

DEPARTMENT OF DEFENSE CERTIFICATION AND ACCREDITATION (DIACAP) PROCESS

A NOVA DATACOM WHITEPAPER

INTRODUCTION

All Department of Defense (DoD) information systems (IS) MUST be certified and accredited per the guidance in Department of Defense Instruction (DoDI) 8510.01, dated November 28, 2007.

The process described in this instruction is the Department of Defense Certification and Accreditation Process (DIACAP).

The DIACAP is a complex and lengthy process that is completed in five phases. This process can take months, or even years, depending on the size of the IS, the competence of the DIACAP team, and the availability and competence of the personnel responsible for completing the different aspects of the DIACAP process.

However, just because your IS is accredited does not mean that you can connect to the DoD. Once your IS is accredited, you must then request an Authority to Connect (ATC) before you can connect to the DoD.

The DIACAP defines the following activities for the certification and accreditation of a specific DoD Information System. These activities may occur concurrently or sequentially, or at varied frequencies for different Information Assurance (IA) controls. The DIACAP parallels the system life cycle, and its activities should be initiated at inception. However, failure to initiate the DIACAP at system inception is not a justification for ignoring or non-complying with the DIACAP. Regardless of the system life cycle stage, unaccredited systems shall initiate the DIACAP immediately. The implementation of IA and services will be less expensive and problematic if the DIACAP is initiated early in the system life cycle.

The entire DIACAP process is described below. The five phases of the DIACAP will be discussed followed by a discussion describing the process for obtaining the ATC.

Note: As of 1 July 2009, no further Department of Defense Information Technology Certification and Accreditation Program (DITSCAP) documents will be accepted.

PHASE 1:

INITIATE AND PLAN INFORMATION ASSURANCE (IA) CERTIFICATION AND ACCREDITATION (C&A)

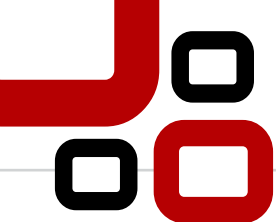
This activity includes registering the system with the governing Department of Defense (DoD) Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIACAP Implementation Plan (DIP).

Register the System with the DoD IA Program

System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. DIACAP registration facilitates organizational Information Technology (IT) management and Federal Information Security Management Act of 2002 (FISMA) reporting. It involves recording descriptive system acquisition and information assurance data in a manner as to allow unique system identification. Registration commences a dialog between the DoD information system owner and the DoD Component Chief Information Officer (CIO), which should continue until the DoD information system is decommissioned.

The set of information gathered during system registration is referred to as the System Identification Profile (SIP), which becomes part of the DIACAP package for the information system, and is

"All Department of Defense (DoD) information systems (IS) MUST be certified and accredited per the guidance in Department of Defense Instruction (DoDI) 8510.01, dated November 28, 2007."



maintained throughout the system's life cycle. The SIP identifies the minimum data requirements, plus explanations, for registering an information system with the Component. Typically, this information can be found in program/project documentation, such as the initial capabilities document, system requirements/specifications, architecture and design documents, etc.

Assign IA Controls

Identifying the baseline DoD Enterprise IA controls that apply to a particular IS is a critical DIACAP implementation activity. To execute this activity, an appropriate MAC and CL must be established for each IS. DoD Instruction 8500.2, "Information Assurance Implementation," identifies IA control sets applicable to a system specific MAC and CL designation. A DoD Component CIO, Mission Area (MA) Designated Approval Authority (DAA), local system DAA or official DoD Community of Interest (COI) representative may add additional IA controls, to locally augment the security stringency of baseline control set, only when the augmented controls increase the security stringency established by the enterprise baseline IA controls.

The baseline IA control sets are taken from DoDI 8500 - 2 IA Control Checklists. There are approximately 240 baseline IA controls that are taken from DoDI 8500 - 2. Further, there are additional augmented controls that are taken from the various regulations such as Army Regulation 25 - 2 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS). Generally speaking, there are hundreds of IA controls associated with the DIACAP process for an IS.

