

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICE (DON CIO) INFORMATION ASSURANCE STRATEGY GUIDANCE

15 DECEMBER 2008

Enclosures:

- (1) DON CIO IA Strategy Template
- (2) DoD IA Strategy Checklist
- (3) IA Strategy Background Information

1. Document Purpose

The primary purpose of the Acquisition Information Assurance (IA) Strategy (IAS) is to ensure compliance with the statutory requirements of the Clinger-Cohen Act (CCA) and related legislation, as implemented by Department of Defense (DoD) Instruction 5000.2, *Operation of the Defense Acquisition System*, and Secretary of the Navy (SECNAV) Instruction 5000.2D, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System*. The IAS is to state unambiguously how the program ensures the IA functions of confidentiality, integrity, availability, authentication, and non-repudiation of information that is processed, transported, or stored by the program. It documents the program's overall IA approach.

2. IA Strategy Format

The IA Strategy should be a stand-alone document. Although other key documents can, and in some cases must, be referenced within the IA Strategy to identify supplemental or supporting information, the IA Strategy should contain sufficient content to clearly communicate the strategy to the reader. The IA Strategy should be as simple and concise as possible while providing enough information to detail the program's strategy to implement IA throughout the system life cycle. The objective is to have a document that clearly conveys the intent of the program to comply with relevant policy at a strategic level, but not burden leadership with describing how the program will comply in great detail.

The DON CIO IA Strategy Template, included as enclosure (1), is provided to assist in the development of an acquisition program IA Strategy document that will satisfy statutory review requirements. It is critical that all sections of the template be addressed. If a section does not apply, so justify in writing. If the program is in the early stages of development and the section is not applicable or information required is not known at the time, so state indicating at what stage the information will be applicable or known. If a program cannot maintain functionality or cannot support one of the IA functions, then this failure becomes an IA shortfall and should be documented in the IAS. Citing other documents will not substitute for essential information that can be supplied in the context. The reader should not need to go to another document to obtain information needed to make a decision.

The DON CIO IA Strategy Template mirrors the format of the DoD CIO template provided in the Defense Acquisition Guidebook. The IA Strategy is a "living document" and as such will change over time as the program evolves or until the system is retired or phased out. Enclosure (3) provides background, supplemental information, and list of acronyms.

3. Submission and Review

The DON CIO now requires that the IA Strategy be reviewed by the Navy Echelon 2 or Marine Corps Major Subordinate Command Information Officer, and approved by the appropriate Designated Accrediting Authority (DAA) prior formal submission to the DON CIO.

The IA Strategy document is submitted to the DON CIO along with the CCA Compliance Package. The DON CIO CCA Compliance Coordinator will separate the IA Strategy from the CCA Compliance package for the DON CIO IA Team to review. The Program Office representative should reach out to the DON CIO IA staff to resolve questions or concerns about the IA Strategy. Approval of the IA Strategy is an iterative process and requires close coordination between the Program Office and the DON CIO IA Team. For Acquisition Category (ACAT) ID, IAC, and IAM programs, the DON CIO staff will coordinate the DoD review process. The Program Office may direct liaison with the DoD reviewer as necessary, and vice versa, always keeping the DON CIO IA reviewer informed. The enclosure (2) DoD checklist is recommended for use as a final check prior to IA Strategy submission.

To facilitate reviews of IA Strategies, the Program Offices / Systems Commands should inform the DON CIO of CCA submissions planned for the next two calendar quarters.

4. Approval Process

The DON CIO review process includes many activities that are conducted concurrently and sequentially. Allow 90 days for concurrent DON CIO and DoD CIO review and approval of an IA Strategy. The DON CIO IA Staff strongly encourages the Program Office to submit draft IA Strategies for early informal review and will make every effort to promptly review them subject to the staff's workload. When submitted for informal review, DON CIO will solicit a DoD CIO early review (as appropriate) to identify any potential DoD CIO issues early in the process.

The flow of activities and the approval process is described below and illustrated in Figure One.

a. Program Office submits CCA Compliance Package (including IA Strategy) to the DON CIO. The respective Command Information Officer must be kept in the loop. The Program Office may discuss the development and submission of the IA Strategy with, or provide a draft early copy to, the DON CIO prior to formal submittal.

b. Concurrent DON CIO processes are:

(1) The DON CIO CCA Compliance Coordinator will separate the IA Strategy from the CCA Compliance package for the DON CIO IA Team to review.

(2) The DON CIO IA Staff reviews the IA Strategy.

(a) Acquisition Category (ACAT) IC and II programs: The DON CIO IA Staff will coordinate with the DON CIO CCA Compliance Coordinator for input into the overall CCA Compliance package for DON CIO approval.

