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

FEBRUARY 2013

CONTENTS:

INTRODUCTION

1. Purpose:

The primary purpose of the Acquisition Information Assurance Strategy (AIAS) is to ensure compliance with the statutory requirements of the Clinger-Cohen Act (CCA), as implemented by Department of Defense (DoD) Instruction 5000.02, *Operation of the Defense Acquisition System*, and Secretary of the Navy (SECNAV) Instruction 5000.2E, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System.* The AIAS shall clearly describe the program's overall IA approach. Acquisition IA Strategies shall be updated, as necessary, at each program milestone, program initiation for ships, full rate production (FRP), full deployment decision (FDD), and with major changes to the system.

2. Acquisition IA Strategy Format

The latest DoD guidance (DoDI 5000.02 and DoDI 5200.39 (*Critical Program Information (CPI) Protection within the Department of Defense))* requires the AIAS be appended to the Program Protection Plan (PPP).The AIAS may be submitted separately and in advance of the CCA package. Early staffing and approval of the AIAS in advance of the CCA package enables the AIAS to be cited as a "fait accompli" in the CCA package approval.

The Acquisition IA Strategy remains a stand-alone document. Although other key documents are referenced within the AIAS to identify supporting information, the AIAS should contain sufficient content to clearly communicate the strategy to the reader. The AIAS 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 Department of the Navy Chief Information Officer (DON CIO) AIAS Template, Part (1) of this guidance, is provided to assist in the development of a document that will satisfy statutory review requirements. All sections of the template need to be addressed. If a section does not apply, justify that point 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, state that point, 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 AIAS. Citing other documents will not substitute for this essential information.

The DON CIO AIAS Template mirrors the format of the DoD CIO template, which is based on the PDUSD (AT&L) memorandum of 18 July 2011 *Document Streamlining – Program Protection Plan (PPP),*.The DoD guidance will be incorporated in the Defense Acquisition Guidebook, Chapter 7.5.

Part (2) of this document provides a checklist as a final check of the AIAS prior to submission for review and approval. Part (3) provides background, supplemental information, and list of acronyms.

In consideration of the different levels of maturity relative to acquisition phases, and to encourage brevity and focus of the Acquisition IA Strategy, DoD has imposed the following guidelines:

- AIAS isnot required for Material Development Decisions (MDD)
- AIAS for Milestone (MS) A – 7 pages
- AIAS for MS B or C – 15 pages
- AIAS for Full Rate Production (FRP) or Full Deployment Decision (FDD) –15 pages

The cover page, tables of contents, acronym lists, signature sheets, and executive summaries do not count against these guidelines/limitations.

3. Submission and Review

Even though the Acquisition IA Strategy is an appendix of the PPP, approval of the AIAS is independent of the approval of the PPP, which is approved by separate authorities. The DON CIO requires that the AIAS be approved by the Navy Echelon II or Marine Corps Major Subordinate Command Information Officer prior to formal submission to the DON CIO.

Submitters should plan for 90 days for DON CIO and DoD CIO review and approval of an AIAS and CCA package. To facilitate reviews of Acquisition IA Strategies, Program Offices / Systems Commands should inform the DON CIO of CCA submissions planned for the next two calendar quarters, if possible.

For Acquisition Category (ACAT) ID, IAC, and IAM programs, the DON CIO staff will coordinate the DoD review process. The Program Office representative should reach out early to the DON CIO Cybersecurity (CS) Team to resolve questions or concerns about the AIAS. Both the DON CIO and the DoD CIO CS staffs strongly encourage the Program Office to submit draft Acquisition IA Strategies for early informal review. They will make every effort to promptly review them. A copy of the draft AIAS will also be provided to the respective Echelon II Command Information Officer (Command IO) at the same time it is submitted to the DON CIO for review. Additionally, the respective Command IO will be kept informed during the review process. When submitted for informal review, the DON CIO will solicit a DoD CIO early review (as appropriate) to identify any potential DoD CIO issues early in the process. Approval of the AIAS is an iterative process facilitated by close coordination between the Program Office, the Echelon II CS Staff, and the DON CIO CS Team.