Assemble the DIACAP Team

The members of the DIACAP Team are required to meet the trustworthiness investigative levels for users with IA management access to DoD unclassified ISs. Senior Information Assurance Officers (SIAOs) shall meet the same investigative requirements as those for DAAs, and certification cadre members shall meet the same requirements as those established for monitoring and testing.

The DIACAP team members and their respective roles are identified below:

Designated Approval Authority (DAA) – The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority. The DAA is designated by the Principal Accrediting Authority (PAA) or the Heads of DoD Components, and is responsible for authorizing or denying the operation (or the testing) of the assigned DoD IS by issuing an accreditation decision. The possible accrediting decisions are: 1) Authority To Operate (ATO), 2) Interim Authority To Operate (IATO), 3) Interim Authority To Test (IATT), and 4) Denial of Authority To Operate (DATO). A DAA bases this decision on a recommendation of the Certifying Authority (CA), accompanied by supporting material from the DIACAP Comprehensive Package. A DAA may downgrade or revoke an accreditation decision any time risk conditions or concerns so warrant.

In addition to the responsibilities established in DoDI 8500.2, a DAAs is also expected to:

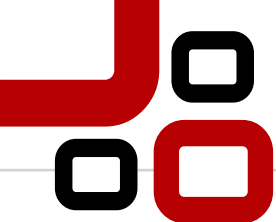
- ❑ *Comply with Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel direction issued on behalf of the GIG MA PAAs.*
- ❑ *Ensure a DIACAP package is initiated and completed for assigned ISs.*
- ❑ *Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.*
- ❑ *Ensure security classification guides are established according to DoD 5200.1 - R.*
- ❑ *Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.*

Senior Information Assurance Officer (SIAO) – The Senior Information Assurance Officer is the official responsible for directing an organization's IA program on behalf of the organization's CIO. SIAOs are appointed by Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD CIO to direct and coordinate the DoD IA Program.

The SIAO has the following responsibilities:

- ❑ *Establish and enforce the C&A process within the DoD Component IA program.*
- ❑ *Ensure DoD Component - level participation in the DIACAP Technical Advisory Group (TAG).*

"Information Assurance Implementation,' identifies IA control sets applicable to a system specific MAC and CL designation."



- ❑ *Track the C&A status of ISs that are governed by the DoD Component IA program.*
- ❑ *Establish and manage a coordinated IA certification process for ISs governed by the DoD Component IA program. This includes functioning as the CA or formally delegating CA for governed ISs.*
- ❑ *Identifying and recommending changes and improvements to certification and validation procedures to the TAG for inclusion in the DIACAP Knowledge Service (KS).*
- ❑ *Ensuring that DoD Component certification guidance is posted to the DoD Component portion of the KS.*
- ❑ *Serve as the single IA coordination point for joint or Defense - wide programs that are deploying ISs to DoD Component enclaves.*
- ❑ *Comply with DISN/GIG Flag Panel direction issued on behalf of the GIG MA PAAs.*
- ❑ *Ensure a DIACAP package is initiated and completed for assigned ISs.*
- ❑ *Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.*
- ❑ *Ensure security classification guides are established according to DoD 5200.1 - R (Reference (n)).*
- ❑ *Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.*

Certification Authority (CA) – The CA is the senior official having the authority and responsibility for the certification of all information systems governed by a DoD Component IA Program, and may designate a Certifying Agent to act on behalf of the Certifying Authority. The CA has the authority to formally evaluate the IA capabilities and services of a DoD information system and issue a Certification Determination. This determination accompanies the DIACAP package for review by the DAA towards an accreditation decision. The CA continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts. The SIAO functions as the CA and formally appoints CA Representatives for all governed ISs.

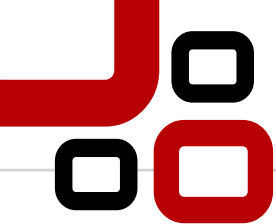
Program Manager (PM)/System Manager (SM) – A Program or System Manager is the official responsible for and authority to accomplish program or system objectives for development, production and sustainment to meet the user’s operational needs. Additionally, the PM serves as the focal point for the integration of IA into and throughout the system life cycle of an assigned DoD Information System.