(b) ACAT ID, IAC, and IAM programs: The IA staff will forward the IA Strategy to the DoD CIO for formal review. The DON CIO is required to obtain DoD CIO formal review of IA Strategies for ACAT ID, IAC, and IAM programs before DON CIO approval of the CCA

Compliance packages. The DoD CIO and the Program Office may direct liaison, but all such correspondence shall be “copy to” the DON CIO IA Team.

c. For those IA Strategies requiring DoD formal review, the DON CIO IA Team Leader will forward the IA Strategy to the DoD CIO staff recommending approval. The DoD CIO Staff will respond to the DON CIO Team Leader. After all reviews and approvals, the IA Team Leader approves the IA Strategy and forwards it to the DON CIO CCA Coordinator, who incorporates it into the CCA Compliance Package for DON CIO signature.

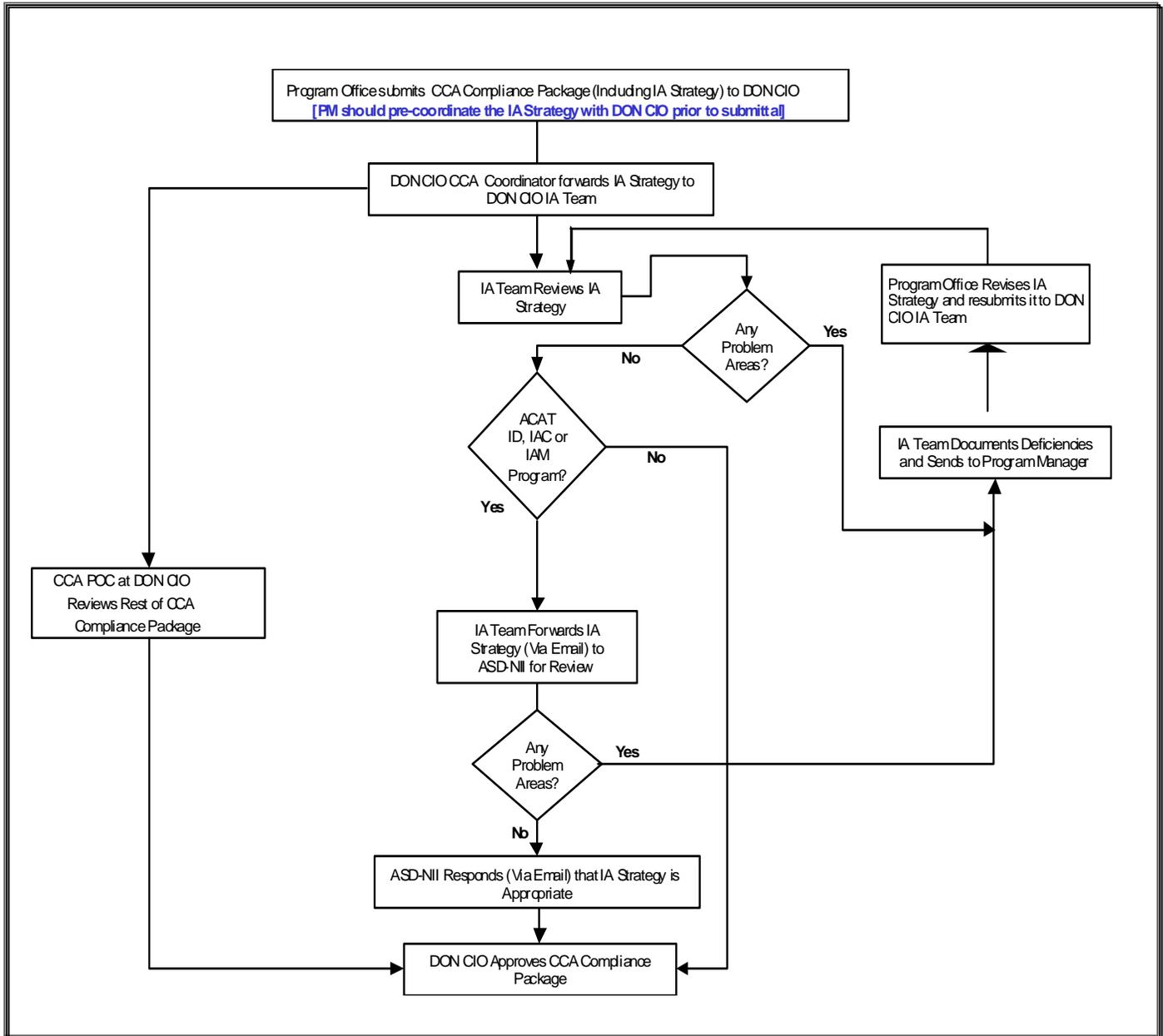


Figure 1 – IA Strategy Approval Process

This Page Intentionally Blank

ENCLOSURE (1): DON CIO IA STRATEGY TEMPLATE

This enclosure provides detailed instructions for completing an IA Strategy as required by the Clinger-Cohen Act and SECNAVINST 5000.2D, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities*.

COVER PAGE

The Cover Page needs to include the following items:

- Full Program Name with Acronym
- Increment or Phase of Program
- ACAT Level
- Date and Revision Number of IA Strategy
- Program Address
- Special Handling Procedures/Disclaimer Statements, as follows:

Distribution Statement: Distribution authorized to the Department of Defense (DoD) and United States (U.S.) DoD contractors only. Questions concerning technical content or any other requests for this document shall be referred to the (include appropriate program name, and address).