4. Acquisition IA Strategy Approval Process

The approval signature page of the AIAS must include signatures through the appropriate Command Information Officer. The DON CIO signs only the CCA package as a whole (including the AIAS), not the individual parts. The flow of activities and the approval process is described below and illustrated in Figure 1.

a. A Program Office submits the AIAS and, when available, the CCA Compliance Package to the DON CIO, via the respective Command Information Officer.

b. The DON CIO CS Team reviews the AIAS.

(1) Acquisition Category (ACAT) ID, IAC, and IAM programs: The DON CIO CS Team will forward the Acquisition IA Strategy to the DoD CIO for review, after it is

approved tentatively by the DON CIO Director for Cybersecurity. DoD CIO review of Acquisition IA Strategies for these programs is required before DON CIO final approval of the complete CCA Compliance package. The DoD CIO Staff will advise the DON CIO after completion of its review.

(2) ACAT IC and II programs: AIAS approval is at the DON CIO level by the DON CIO Director for Cybersecurity. The DON CIO CS Team will coordinate with the DON CIO CCA Coordinator for input into the overall CCA Compliance package for DON CIO approval.

c. After final approval, the DON CIO Director for Cybersecurity forwards the AIAS to the DON CIO CCA Coordinator, who incorporates it into the CCA Compliance Package for DON CIO signature. The DON CIO will keep the Program Office informed of AIAS and CCA approval progress.