The responsibilities of the PM/SM are:

- ❑ *Ensure that each assigned DoD IS has a designated IA manager (IAM) with the support, authority, and resources to satisfy the responsibilities established in DoDI 8500.01.*
- ❑ *Implement the DIACAP for assigned DoD ISs.*
- ❑ *Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.*
- ❑ *Ensure that information system security engineering is employed to implement or modify the IA component of the system architecture in compliance with the IA component of the GIG Architecture and to make maximum use of enterprise IA capabilities and services.*
- ❑ *Enforce DAA accreditation decisions for hosted or interconnected DoD ISs.*
- ❑ *Develop, track, resolve, and maintain the DIACAP Implementation Plan (DIP) for assigned DoD ISs.*
- ❑ *Ensure IT Security Plan Of Action & Milestones (POA&M) development, tracking, and resolution.*
- ❑ *Ensure annual reviews of assigned ISs required by FISMA are conducted.*

Information Assurance Manager (IAM) – The IAM is responsible for the overall information assurance program of a DoD information system or organization. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore IA posture.

- ❑ *Support the PM or SM in implementing the DIACAP.*



- ❑ *Advise and inform the governing DoD Component IA program on DoD ISs Certification & Accreditation (C&A) status and issues.*
- ❑ *Comply with the governing DoD Component IA program information and process requirements.*
- ❑ *Provide direction to the IA Officer (IAO).*
- ❑ *Coordinate with the organization's Security Manager to ensure issues affecting the organization's overall security are addressed appropriately.*

User Representative – The DoD Information System User Representative is the individual or organization that represents the user community for a particular system during the certification and accreditation process.

The User Representative is responsible for:

- ❑ *Represent the operational interests of the user community in the DIACAP.*
- ❑ *Support the IA controls assignment and validation process to ensure user community needs are met.*

Initiate the DIACAP Implementation Plan (DIP)

The DIACAP Implementation Plan contains both the strategy for implementation along with the current implementation status of assigned IA controls for a system. Specifically, this includes the Information System's assigned IA controls including inherited IA controls. The plan is part of the DIACAP package used by both the certifying authority and the designated accrediting authority for accreditation, and should be consistent with the program schedules.

The DIACAP Implementation Plan should contain the following, minimum information:

- ❑ *Assigned IA controls -inherited and implemented*
- ❑ *Implementation Status*
- ❑ *Responsible entities*
- ❑ *Resources*
- ❑ *Estimated completion date for each IA control*

Completing the DIP can be very time consuming – especially when trying to identify and contact the responsible entities. These are the people who are responsible for supervising, managing, or completing the various portions of the IA controls. Between vacations, business trips, meetings, etc., sometimes the DIP process can add significant additional time to the completion of the DIACAP.

PHASE 2:

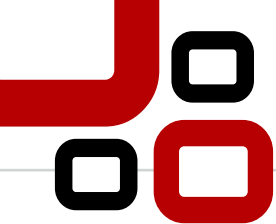
IMPLEMENT AND VALIDATE ASSIGNED IA CONTROLS

This activity includes executing the DIP, conducting validation activities, preparing the IT Security POA&M, and compiling the validation results in the DIACAP Scorecard.

Execute the DIP

This activity includes all tasks related to the execution and resulting update of the DIACAP Implementation Plan, which describes the strategy and current status of the implementation of IA Controls for an information system. Each assigned IA Control is implemented according to the applicable implementation guidelines, which can be found in the description for an IA Control through the IA Controls section of the KS.

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. The process of updating and maintaining a current reflection of the information system's IA posture should be continued throughout the system's life cycle. The DIP will continue to be updated as security relevant events impact the system's status.



Conduct Validation Activities

Validation includes all tasks related to the execution of the validation procedures that are associated with assigned IA controls. For each IA control, one or more validation procedures have been developed which describe requisite preparatory steps and conditions, actual validation steps and expected results. Each procedure includes associated supporting background material, sample results, or links to automated testing tools. Validation procedures are maintained by the DIACAP TAG and published in the IA controls section of the DIACAP KS.