Warning: This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec 2751 et seq.) or the Export Administration Act of 1979, as amended (Title 50 U.S.C. App. 2401 et seq.). Violators of these export laws are subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25.

Handling and Destruction Notice: Comply with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

This document contains information exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Exemption 2 applies.

In addition, each page of the IA Strategy should be marked, at a minimum, "For Official Use Only".

TABLE OF CONTENTS

Page ii should include the Table of Contents and list of all Tables and Figures. Follow the Section Titles and Numbering Scheme found in this template.

IA STRATEGY

Header: Program/System Name, IA Strategy Version Number, Date

Footer: Page Number, "For Official Use Only" Designation.

INFORMATION ASSURANCE (IA) STRATEGY FOR [PROGRAM NAME] [Document Date]

1. OVERVIEW

Table 1: Program/System Overview

ACAT Level	
Acquisition Life Cycle Phase	
Milestone Decision and Date	
DITPR-DON ID Number & Acronym	
Mission Designation (Mission Critical, Mission Essential, or Mission Support)	
MAC and Confidentiality Level	
Next Major Milestone	
Type of System (i.e., AIS Application, Enclave, Outsourced It-Based Process, PIT [must have PIT approval document], Platform IT (PIT) Interconnection)	
Status of GIG connection: Program <u>is</u> connected to the GIG, or Program is <u>indirectly</u> connected to GIG, or Program <u>is not</u> connected to the GIG	

1.1 Program Description

- Brief background and history of the program. (Discuss any previous or subsequent versions of the IA Strategy.)
- Program's mission/objective/concept of operations. (Purpose for the existence of the program or the capability supplied to the user.)
- High level diagram of the program and its interconnections. (A DoD Architecture Framework (DoDAF) Operational View level 1 (OV-1) would suffice.)

1.2 Program Schedule

- Graphic representation of the program's schedule (high-level – milestones, major decision points, critical events, DT/OT milestones, spirals/builds if applicable).

2. MISSION ASSURANCE CATEGORY (MAC) & CONFIDENTIALITY LEVEL (CL)

2.1 Brief rationale for the current Mission Assurance Category (MAC) Level. (Enclosure (3) Section 1 provides additional guidance.)

2.2 Brief discussion of Confidentiality Level (CL) for the system.

- 2.3 If a mix of MACs/CLs exists, explain how consistently effective data protection is achieved between the differing levels of Mission Assurance Categories and Confidentiality Levels.
- 2.4 Brief description of protection for each classification level, if the system accesses different levels of classifications (e.g., Secret, Unclassified).

3. SYSTEM DESCRIPTION

- High-level descriptive overview of the system being acquired.
- Graphic (block diagram) showing the major elements/subsystems of the system/service being acquired, and how they fit together, to include the Platform IT (PIT) boundary, if the system is approved as PIT.
- Interconnection of this program with other programs. A DoDAF System Interface Description View (SV-1) would suffice.
- System's basic function(s).
- Timeline and relationship between the builds, if Spiral Development or incremental build processes employed.
- System's information exchange requirements (IERS).
- System interface with the GIG, other IT or systems, and primary databases supported (or explanation if not interfacing with the GIG).
- Exchange of information at higher/lower security classifications, if applicable.
- High level description of the IA technical approach that will secure the system, including any protection to be provided by external systems or infrastructure, and protection of data at rest.

4. THREAT ASSESSMENT (at unclassified level)

- 4.1 Methodology used to determine threats to the system (such as a System Threat Assessment Report (STAR), although STARs is no longer required to substantiate IA threat). Provide list of applicable threat assessments such as Threat Environment Descriptions (TED), Defense Intelligence (DI) reports, and Office of Naval Intelligence (ONI) reports that address potential threat vectors to the program or system.
- 4.2 For AIS applications, unique threats to the system's IT resources due to mission or area of proposed operation (including internal threats).
- 4.3 For MAIS programs, utilization of the Information Operations Capstone Threat Capabilities Assessment is required by DoD 5000.2. Note: The Defense Intelligence Agency (DIA) updates this document every six months.

5. RISK ASSESSMENT (at unclassified level)

- 5.1 Program's planned regimen of technical IA risk assessments. (Do not confuse IA risk assessment with Program Risk Management as a function of program management.) Enclosure (3) Section 2 provides additional guidance.
- 5.2 Summary of how any completed risk assessments were conducted.

- 5.3 For systems where software development abroad is a possible sourcing option, description of how risk was assessed.
- 5.4 For Platform IT programs, description of how IA risk is addressed in system engineering.