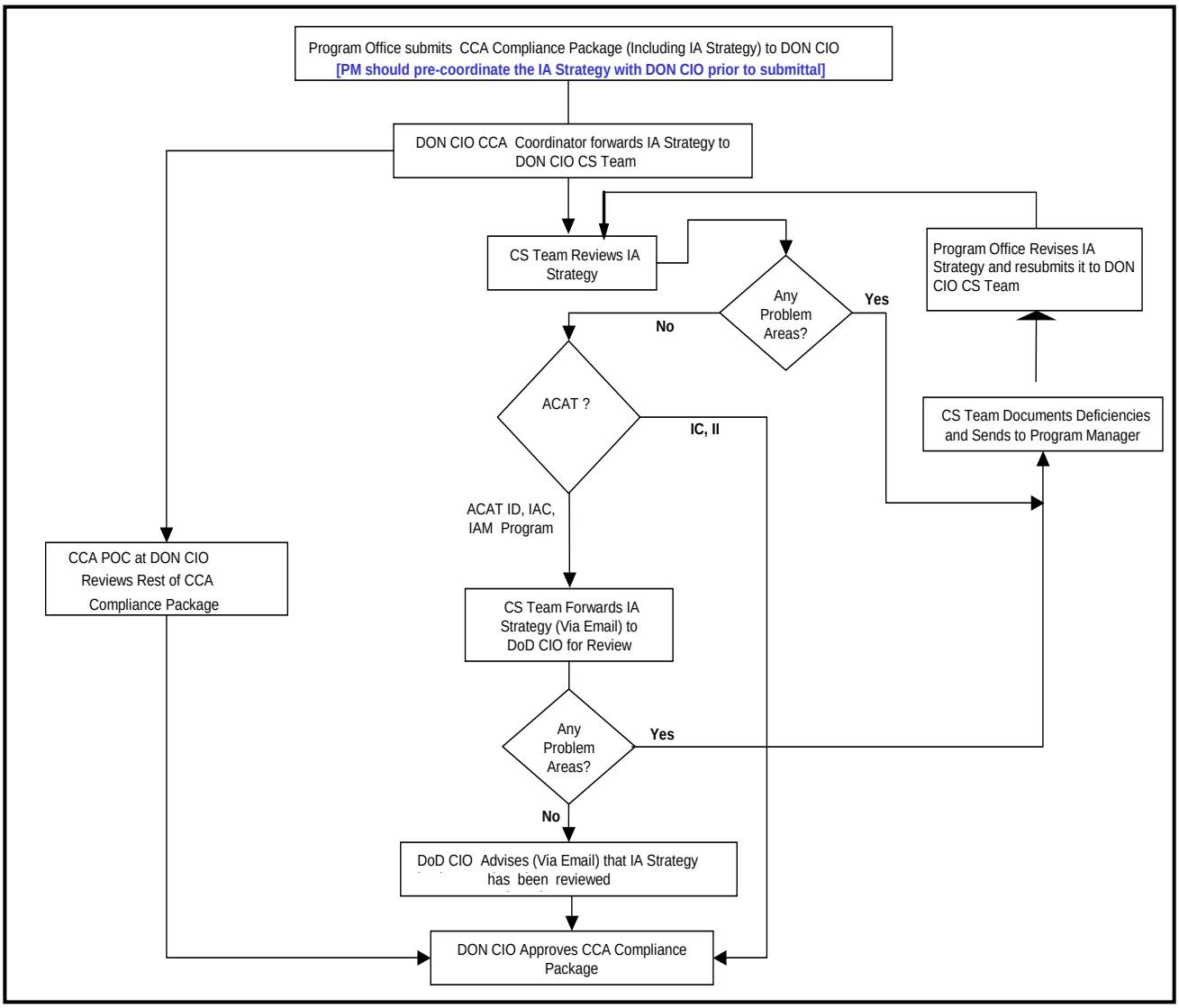

Figure 1 – Acquisition IA Strategy Approval Process

This Page Intentionally Blank

PART (1): DON CIO ACQUISITION IA STRATEGY TEMPLATE

This part provides detailed guidance for completing an Acquisition IA Strategy as required by the Clinger-Cohen Act and SECNAVINST 5000.2E, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System*.

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 Version Number of Acquisition IA Strategy
- Program Address
- Special Handling Procedures/Disclaimer Statements, as follows:

  Distribution authorized to the United States Department of Defense (DoD) and DoD staff and 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.

At a minimum, each page of the AIAS should be marked "For Official Use Only".

TABLE OF CONTENTS (OPTIONAL)

If included, page ii should provide a Table of Contents, including all tables and figures. The document should follow the section titles and numbering scheme found in this template; this section does not count against page limitations.

ACQUISITION INFORMATION ASSURANCE (IA) STRATEGY FOR [PROGRAM NAME]

I. PROGRAM AND SYSTEM DESCRIPTION (Applicable to MS A, B, C, FRP/FDD)

A. Program Information:

Table 1: Program/System Overview

Acquisition Category (ACAT) Level	
Acquisition Life Cycle Phase	
Current Milestone Decision and Date	
Next Major Milestone and Date	
DITPR-DON ID Number & Acronym	
Mission Designation (Mission Critical, Mission Essential, or Mission Support)	
Mission Assurance Category (MAC) and Confidentiality Level (CL)	
Type of System (i.e., AIS Application, Enclave, Outsourced IT-Based Process, Platform IT (PIT) [must provide Operational Designated Accrediting Authority (ODAA) dated PIT approval document], PIT Interconnection - PITI) (**PIT Designation not required for Milestone A**)	
Status of Global Information Grid (GIG) connection: Program *is* or *is not* connected to the GIG	
Risk Management Process to be employed	
Primary Network to which this system will be connected to	

Program Schedule: A graphic representation of the program's schedule (high-level: milestones, major decision points, critical events, DT/OT milestones, spirals/builds if applicable)

B. System Description:

- Brief descriptive overview of the system being acquired, to include the system's function.
- High level diagram of the program and its interconnections. (A DoD Architecture Framework (DoDAF) Operational View level 1 (OV-1) would suffice.).

- Graphic (block diagram) showing the major elements/subsystems of the system/service being acquired, and how they fit together, to include the accreditation boundary and/or the Platform IT (PIT) boundary.
- Interconnection of this program with other IT or systems, as well as primary databases supported.

II. INFORMATION ASSURANCE REQUIREMENTS

A. Sources (Applicable to MS A, B, C, FRP/FDD)

1. Mission Assurance Category & Confidentiality Level

- Brief rationale for the current Mission Assurance Category (MAC) Level. (Part (3) Section 1 provides additional background.)
- Brief discussion of Confidentiality Level (CL) for the system.
- If the system architecture includes multiple segments with differing MAC and CL combinations, include a table listing all segments and their associated MAC and CL designations, as well as a brief rationale for the segmentation.

2. Baseline IA Control Sets

- Identify the applicable sets of baseline IA Controls from DoDI 8500.2 that will be implemented. A listing of individual controls is not required.

3. ICD/CDD/CPD Specified Requirements

- List any specific IA requirements identified in the approved governing capability documents (e.g., Initial Capabilities Document (ICD), Capability Development Document (CDD), or Capability Production Document (CPD), and other Component Specified Requirements).