Actual results of the validation procedures are recorded according to the criteria and protocols specified in each procedure and are made a permanent part of the extended DIACAP package, along with any artifacts produced during the validation (e.g., output from automated test tools or screen shots that depict aspects of system configuration). For inherited IA controls, validation test results and supporting documentation are maintained by the originating IS and are made available to CAs of receiving ISs by request. Upon completion of the validation procedures, a POA&M is initiated to document non-compliance results and non applicable IA controls, if necessary. For any identified IA weakness, an associated Severity Category is assigned by the CA (and documented within the POA&M) to indicate the likelihood of the weakness being exploited.

The status of actual results for all assigned Validation Procedures is compiled into a DIACAP Scorecard. The status of assigned IA controls are indicated on the Scorecard as:

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

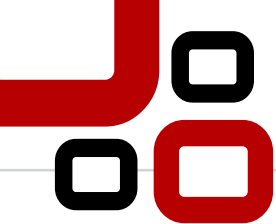
Non - Compliant (NC). IA controls are those for which one or more expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.

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

Prepare an IT Security POA&M

The purpose of an IT Security POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities. The Office of Management and Budget (OMB) requires agencies to prepare IT Security POA&Ms for all programs and systems where an IT security weakness has been found. The IT Security 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. The DoD is responsible for maintaining the confidentiality of IT Security POA&Ms because they may contain pre-decisional budget information. The IT Security 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. This section provides the instructions for filling out both the System level IT Security POA&M and the Component level IT Security POA&M.

IT Security POA&Ms are permanent records. Once posted, weaknesses will be updated, but not removed, after correction or mitigation actions are completed. Inherited weaknesses are reflected on the IT Security POA&Ms. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA, the SIAO, and the governing DoD Component CIO. In order to reflect the complete IA posture of a DoD IS at all times in a single document, the IT Security POA&M is also used to docu-



ment DAA - accepted NC IA controls and baseline IA controls that are NA because of the nature of the system.

DoD IT Security POA&Ms shall:

- ❑ *Be tied to the agency's budget submission when required through the project identifier(s) of the system. This links the security costs with security performance. OMB Circular No. A - 11 requires that agencies develop and submit to OMB business cases for major IT investments. Additionally, each agency submits a list of both major and non - major IT investments. The agency assigns a project identifier(s) to each investment and includes it with these exhibits.*
- ❑ *Address all IT security weaknesses, including but not limited to those found during Government Accountability Office (GAO) audits, financial system audits, official security tests and evaluations or compliance reviews, and critical infrastructure vulnerability assessments.*
- ❑ *Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.*
- ❑ *Follow the format detailed below that is consistent with the examples provided by OMB.*
- ❑ *Be submitted to the DoD SIAO when directed.*

DIACAP Scorecard

The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD Public Key Infrastructure (PKI) - certified digital signature. The DIACAP Scorecard contains a listing of all IA controls and their status of either C, NC, or NA.

Compliant (C) IA controls are those for which the expected results for all associated validation procedures have been achieved. Non - compliant (NC) IA controls are those for which one or more of the expected results for all associated validation procedures are not achieved. Not applicable (NA) IA controls are those that do not impact the IA posture of the IS as determined by the DAA.

All IA controls are labeled compliant, non - compliant, or not applicable. The results of IA control validation are annotated in the DIACAP scorecard. This scorecard, along with the associated POA&M, is evaluated by the DAA for an accreditation decision. The accreditation decision is annotated on the scorecard and becomes a part of the DIACAP package.

PHASE 3:

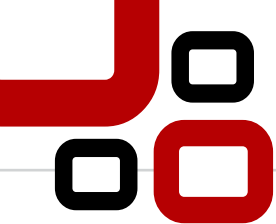
MAKE CERTIFICATION DETERMINATION AND ACCREDITATION DECISION

In this phase the Certification Authority (CA) makes the certification determination and the DAA makes the accreditation decision.