6. INFORMATION ASSURANCE REQUIREMENTS, STANDARDS, & ARCHITECTURE

6.1 Documentation of IA Requirements and Specifications

- Program's methodology for addressing IA requirements early in the acquisition lifecycle, with specific attention to DoDI 8500.2 Baseline IA Controls. Identify the applicable sets of Baseline IA Controls from DoDI 8500.2 that will be implemented. (Only identify what sets are being used, do not list all individual IA controls)
- Specify whether any specific IA requirements are identified in the approved governing capabilities documents (e.g., MNS, CRD, ORD, ICD, CDD, and/or CPD). List applicable documents in Section 11 of the IAS.
- Indicate whether or not costs for IA development, test, implementation, and maintenance (including costs associated with certification and accreditation activities) are incorporated into the program budget and if the budget is adequate and visible in the overall program budget. (Actual budget figures not desired.) Ensure IA cost considered the program's Configuration Management Program's Engineering Change Proposal approval process.
- Acknowledge IA training requirements for personnel (DoDD 8570.01, *Information Assurance (IA) Training, Certification, and Workforce Management*).

6.2 Privacy

- Explanation of whether system collects, processes, stores, and/or transmits Personally Identifiable Information (PII), including brief description of protection of PII, and if so, whether Privacy Impact Assessment (PIA) has been submitted. Enclosure (3) Section 3 provides additional guidance.

6.3 System Protection

- Brief description of how information will be protected and information system survivability will be incorporated into the system design for protection, detection, reaction, and reconstitution capabilities.
 - Protection of sensitive or classified information in the event of compromise of system defense in depth.
 - Description of how classified information or cryptographic keys will be purged in the event the system falls into enemy hands.
- Brief description of any comprehensive contingency/disaster recovery plans.
- Description of whether the system implements DoD-mandated PKI authentication and in the case of a web server, whether it is Public Key Enabled. Enclosure (3) Section 4 provides additional guidance on PKI/PKE.

7. ACQUISITION STRATEGY

- 7.1 Summary of how IA is addressed in the program's overall acquisition strategy document.

- 7.2 Description of how the Request for Proposal (RFP) for the System Development and Demonstration Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and testing.
- 7.3 Description of how the RFP communicates the requirement for personnel that are trained and appropriately certified in accordance with DoDD 8570.01 for providing IA functional services for DoD information systems.
- 7.4 Description of the means for verifying that the mandates of National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) in IA-Enabled Information Technology Products*, will be followed in accordance with DoDI 8500.2 paragraph E.3.2.5, if the program will be purchasing commercial off-the-shelf IA or IA-enabled products. Enclosure (3) Section 5 provides additional guidance.

8. CERTIFICATION AND ACCREDITATION (C&A)

8.1 C&A Process and Status

- Identification of the specific C&A process to be employed (e.g., DIACAP, DITSCAP, NISCAP, DODIIS, or NIACAP). The DON DITSCAP to DIACAP Transition Guide and the DIACAP Handbook (both available on the DON CIO website) provide additional guidance. (Enclosure (3) Section 6 provides a link.)
- Name, title, and organization of the Developmental and Operational DAAs, Certification Authority (CA), and User Representative.
- If the program is pursuing an evolutionary acquisition approach (spiral or incremental development), description of how each increment will be subjected to C&A.
- Timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of an Interim Authority to Test (IATT), Interim Authority to Operate (IATO), and/or Authority to Operate (ATO). Link IATO and ATO to Developmental Test and Evaluation (DT&E) events to show how and when they support DT/OT. (Normally, it is expected that an ATO will be issued prior to Operational Test and Evaluation.)
- If the C&A process has been started, identification of significant activity completed, and whether an IATO or ATO was issued (with dates of issuance and expiration). If the system does not have an ATO, the plan of action and milestones (POA&M) should be referenced for obtaining full accreditation.
- A timeline graphic depicting C&A schedule and milestones, with supporting information if an alternative C&A process is to be employed in lieu of DIACAP.

8.2 For Platform IT (PIT) Systems (Enclosure (3) Section 7 provides information):

- Note that while PIT systems may not require C&A, PIT Interconnections (PITI) are DoD Information Systems and therefore do require C&A.
- Description of how the program will use the System Engineering Technical Review (SETR) process to establish confidence in the IA portion of the program.
- Provision of a table to show the linkage between key events in the SETR process and the need to support DT/OT with artifacts equivalent to the IATO and ATO.

- 8.3 If under Intelligence Community Directive 503, *Intelligence Community Information Technology systems Security Risk Management Certification and Accreditation*, or the Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information (SCI) within Information Systems*, i.e., or the system or a segment of the system processes, stores, or distributes Sensitive Compartmented Information (SCI), indication of Intelligence Community (IC) involvement and whether dual DAAs will be involved. Enclosure (3) Section 8 provides guidance.

9. IA TESTING

- 9.1 Explanation of how IA testing is integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test & Evaluation Master Plan (TEMP).
- 9.2 Explanation of how training and system support documentation will be included in DT/OT.