B. Budget Scope and Adequacy (Applicable to MS A, B, C, FRP/FDD)

- Describe how IA requirements for the full life cycle of the system (including costs associated with certification and accreditation (C&A) activities) are included and visible in the overall program budget. Include a statement of the adequacy of the IA budget.

III. SYSTEM IA APPROACH (high level) (Applicable to MS B, C, FRP/FDD)

A. System IA Technical Approach

- Describe at a high level the IA technical approach that will secure the system.
- Describe how protection and survivability of information will be incorporated into the system design including 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.

- Explain whether system collects, processes, stores, and/or transmits Personally Identifiable Information (PII), including brief description of protection of PII, and if so, whether a Privacy Impact Assessment (PIA) has been submitted. Part (3) Section 2 provides additional guidance.
- Describe whether the system implements DoD-mandated Public Key Infrastructure (PKI) authentication and in the case of a web server, whether it is Public Key Enabled (PKE). Include waiver status if applicable. Part (3) Section 3 provides additional guidance on PKI/PKE.
- Describe Data-at-Rest (DAR) protection.
- Describe Host-based Security System (HBSS) protection. Include waiver status if applicable.

B. Protections Provided by External Systems, Infrastructure, or Policies

- List any protection to be provided by external system or infrastructure (e.g., inherited control solutions).

IV. ACQUISITION OF IA CAPABILITIES AND SUPPORT (Applicable to MS B, C, FRP/FDD)

- Describe how the program's contracting/procurement approach is structured to ensure each of the IA requirements listed below is included in system performance and technical specifications, RFP, and contracts (as well as other agreements such as Service Level Agreements, Memorandums of Agreement, etc.) early in the acquisition life cycle. Describe Original Equipment Manufacturers (OEM) role in lifecycle phases and IA requirements levied in contracts planned for each acquisition phase including intention to require data deliverables supporting C&A of both the product and the facility.
  - System IA capabilities (commercial off-the-shelf-software (COTS) or developmental contract)
  - Government Furnished Equipment/Government Furnished Material (GFE/GFM) (external programs)
  - System IA capabilities as services (commercial or governmental)
  - Information System Security Engineering (ISSE) services
  - IA professional support services to the program (commercial or governmental, including C&A support)
- Confirm that program contacts/agreements communicate the requirement for personnel performing IA roles to be training and appropriately certified in IA in accordance with DoDD 8570.01, SECNAVINST 5239.20, and SECNAV M-5239.2.

V. SYSTEM CERTIFICATION AND ACCREDITATION (C&A)

- **Process** (Applicable to MS A, B, C FRP/FDD)
  - Identify systems or networks to be subject to C&A including OEM owned and operated systems, networks, or enclaves.

- All PIT data may be combined in this section. Part (3) Section 4 discusses PIT guidance. If PIT, must include a description of any PIT Interconnection (PITI) and its accreditation status, including discussion of any required memoranda of understanding or agreement (MOU/MOA) between responsible parties.

- **Key Role Assignments** (Applicable to MS B, C, FRP/FDD)
  - Include the name, title, and organization of the DAA, Certifying Authority (CA), and User Representative for each separately accreditable system being acquired by the program. If the system is to be operated or used by both Navy and Marine Corps personnel, include user representatives from each Service.

- **C&A Timeline** (Applicable to MS B, C, FRP/FDD)
  - Include a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of Interim Authorization to Test (IATT), Interim Authorization to Operate (IATO), and Authorization to Operate (ATO), or if PIT, provide similar information for obtaining a PIT Risk Approval (PRA). Normally, an IATT, IATO (or IPRA for a PIT system) will be issued prior to Operational Test and Evaluation. Please explain if that is not the case.

- **C&A Approach** (Applicable to MS B, C, FRP/FDD)
  - If the program is pursuing an evolutionary acquisition approach (e.g., spiral), describe how each increment will be subjected to the C&A process or PIT process.
  - If the system being acquired will process, store, or distribute Sensitive Compartmented Information (SCI), compliance with Intelligence Community Directive (ICD) 503, *"Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation"* is required. Part (3) Section 5 provides background.
  - Please do not include reiterations of the generic descriptions of the C&A/PRA process (e.g., general descriptions of the DIACAP activities from DoDI 8510.01 and/or the DIACAP Knowledge Service located at https://diacap.iaportal.navy.mil).