Make Certification Determination

When the system has completed all implementation and validation tasks, the DIACAP package is submitted to the Certifying Authority (CA) for a certification determination. 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:

- ❑ *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. The majority of this evidence comes from the implementation and validation evidence for the IA controls. Each control is validated according to the requisite validation procedures, and the expected results compared to the actual results give the CA an indication of the compliance status for each IA control.*
- ❑ *How does the system behave in the larger information environment? 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?

The Certification Determination is based on the actual validation results. It considers Impact Codes associated with IA controls in a non-compliant status, associated Severity Categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate. The weaknesses identified on the IT Security POA&M reflects residual risk to the system.

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

As part of the certification decision, and after the individual IA controls have been validated as compliant, non-compliant, or not applicable, a residual risk analysis (an analysis that determines risk due to partial or unsatisfactory implementation of assigned IA controls) should be conducted. In order to determine the likelihood of a future adverse event, threats to a system must be analyzed in conjunction with potential vulnerabilities along with the IA controls that are in place for the system as well as the urgency of completing corrective action. Two indicator codes aid in this analysis: Impact Codes and Severity Categories.

Impact Codes are assigned to IA controls at the time of authoring and maintained by the DIACAP Technical Advisory Group (TAG). They indicate the TAG's assessment of the magnitude of network-wide consequences of a failed IA control and are used to assess community risk. Impact codes are expressed as High, Medium, and Low, where High is the indicator of greatest impact or urgency. In conjunction with the severity category, it also indicates the urgency with which corrective action should be taken. Within a severity category, non-compliant IA controls should be prioritized for correction or remediation according to their impact codes.

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

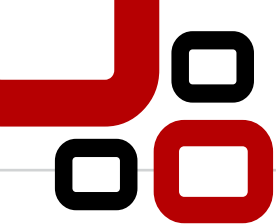
Make Accreditation Decision

An accreditation decision is issued by the DAA, and is communicated via the DIACAP Scorecard and accompanying IT Security POA&M, if required. Documentation (e.g., artifacts, actual validation results) supporting an accreditation decision will be provided in electronic form if requested by DAAs of interconnecting systems. The accreditation decision is expressed as an ATO, IATO, IATT, or DATO. Absent an accreditation decision, a system is considered unaccredited.

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

The formulation of an accreditation decision is supported by the DIACAP package, and always requires a certification determination. If the validation is abbreviated due to mission urgency, the accreditation decision cannot exceed an IATO. If operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

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



cepted non-compliant IA controls and baseline IA controls that are not applicable.

Authority To Operate (ATO)

Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years. The conditions are as follows:

- ❑ *The ATO accreditation decision must specify an Authorization Termination Date (ATD) that is within three years of the authorization date.*
- ❑ *A system with a CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. When requested by an affected military commander, the DoD Component CIO shall authorize operation of a system with a CAT I weakness through an IATO. This responsibility cannot be delegated below the DoD Component CIO, and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO and the system's DAA.*
- ❑ *A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.*
- ❑ *An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA."*

Interim Authority To Operate (IATO)

An IATO is a temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.

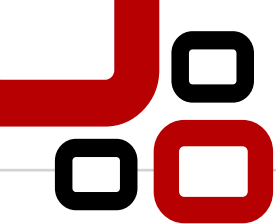
An IATO accreditation decision is intended to manage IA security weaknesses while allowing system operation. It is not intended to be a device for signaling an evolutionary acquisition. A version of a DoD IS acquired in one of a planned series of acquisition increments or development spirals should be granted an ATO, even if additional or enhanced capabilities and services are planned for future increments or spirals. Conditions are as follows:

- ❑ *The IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days.*
- ❑ *A request for an IATO must be accompanied by a DIACAP POA&M. Corrective actions specified in the IT Security POA&M must be achievable within the authorization period and must be resourced accordingly.*
- ❑ *If CAT II weaknesses have not been corrected or satisfactorily mitigated after system operation under IATOs for a total of 360 days, the DAA will normally issue a DATO that will remain in effect until all corrective actions identified in the IT Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO.*
- ❑ *The DoD Component CIO may authorize continuation of operation under an IATO for systems with CAT II weaknesses that have operated for 360 consecutive days. This responsibility cannot be delegated below the DoD Component CIO. The DAA must certify in writing or through DoD PKI-certified digital signature that continued system operation is critical to mission accomplishment. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.*

Interim Authority To Test (IATT)

An IATT is a temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

Authorization is based on an assessment of impact to the information environment, or in the case



of live data, an assessment of mission impact. In many cases, not all IA controls need to be satisfied for testing. In concert with the PM/SM, the DAA will determine what IA controls must be satisfied for a specific testing event. The IATT accreditation decision establishes the agreed upon test duration and any special conditions or constraints, to include notification thresholds and addressees. Conditions include:

- ❑ *The IATT accreditation decision is a special case for authorizing testing in a live information environment or with live data for a specified time period. IATTs should be granted only when operational environment/live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical).*
- ❑ *All applicable IA controls should be tested and satisfied prior to testing in an operational environment or with live data except for those which can only be tested in an operational environment. In consultation with the PM or SM, the DAA will determine which IA controls can only be tested in an operational environment.*
- ❑ *An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate. Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).*

Denial of Authority To Operate (DATO)

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

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

PHASE 4:

MAINTAIN AUTHORIZATION TO OPERATE AND CONDUCT REVIEWS

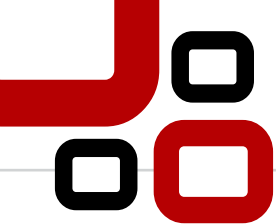
Maintain Situational Awareness

Continued authorization to operate is contingent upon the sustainment of an acceptable IA posture, which is accomplished through ensuring continued compliance with assigned IA controls, and by maintaining a current and appropriate Authorization Decision. The DoD IS IAM has primary responsibility for maintaining situation awareness and initiating actions to improve or restore IA posture.

Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM continuously monitors the system or information environment for security - relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations.

Security relevant events may include:

- ❑ *Expiration of an IA control re-validation period -Certain IA controls will have assigned re-validation periods in which the IA control must be re-validated.*
- ❑ *Security events defined by the IA control -The IAM must also remain cognizant of the IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations, e.g., penetration testing.*
- ❑ *Significant changes to an information system -Configuration changes to the system or information environment could impact the IA posture of the system. In addition, the IAM may, independently or at the direction of the CA or DAA, schedule a revalidation of any or*



all IA controls at any time. FISMA requires revalidation of a select number of IA controls at least annually.

DoD ISs with a current ATO that are found to be operating in an unacceptable IA posture through GAO or IG audits, or other reviews or events, such as an annual security review or compliance validation, shall have the newly identified weakness added to an existing or newly created IT Security POA&M.

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 as follows:

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

If a newly discovered CAT II weakness on a DoD IS operating with a current ATO cannot be corrected or satisfactorily mitigated within 90 days, the system can only continue to operate as follows:

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

Maintain IA Posture

Sustainment of an adequate IA posture is accomplished through ensuring continued compliance with identified IA controls and by maintaining a current and appropriate Authorization Decision. The DoD information system IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore an acceptable IA posture.

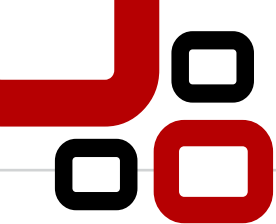
The IAM may recommend changes or improvement to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements to the design of the information system itself.

Perform Reviews

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

Initiate Reaccreditation

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



PHASE V:

DECOMMISSION

Decommission

When a DoD IS is removed from operation, a number of DIACAP - related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, Lines 8, "DIACAP Activity," and 9, "System Life Cycle Phase," of the SIP should be updated to reflect the IS decommissioned status. Concurrently, the DIACAP Scorecard and any POA&Ms should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management should be reviewed for impact.