10. IA SHORTFALLS (IA shortfalls can be included in a classified annex if appropriate)

- 10.1 Description of any significant IA shortfalls and the proposed solutions and/or mitigation strategies for these IA shortfalls.
- 10.2 Impact of failure to resolve shortfalls in program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability.
- 10.3 If the solution to an identified shortfall lies outside the program office's control, identification of the recommended organization with the responsibility and authority to address the shortfall.
- 10.4 Identification of any Acquisition Decision Memoranda that cite IA issues (if applicable).

11. POLICIES AND DIRECTIVES

DoD and DON policies and directives applicable to the program, with a brief overall explanation of how the program complies with those policies. Policies applicable to all programs or systems are listed in Enclosure (3) Section 9.

12. RELEVANT ASSOCIATED PROGRAM DOCUMENTS

Statement that this version of the acquisition IA strategy is reflective of the Program CRD/ORD/ICD/CCD/CPD dated _____, and the Information Support Plan (ISP) dated _____. If the Net-Ready KPP (NR-KPP) has been certified, identify the date of the certification. (Note: Subsequent revision to the requirements documents or ISP will require a subsequent revision or revalidation of the Acquisition IA Strategy.)

13. POINT OF CONTACT

Name and contact information for the program management office individual responsible for the IA Strategy document. (DoD recommends the Program Office's formally appointed IA Manager be the point of contact.)

14. IA STRATEGY APPROVAL BY PROGRAM OFFICE, CIO, AND DAA

Approval signatures and dates.

ENCLOSURE (2): IA STRATEGY CHECKLIST

This enclosure provides a check list that can be used to assist in IA Strategy approval.
This checklist is used by both DON CIO and DoD for reviewing IA Strategies.

Program Name:

Reviewed By:

Date of Review:

IAS Version/Date:

1.0 Program Category and Life Cycle Status:

- Identify the Acquisition Category (ACAT) of the program.
- Identify current acquisition life cycle phase.
- Identify next milestone decision.
- Identify the mission criticality of the system in accordance with DODI 5000.2.
- Include graphic depicting program schedule showing all major milestones, SDD spirals (if applicable), DT/OT milestones, and IOC/FOC milestones if clarity is needed.

2.0 Mission Assurance Category (MAC) and Confidentiality Level:

- Identify the system's MAC and Confidentiality Level as specified in the applicable requirements document, or as determined by the system User Representative on behalf of the information owner, in accordance with DODI 8500.2.

3.0 System Description:

- Provide a high-level overview of the specific system being acquired.
- Provide a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together.
- Describe the system's function, and summarize significant information exchange requirements (IER), interfaces with other IT or systems, and primary databases supported.
- Describe, at a high level, the IA technical approach that will secure the system, including any protection to be provided by external systems or infrastructure.

4.0 Threat Assessment:

- Note: System Threat Assessment Reports (STARs) are no longer required for the purpose of substantiating IA threat. STARs may be developed to satisfy other discipline requirements, and considered as part of the IA risk assessment.
- For MAIS programs, utilization of the "Information Operations Capstone Threat Capabilities Assessment" (DIA Doc # DI-1577-26-04) [3rd Edition Aug 04] is required by DoD Instruction 5000.2.

5.0 Risk Assessment:

- Describe the program's planned regimen of risk assessments, including a summary of how any completed risk assessments were conducted.

6.0 Information Assurance Requirements:

- ❑ Describe the program's methodology used for identifying IA requirements early in the lifecycle (with specific attention to DoDI 8500.2 Baseline IA Controls).
- ❑ Specify whether any specific IA requirements are identified in the approved governing capabilities documents (e.g. Capstone Requirements Document, Initial Capabilities Document, Capabilities Design Document, or Capabilities Production Document).
- ❑ Describe at a high level how IA development, test, implementation, and maintenance costs (including costs associated with C&A activities) are incorporated into the program budget and if the budget is adequate. Actual budget figures not required.
- ❑ Describe intent to comply with DoDD 8570.1, Information Assurance (IA) Training, Certification, and Workforce Management.

7.0 Acquisition Strategy:

- ❑ Provide a summary of how information assurance is addressed in the program's overall acquisition strategy document.
- ❑ Describe how the RFP for the System Development and Demonstration Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and testing.
- ❑ Describe how the RFP communicates the requirement for personnel that are trained and appropriately certified in IA, in accordance with DoDD 8570.1.
- ❑ Address whether the program will be purchasing commercial off-the-shelf IA or IA-Enabled products, and the program's means for verifying that the product specification and evaluation requirements of DoDI 8500.2 paragraph E3.2.5. (DoD's implementation of National Security Telecommunications and Information Systems Security Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products*) will be followed.

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

- ❑ Identify the specific C&A process to be employed (e.g. DIACAP, DITSCAP, NISCAP, and DODIIS). If DITSCAP, cite the specific transition authority from the Interim DoD C&A Guidance that permits the system to remain under DITSCAP.
- ❑ Provide the name, title, and organization of the Designated Approving Authority (DAA), Certification Authority (CA), and User Representative.
- ❑ If the program is pursuing an evolutionary acquisition approach (spiral or incremental development), describe how each increment will be subjected to the certification and accreditation process.
- ❑ Provide a timeline graphic depicting the target initiation and completion dates for the Certification and Accreditation (C&A) process, highlighting the issuance of IATT, IATO, and ATOs.
 - Normally, it is expected that an Authorization to Operate (ATO) will be issued prior to operational test and evaluation.
- ❑ If the C&A process has been started, identify significant activity completed, and whether an Authority to Operate (ATO) or Interim Authority to Operate (IATO) was issued.