VI. IA TESTING

A. Testing Integration (Applicable to MS A, B, C, FRP/FDD)

- Confirm that all IA testing and C&A Activities will be/have been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test & Evaluation Master Plan (TEMP).

B. Product Evaluation (e.g., IA/IA Enabled Products) (Applicable to MS B, C, FRP/FDD)

- List any planned incorporation of IA products/IA Enabled products into the system being acquired, and address any acquisition or testing impacts stemming from compliance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11, "*National Policy Governing the Acquisition*

of Information Assurance (IA) in IA-Enabled Information Technology Products." Part (3) Section 6 provides additional guidance.

C. Cryptographic Certification (Applicable to MS B, C, FRP/FDD)

- List any planned incorporation of cryptographic items into the system being acquired and address any acquisition or testing impacts stemming from the associated certification of the items by the National Security Agency (NSA) or National Institute of Standards and Technology (NIST) prior to connection or incorporation.

VII. IA SHORTFALLS (Applicable to MS B, C, FRP/FDD) (If none, state "None.") (Include as classified annex if appropriate)

A. Significant IA Shortfalls

- Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies.
- Specify the impact of failure to resolve shortfalls in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability.
- If applicable, identify any Acquisition Decision Memoranda that cite IA issues.

B. Proposed Solutions and/or Mitigation Strategies

- If the solution to an identified shortfall lies outside the control of the program office, include a recommendation identifying the organization with the responsibility and authority to address the shortfall.

VIII. POLICIES AND GUIDANCE (Applicable to MS A, B, C, FRP/FDD)

- List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy. Capsule descriptions of the issuances are not required.
- Policies applicable to all programs or systems are listed in Part (3) Section 7.

IX. POINT OF CONTACT (Applicable to MS A, B, C, FRP/FDD)

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

APPENDICES: (Do not count against page limitations)

A. Acquisition IA Strategy Approval by Program Office and Cognizant Command IO

- Approval signatures and dates.

B. Acronym List

PART (2): ACQUISITION IA STRATEGY CHECKLIST

This check list can be used to assist in Acquisition IA Strategy approval. This type of checklist is used by both the DON and DoD CIOs for reviewing Acquisition IA Strategies.

Program Name:
Reviewed By:
Date of Review:
AIAS Version/Date:

I Program Category and Life Cycle Status: (MS A, B, C, FRP/FDD)

- ❑ 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.
- ❑ Characterize the system as to type (e.g., Weapon System, Automated Information System (AIS), enclave, PIT, PITI).
- ❑ Include graphic depicting program schedule showing all major milestones, Spiral Developments Division (SDD) spirals (if applicable), Developmental Test / Operational Test (DT/OT) milestones, and Initial Operational Capability/Full Operational Capability (IOC/FOC) milestones if clarity is needed.
- ❑ Identify system functions and interconnections.

II IA Requirements: (MS A, B, C, FRP/FDD)

- ❑ Identify the system's MAC and Confidentiality Level.
- ❑ Discuss any MAC and CL combinations.
- ❑ Identify Baseline Control Sets.
- ❑ List any ICD/CDD/CPD IA requirements.
- ❑ List any other imposed IA requirements.
- ❑ Identify IA budget scope and adequacy.

III System IA Approach (high level): (MS B, C, FRP/FDD)

- ❑ Describe, at a high level, the IA technical approach that will secure the system,
- ❑ Include any protection to be provided by external systems or infrastructure.

IV Acquisition of IA Capabilities and Support: (MS B, C, FRP/FDD)

- ❑ Describe how the program's contracting/procurement approach is structured to ensure IA requirements are included in system performance and technical specifications, RFPs and contracts (as well SLAs, MOAs, etc.) early in the acquisition life cycle.
- ❑ Describe how the contracts, etc., communicate the requirement for personnel that are trained and appropriately certified in IA, in accordance with DoDD 8570.1.

V System Certification and Accreditation: (MS A, B, C, FRP/FDD)

- ❑ Identify the specific C&A process to be employed (e.g., DIACAP, NISCAP, and DODIIS).

