Chiefs of Staff Instruction 6211.02C, "DISN Policy and Responsibilities," November 12, 2007

(h) DoD Directive 8570.01, "Information Assurance Training, Certification and Workforce Management," August 15, 2004

(i) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004

(j) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004

ATTACHMENT 4

DEFINITIONS

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. 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); 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, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application;" however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System. (DoD Directive 8500.01E)

DoD Information Enterprise. The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoD Directive 8000.01)

Enterprise IS. An AIS Application as defined in DoD Directive 8500.1 that is designed to satisfy a DoD-wide requirement and is deployed to multiple DoD Components across the DoD Information Enterprise. Note: An Enterprise IS is normally the product of an ACAT 1 (MDAP or MAIS) acquisition program but may also include AIS Application acquisitions below the MAIS threshold if they meet the foregoing criteria.

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. (DoD Directive 8500.01E)

Non-Enterprise IS. An AIS Application that is deployed to two or more DoD Components, but is not designated an Enterprise IS.