- ❑ Is there indication that the system will be communicating/processing Intelligence Community info (SCI)? If so, are they using DCID 6/3 (or ICD 503) as the C&A process for that segment of the system? Are there dual DAA's? Is DIA involved?
- ❑ Identify any other alternative C&A process that will be employed in lieu of the DIACAP (i.e., NISCAP). Provide supporting information concerning C&A schedule, milestones, etc.

9.0 IA Testing:

- ❑ Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test & Evaluation Master Plan (TEMP).

10. IA Shortfalls:

- ❑ Identify any significant IA shortfalls, and the proposed solutions and/or mitigation strategies.
- ❑ Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability.
- ❑ If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall.
- ❑ If applicable, identify any Acquisition Decision Memoranda that cite IA issues.

11. Policy/Directives.

- ❑ List the primary policy guidance employed by the program in preparing and executing the acquisition IA strategy, including any Component, MAJCOM/SYSCOM, or program-specific guidance, as applicable.
 - Should include DoDI 5000.2, NSTISSP 11, DoDD 8500.1, DoDI 8500.2, DoDI 8580.1, DoDD 8570.1, DoD 8570.1-M, DIACAP.
 - May include DoDI 5200.40, and DoD 8510.1-M if they are still following DITSCAP per the DIACAP Transition Timeline and Instructions.
 - Space systems should include DoDD 8581.1.

12. Relevant Associated Program Documents:

- ❑ Provide statement that this version of the Acquisition IA Strategy is reflective of the Program CRD/ICD/CDD/CPD dated _____, and the Information Support Plan (ISP) dated _____. [Note: subsequent revisions to the requirements documents or ISP will require a subsequent revision or revalidation of the Acquisition IA Strategy.]

13. Point of Contact:

- ❑ Provide the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document.

This Page Intentionally Blank

ENCLOSURE (3): IA STRATEGY BACKGROUND INFORMATION

This enclosure provides additional or background information to assist in completion of an IA Strategy submitted to the DON CIO. It includes information on:

1. Mission Assurance Category and Confidentiality Level
2. Risk Assessment
3. Privacy (E-Gov Act of 2002)
4. DoD PKI and PKE
5. Use of COTS/GOTS (DoDD 8500.01E and DoDI 8500.2 Requirements)
6. Certification and Accreditation (C&A)
7. Platform IT (PIT),
8. ICD 503 (replacement for former DCID 6/3)
9. DoD and DON IA Policies
10. Acronyms

1. MISSION ASSURANCE CATEGORY AND CONFIDENTIALITY LEVEL

Information on Mission Assurance Category and Confidentiality Levels can be found in the Defense Acquisition Guidebook, Chapter 7, *Acquiring Information Technology and National Security Systems*. It is also thoroughly detailed in DoD Directive (DoDD) 8500.01E, *Information Assurance (IA)*, and DoDI 8500.2, *Information Assurance (IA) Implementation*.

2. RISK ASSESSMENT

Risk methodology is described as the method the program used to determine IA risk. The Chief of Naval Operations (CNO) Information Assurance (IA) Publication Module 5239-16 of October 2003, available on the Navy INFOSEC web site (<https://infosec.navy.mil/> - CAC required), provides a good discussion of IA risk methodologies that programs should use in their assessment of risk. (It is also termed NAVINFOSEC P 5239-16 Risk Assessment Guidebook.) It should be noted that the risk methodology described in this paragraph refers solely to that used during DITSCAP phases. When operating under DIACAP, risk is determined differently since the impact codes are hard coded based on specific IA controls.

In describing how risk was assessed for systems where software development abroad is a possible sourcing option, refer to DoD Directive 5160.54, *Critical Asset Assurance Program (CAAP)*, available at the DTIC website: <http://www.hqda.army.mil/ogc/EXEC%20AGENTS%20REF%20LIBRARY/10%20d516054p.pdf> and SECNAVINST 3501.1, *Department of the Navy (DON) Critical Infrastructure Protection (CIP)*, available at the DON Navy Electronic Directives System website: <http://doni.daps.dla.mil/Directives/03000%20Naval%20Operations%20and%20Readiness/03-500%20Training%20and%20Readiness%20Services/3501.1A.pdf> for guidance in defining requirements for critical assets.

3. PRIVACY

The E-Government Act of 2002 includes Privacy requirements and can be accessed at: <http://www.whitehouse.gov/omb/egov/g-4-act.html>. In addition, the Office of Management and Budget has links to Privacy Guidance and Privacy Reference Materials at its web site: <http://www.whitehouse.gov/omb>.