- If PIT without GIG interconnection, describe process to allocate and validate IA requirements prior to operation.
  - If PIT, provide status of approval as PIT by the ODAA.
  - If PIT, include a description of any PITI and its accreditation status, including discussion of any required MOU/MOAs between responsible parties.
- Identify the Designated Accrediting Authority (DAA), Certifying Authority (CA), and User Representative(s).
- Provide a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of IATT, IATO, and ATOs (or PRA) as applicable.
- If the program is pursuing an evolutionary acquisition approach (spiral or incremental development), describe how each increment will be subjected to the C&A process.
- If the C&A process has been started, identify significant activity completed, and whether an ATO, IATO, or PRA was issued.
- If the system will be communicating/processing Intelligence Community information (SCI), 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 the Defense Intelligence Agency (DIA) involved?

VI IA Testing: (MS A, B, C, FRP/FDD)

- Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the TEMP.
- List any commercial off-the-shelf IA or IA-Enabled products, and the program's means for verifying that the product meets the specification and evaluation requirements of DoDI 8500.2 paragraph E3.2.5 (DoD's implementation of NSTISSP No. 11)
- List any planned incorporation of cryptographic items into the system being acquired, including acquisition or testing impacts.

VII IA Shortfalls: (MS B, C, FRP/FDD)

- Identify any significant IA shortfalls, and the proposed solutions and/or mitigation strategies, or insert "None."
- 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.

VIII Policy and Guidance: (MS A, B, C, FRP/FDD)

- 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.

IX Point of Contact: (MS A, B, C, FRP/FDD)

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

PART (3): ACQUISITION IA STRATEGY BACKGROUND INFORMATION

This part of the guidance provides additional or background information to assist in completion of an AIAS submitted to the DON CIO. It includes information on:

1. Mission Assurance Category and Confidentiality Level
2. Privacy
3. PKI and PKE
4. Platform IT (PIT) and PIT Interconnections (PITI)
5. ICD 503 (replacement for former DCID 6/3)
6. Use of COTS/GOTS (DoDD 8500.01E and DoDI 8500.2 Requirements)
7. DoD and DON IA Policies
8. Acronyms used in this template

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. PRIVACY

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.)"

3. 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 Acquisition IA strategies submitted to the DON CIO should contain explicit reference to the program's plans regarding PKE.

DoD and DON policy states that all DON information systems that connect to the GIG, 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.

References:

1. DoDI 8520.03, Identity Authentication for Information Systems dated 13 May 2011, http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf

2. DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling dated 24 May 2011,: http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf
3. DON CIO WASHINGTON DC 211312Z APR 11: DON Public Key Enablement Waiver Request Process for Unclassified Networks, Private Web Servers, Portals and Web Applications, http://www.doncio.navy.mil/PolicyView.aspx?ID=2201

Authors of Acquisition 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 applicable and not being met, a PKI/PKE compliance waiver must be requested following the DON guidance outlined in Ref 3 above.

This section of the AIAS should include a brief summary of the information provided in the waiver request package (including a justification for non-compliance) and reference a high level summary of the 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., Navy Marine Corps Intranet (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,
- Situations where an exception may be warranted based on technical or operational environment constraints,
- Situations where support is required for users who are not eligible to obtain DoD PKI certificates, or
- Situations involving operation intended solely in a tactical or deployed environment where infrastructure components are not yet available.

4. 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, operation, maintenance, and sustainment. The status of PIT designation approval must be included in the AIAS (PIT Designation not required for Milestone A AIAS). Further, PMs 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 2008, which can be found at: http://www.doncio.navy.mil/uploads/ASN_RDA_SETR_Memo_JUN08.pdf .

A thorough discussion of Platform IT Interconnections (PITI) must be included in the Acquisition IA Strategy. The discussion should include for the PITI their accreditation status, and the existence of any Memoranda of Understanding (MOU) or Memoranda of Agreement (MOA) that relate to the accreditation responsibilities of the PITI.

5. 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 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.

6. 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. The policy may be found at the link: http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf . 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 Evaluation and Validation Scheme (CCEVS)), or
  - The Federal Information Processing Standard (FIPS) validation program.
- Acquisitions of government off-the-shelf (GOTS) IA and IA-enabled products are 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 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."

7. DOD AND DON IA POLICIES

The list below contains the minimum policies for which systems must comply. In the case of systems that process SCI, the ICD 503 and DoD Intelligence Information Systems (DODIIS) Security Certification and Accreditation Guide must also be considered. Note that SECNAVINST 5000.2E 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 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."