The program manager should coordinate with DoD governing GIG activities, as appropriate, to identify and apply applicable decommissioning requirements necessary to eliminate the functional or military capabilities of systems. Decommissioning requirements and procedures change over time as the GIG enterprise information environment changes and are maintained through by the DIACAP TAG.

CONCLUSION

The DoD C&A and connection processes can be daunting. A system must first be certified and accredited via the five phase DIACAP process.

Once the DIACAP process has been completed, an IS then requires an IATC or ATC in order to connect to the network.

This process can be plagued with obstacles and roadblocks. It can take anywhere from 6 months to 2 years to complete the entire process.

For many people in DoD responsible for the DIACAP process it is an additional duty that interferes with their daily responsibilities. And because it may also be a new process to them, they have a lack of understanding of how the process works. Many DIACAP practitioners do not fully understand the process themselves. Further, the DIACAP process is constantly changing and adapting to new threats and technologies. Most think they can just "get by" when completing the DIACAP and then they do not have to worry about it for another 3 years. It would be great if it really worked that way.

Because of the way the DIACAP process is approached, with a sense of dread and foreboding, those in responsible positions, such as the Information Assurance Manager, just want to get it done and over with. This is one reason that DoD ISs are not as secured as they could be and adversaries are able to penetrate the systems.

We at Nova Datacom can provide a very important and needed service by helping those responsible to complete a high quality, efficient, and effective DIACAP process. Our goal should not be just "get it done", but actually build security into the system in order to successfully fight "Cyber Warfare".



ABOUT THE AUTHOR

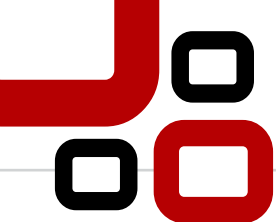
Timothy Taylor, CISSP, Information Assurance Engineer

Mr. Taylor recently retired from the U.S. Army with 31 years of honorable service. He has over 10 years of Information Security experience in addition to a combination of over 20 years Emergency Response, DoD Telecommunications, Physical Security, and Investigative experience. He has managed all activities related to the "Maintain Accreditation" phase of the Department of Defense Information Assurance Certification and Accreditation Program (DIACAP) for the U.S. Army Corps of Engineers Secure Internet Protocol Router Network (SIPRNet) and Managed computer security and information assurance support for the U.S. Army National Guard Headquarters. He has served as a Government Information Assurance Manager and an Active Agent of the Certification Authority (ACA) team member for National Guard Headquarters. He has coordinated and managed the National Guard's Information Technology Requirements Control Board (ITRCB).

Mr. Taylor holds a Masters Degree in Homeland Security, specializing in Security Management. He also holds a B.A. in Public and Criminal Justice Administration. Mr. Taylor has a Top Secret clearance with Sensitive Compartmented Information (SCI) eligibility. He is a Certified Information Systems Security Professional (CISSP) and a Certified Computer Examiner (CCE).

Relevant positions include:

- ▣ *Nova Datacom / U.S. Army Corps of Engineers (USACE) - Information Assurance Engineer*
- ▣ *U.S. Army National Guard Headquarters – Tactical Communications Branch Telecommunications Operations Chief*
 - ▣ *Certification Authority Agent*
 - ▣ *Information Systems Technician*
 - ▣ *Systems Administrator/Global Command and Control Systems (GCCS) Analyst*
 - ▣ *Chief Information Officer (CIO), C6 Operations*
 - ▣ *Physical Security Manager*
 - ▣ *Continuity of Operations (COOP) Team Member*
- ▣ *U.S. Army / U.S. Army Criminal Investigation Command (CID) - Special Agent*
 - ▣ *Counter Terrorist Team*
 - ▣ *White Collar Crime Team*



APPENDIX

AUTHORITY TO CONNECT (ATC) SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)

DISA is the connection approval authority for all DISN connections. The network that supports classified Internet Protocol (IP) based communications is the SECRET Internet Protocol Router Network (SIPRNET).