The definition of "personally identifiable information" (PII) is data that can be linked to specific individuals and includes, but is not limited to such information as name, postal address, phone number, e-mail address, social security number, and driver's license number.

The definition of "Information in identifiable form" (IIF), as it is related to a Privacy Impact Assessment (PIA), is specifically defined in the E-Government Act of 2002 as "information in an IT system or online collection: (a) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (b) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)"

4. DOD PUBLIC KEY INFRASTRUCTURE (PKI) & PUBLIC KEY-ENABLING (PKE)

The DoD PKI, in concert with the Common Access Card (CAC), provides a solid foundation for interoperable, public key enabled security services at multiple levels of assurance. Public key cryptography is a critical element of the DoD and DON overall technical strategy for information assurance. Given the importance of PKI, all IA strategies submitted to the DON CIO should contain explicit reference to the program's plans regarding PKE. Authors of IA strategies must consider that applications and systems connected to the GIG must comply with DoD policy and guidance on PKI and PKE.

DoD and DON policy states that all DON information systems, including networks, e-mail, private web servers, and applications must be enabled to use certificates issued by the DoD PKI and approved external PKIs as appropriate to support authentication, access control, confidentiality, data integrity, and non-repudiation. DON approved mobile code shall also be signed using DoD PKI mobile code signing certificates. DoDI 8520.2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, is available from the DTIC website: <http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf>.

Authors of IA strategies should identify the PKI/PKE requirements that apply to their system and address how the requirements are or will be met. If the requirements are not being met, and the system does not qualify for a PKI/PKE compliance waiver, a justification for non-compliance must be provided in addition to a plan of action and milestones (POA&M) for achieving compliance. Authors should also indicate whether future versions of the system or application are envisioned to support PKI and PKE or if compliance may be achieved through future changes in technology.

Examples of situations in which PKI/PKE compliance waivers may be requested include:

- Legacy information systems that will be phased out, accessed through the PK-enabled portal, or replaced by an approved PK-enabled information system (e.g., NMCI),
- Situations in which the projected cost to PK-enable significantly exceeds the expected return on investment (ROI),
- Situations involving undue hardship that prevents PK-enablement, or
- Situations where an exception may be warranted based on technical or operational environment constraints.

5. COTS IA AND IA-ENABLED PRODUCTS AS PART OF THE SECURITY ARCHITECTURE

Per the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, an IA product is an IT product or technology whose primary purpose is to provide security services, correct known vulnerabilities, and/or provide layered defense against various categories of threats. Examples of IA products include data/network encryptors and firewalls. An IA-enabled product is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Security-enabled web browsers and email applications are examples of IA-enabled products. A product that audits user actions or authenticates users, such as most operating systems, is considered IA-enabled.

- Section 4.17 in DoDD 8500.01E requires that all IA and IA-enabled IT hardware, firmware, and software components and products incorporated into DoD information systems comply with the evaluation and validation.
- Acquisitions of commercial off the shelf (COTS) IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) shall be limited to only those products that have been evaluated and validated in accordance with:
 - The National Information Assurance Partnership (NIAP) program (Common Criteria), or
 - The Federal Information Processing Standard (FIPS) validation program.
- Acquisitions of government off the shelf (GOTS) IA and IA-enabled products be limited to only those products that have been evaluated by the National Security Agency (NSA) or in accordance with NSA-approved processes.
- For additional information, consult the following references:
 - DoDD 8500.01E, *Information Assurance (IA)*, and DoDI 8500.2, *Information Assurance (IA) Implementation*, available at the DTIC website: <http://www.dtic.mil/whs/directives/>
 - National Information Assurance Partnership (NIAP) Web site, available at: <http://www.niap-ccevs.org/>.

The following is provided as a model of a well-written section on the COTS/GOTS IA and IA-enabled products.

“The system will employ COTS IA and IA-enabled products as part of the security architecture. These products will be compliant with DoDD 8500.01E and DoDI 8500.2, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). Similarly, GOTS IA or IA-enabled products employed by the system will be evaluated by the National Security Agency (NSA) or in accordance with NSA-approved processes.”

6. CERTIFICATION AND ACCREDITATION (C&A)

In accordance with DoDI 8510.01, “DIACAP,” all DoD-owned information systems (ISs) and DoD-controlled ISs operated by a contractor or other entity on behalf of the DoD that receive,

process, store, display, or transmit DoD information, regardless of classification or sensitivity, consistent with DoD Directive 8500.01E, "Information Assurance (IA)," must be certified and accredited. Program Managers should adhere to the instructions of IA Implementation, DoDI 8500.2, for the selection and application of appropriate IA controls for all acquisitions that involve the use of IT.