- DoD Instruction 5000.02, *Operation of the Defense Acquisition System,* found at http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf; with Directive-Type Memorandum (DTM) 09-027 "*Implementation of the Weapon Systems Acquisition Reform Act of 2009*" – the DTM is available at http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-027.pdf.
- SECNAVINST 5000.2E, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System:* http://doni.daps.dla.mil/default.aspx
- 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.
- DoDI 8551.01, *Ports, Protocols, and Services (PPSM),* available at the DTIC web site: http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.
- SECNAVINST 5239.3B, *Department of the Navy Information Assurance (IA) Policy*, available at the Navy Electronics Directives System web site: http://doni.daps.dla.mil/

- 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
- SECNAVINST 5239.20 and associated SECNAV Manual 5239-2 regarding IA workforce, available at the Navy Electronics Directives System web site: http://doni.daps.dla.mil/.
- 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
- For Platform IT, the latest DON CIO PIT Policy of 26 April 2010, located at http://www.doncio.navy.mil/PolicyView.aspx?ID=873
- As appropriate, Navy Ports, Protocols, and Services guidance on the Navy INFOSEC web site, https://infosec.nmci.navy.mil/docs/index.jsp?tab=4&folder=188 (CAC required). (Note that DoDI 8551, *Ports, Protocols, and Services (PPSM)* is being updated to be released sometime in 2012-13.)
- As appropriate, SECNAVINST 5230.15, *Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software*, available at the Navy Electronics Directives System web site: http://doni.daps.dla.mil/.
- As appropriate, DoDD O-8530.1 (*Computer Network Defense – CND*) and CJCSM 6510.01 (*IA and CND*) which require that programs of record (PORs) ensure compliance with mandatory vulnerability patches and actions. (DoD 8530 update is in progress)
- Space systems should include DoDD 8581.1 available at http://www.dtic.mil/whs/.
- As appropriate, ICD-503, discussed in paragraph 5 above.

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/, or the DON CIO web site at: http://www.doncio.navy.mil/.

8. ACRONYMS

ACAT	Acquisition Category
AIAS	Acquisition Information Assurance Strategy
AIS	Automated Information Systems
ATO	Authorization to Operate
C&A	Certification and Accreditation
CA	Certifying Authority
CAC	Common Access Card
CCA	Clinger-Cohen Act
CCEVS	Common Criteria Evaluation and Validation Scheme
CL	Confidentiality Level`

CDD	Capability Development Document
CND	Computer Network Defense
COTS	Commercial Off-the-Shelf
CPD	Capability Production Document
CRD	Capabilities Requirements Document
CS	Cybersecurity
CVMP	Cryptographic Module Validation Program
DAA	Designated Accrediting Authority
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DODIIS	Department of Defense Intelligence Information System
DT/OT	Developmental Test / Operational Test
DTIC	Defense Technology Information Center
DTM	Directive Type Memorandum (normally issued by OSD)
FDD	Full Deployment Decision
FIPS	Federal Information Processing Standard
FRP	Full Rate Production
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
HBSS	Host-based Security System
IA	Information Assurance
IASE	Information Assurance Support Environment
IATO	Interim ATO
IATT	Interim Authorization to Test
ICD	Initial Capabilities Document or Intelligence Community Directive
IIF	Information in Identifiable Form
MAIS	Major AIS (as defined in SECNAVINST 5000.2E)
MAC	Mission Assurance Category
MDD	Material Development Decisions
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS	Milestone
NISCAP	NSA Information Systems C&A Process
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
ODAA	Operational Designated Accrediting Authority
OEM	Original Equipment Manufacturer
OV	Operational View
PIA	Privacy Impact Assessment

PII	Personally Identifiable Information
PIT	Platform Information Technology
PITI	PIT Interconnection
PKI/PKE	Public Key Infrastructure / PK Enabling
POA&M	Plan of Action and Milestones
PPP	Program Protection Plan
PRA	PIT Risk Approval
RFP	Request for Proposal
SCI	Sensitive Compartmented Information
SDD	Spiral Developments Division
SETR	System Engineering Technical Review
SLA	Service Level Agreement
TEMP	Test and Evaluation Master Plan
USD AT&L	Under-Secretary of Defense, Acquisition, Technology, & Logistics