Under the authority of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, Defense Information System Network and Connected Systems, 9 July 2008, the DISN, Classified Connection Approval Office (CCAO) is responsible for monitoring the security compliance of SIPRNET customers. Its mission is to ensure that:

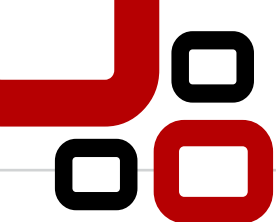
1. *Customer enclaves are compliant with established directives and guidance, and meet all technical and interoperability requirements.*
2. *Operational requirements have been met and validated.*
3. *Customer sub - networks, systems, and other connected components provide adequate security and have been accredited by the proper authority.*
4. *Customers meet established connection requirements.*
5. *Customers are assessed through the use of remote compliance tools and they have met security standards.*

The Classified Connection Approval Team assesses operational networks and enclaves with requirements for connection to the SIPRNet. The Team performs the necessary evaluation, analysis, review and assessment of customer enclaves including remote vulnerability scanning and validation. The CCAO ensures that all connections meet technical and interoperability requirements, sub - networks, subsystems and other connected components provide enclave accreditation documentation, and that security requirements have been implemented as required by DoD and DISA directives, instructions, and guidance. Additionally, the Team coordinates site compliance visits of SIPRNet customers with the DISA's Field Security Operations (FSO). The CCAO monitors the resolution of FSO's findings and the compliance of the customer's enclave/network connection to the SIPRNet.

Mandatory Requirements for an ATC for DOD Activities

1. *A complete Executive Package IAW DODI 8510.01, Enclosure 3, The DIACAP Package, dated 28 November 2007, must be submitted to the CCAO. SIPRNet customers will only be granted an ATC for a maximum of three years.*
2. *SIPRNet Connection Questionnaire, dated 01 November 2008 (includes the Consent to Monitor).*
3. *Enclave Topology Diagram -Most recent configuration to include firewall(s), IDS, PC's, user terminals, servers, hubs, bridges, routers, major applications, gateways, modems, card readers, backup devices, room and building number, and switches (mechanical – A/B or electrical), backside connections, Internet Protocol (IP) addresses, encryption devices and Cross Domain Solutions (CDS)/boundary crossing/interface devices). The topology must include the model number(s) and IP's of the devices on the diagram. The diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections). Other SIPRNet connections (access points) must be shown. The flow of information to, from, and through all connections, Router Port SIPRNet (RTPS), host IP addresses, and CCSD number, if known must be shown. The topology must be dated and signed by the IAM/IAO.*
4. *Successful completion of a remote compliance assessment by the DISN, CCAO Team.*
5. *All SIPRNet IP's must be registered.*
6. *Indicate and label all of the devices, features, or information. Diagram minimum size: 8.5"x 11".*

It is important to note that in accordance with DoD and DISA guidance, firewalls and Intru-



sion Detection Systems (IDS) are required on all customer enclaves. Approval for connection to the SIPRNet will not be granted unless an approved firewall and IDS have been included in the customer's configuration and are compliant with published guidance. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves.

ATC FOR NON-SECURE INTERNET PROTOCOL ROUTER NETWORK (NIPRNET)

The rules are similar but less strict for the NIPRNet. However, the IS has to have an ATO or IATO and a network topology diagram before an Authority to Connect will be granted.

REFERENCES

1. *Army Regulation (AR) 25 - 2, 24 Oct. 2007, Information Management/Information Assurance*
2. *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, 9 Jul. 2008, DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY AND RESPONSIBILITIES*
3. *Defense Information Systems Agency (DISA), Knowledge Service*
4. *Defense Information Systems Agency (DISA) Field Security Operations, Department of Defense Instruction (DoDI) 8500 - 2, 28 Mar 2008, IA Control Checklists*
5. *Department of Defense Instruction (DoDI) 8500.01, 28 Nov. 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP)*
6. *Department of Defense Instruction (DoDI), 8500.2, 6 Feb. 2003, Information Assurance (IA) Implementation*

For additional information, please contact us at novasales@novadatacom.com to schedule a site visit and/or learn more about our IT contingency/disaster recovery and information assurance solutions.