DIACAP replaced DITSCAP. The DON has developed and promulgated a transition plan and DIACAP Handbook, available on the DON CIO web site:

- DON DITSCAP to DIACAP Transition Plan:
<http://www.doncio.navy.mil/PolicyView.aspx?ID=695>
- DON DIACAP Handbook:
<http://www.doncio.navy.mil/contentview.aspx?id=731>

7. PLATFORM IT (PIT)

Even though a system may be designated as PIT, it is still required to incorporate IA requirements of DoDI 8500.2, which requires that commanders of DON organizations and program managers identify and implement a plan to achieve security control objectives, and ensure that IA is fully integrated into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, and operation. Further, they shall ensure that IA is integrated into the Systems Engineering Technical Review (SETR) process in accordance with ASN(RD&A) memo, Systems Engineering Technical Review Process for Naval Acquisition Programs, of 13 June 2808, which can be found at:

http://www.doncio.navy.mil/uploads/ASN_RDA_SETR_Memo_JUN08.pdf

8. INTELLIGENCE COMMUNITY DIRECTIVE 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*

This document replaced, on 15 September 2008, the Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information (SCI) within Information Systems*.

Compliance with the ICD 503 (or DCID 6/3 if already under the former system), available at the Director of National Intelligence Directives web site: http://www.dni.gov/electronic_reading_room/ICD_503.pdf, is required should the system process Sensitive Compartmented Information (SCI). If only a segment of the system is required to comply with ICD 503, then the program's approach to compliance should be addressed for that segment.

9. DOD AND DON IA POLICIES

The list below contains the minimum policies systems must comply with. In the case of systems that process SCI, then the ICD 503 and DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide must also be considered. Note that SECNAVINST 5000.2D requires "Prior to program initiation, a Capability Development Document (CCD), Capability Production Document (CPD) (for Acquisition Category [ACAT] programs), or program/resource sponsor memorandum (for Abbreviated Acquisition Programs (AAPs) on non-acquisition programs) shall define the program requirements for each platform, system, or initiative for which funding is programmed or planned. Requirements Letters or Letters of Requirements for ACAT programs are not authorized."

- E-Government Act of 2002, Title III of Public Law 1207-347 available at the White House web site: <http://www.whitehouse.gov/omb/egov/g-4-act.html>;
- DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003: <http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf>;
- DoDD 8500.01E, "Information Assurance (IA), available at the DTIC web site: <http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>;
- DoDI 8500.2, *Information Assurance (IA) Implementation*, available at the DTIC web site: <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>;
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004: <http://www.dtic.mil/whs/directives/corres/pdf/858001p.pdf>;
- DoDI 8510.1, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, available at the DTIC web site: <http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>.
- SECNAVINST 5239.3A, *Department of the Navy Information Assurance (IA) Policy*, available at the Navy Electronics Directives System (NEDS) web site: <http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3A.pdf>
- DoDD 8570.01, *Information Assurance Training, Certification, and Workforce Management*, available at the DTIC web site: <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>
- DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, available at the DTIC website: <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, available at the Committee on National Security Systems (CNSS) web site: http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf

These and other related directive documents are available by accessing the Information Assurance Support Environment (IASE) web site at: <http://iase.disa.mil/index2.html>, the Washington Headquarters Service (WHS) web site at: <http://www.dtic.mil/whs/directives/>, and DON CIO web site at: [http://www.doncio.navy.mil/\(2445al45ddfwwuxe0tanmssu0\)/policy.aspx?sType=policy](http://www.doncio.navy.mil/(2445al45ddfwwuxe0tanmssu0)/policy.aspx?sType=policy).

11. ACRONYMS

ACAT	Acquisition Category
AIS	Automated Information Systems
ATO	Authority to Operate
C&A	Certification and Accreditation
CA	Certification Authority
CCA	Clinger-Cohen Act
CL	Confidentiality Level
CDD	Capability Development Document
COTS	Commercial Off-the-Shelf
CPD	Capabilities Production Document

CRD	Capabilities Requirements Document
DAA	Designated Accrediting Authority
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DITSCAP	DoD Information Technology System Certification and Accreditation Process
DoDAF	DoD Architecture Framework
DODIIS	Department of Defense Intelligence Information System
DT/OT	Developmental Test / Operational Test
DTIC	Defense Technology Information Center
FIPS	Federal Information Processing Standard
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
IAS	Information Assurance Strategy
IATO	Interim ATO
IATT	Interim Authority to Test
ICD	Interface Control Document
IER	Information Exchange Requirement
ISP	Information Support Plan
MAIS	Major AIS (as defined in SECNAVOINST 5000.2D)
MAC	Mission Assurance Category
MNS	Mission Need Statement
NIACAP	National IA Certification and Accreditation Process
NIAP	National Information Assurance Partnership
NR-KPP	New-Ready / Key Performance Parameter
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
ORD	Operational Requirements Document
OV	Operational View
PIA	Privacy Impact Assessment
PII	Personally Identification Information
PIT	Platform Information Technology
PITI	PIT Interconnection
PKI/PKE	Public Key Infrastructure / PK Enabling
RFP	Request for Proposal
SCI	Sensitive Compartmented Information
SETR	System Engineering Technical Review
STAR	System Threat Assessment Report
SV	System View
TED	Threat Environmental Description