PLATFORM IT GUIDANCE

1. Introduction

1.1 Purpose and Scope

Acquisition guidance detailed in references (a) through (c) states that Major Defense Acquisition Programs (MDAP) and Major Automated Information System Programs (MAISP) that include information technology (IT) always have information assurance (IA) requirements, but these IA requirements may be satisfied through the normal system design and test regimen, and these programs may not be required to comply with the DoD Information Assurance Policy (reference (d)). Reference (d) defines Platform IT (PIT) and states that programs that develop PIT must include IA requirements, but do not have to comply with reference (e). However, references (a) through (e) do not clearly articulate guidance for certification and accreditation of PIT or guidance to integrate IA into the normal system design and test regimen for MDAPs and MAISPs that have been designated PIT.

This document provides guidance to Program Managers (PM), Acquisition Professionals, Information Assurance Managers (IAM), and associated IA professionals to better integrate IA into the acquisition process for MDAPs and MAISPs that will be or have been designated PIT, and ensures that IA is incorporated into the functional design of all systems. For clarity in guidance and to account for differences between SYSCOMs, PEOs, and Programs, the terms "PM" and "IAM" will refer to the program management team and IA professional staff supporting a particular program. This guidebook includes information on the designation process, implementation of IA requirements, and authorization to operate for Platform IT systems.

1.2 Applicability

The guidelines contained herein are applicable to Department of the Navy (DON) MDAPs and MAISPs (including ACAT IV and abbreviated acquisition programs) that have been designated PIT. This document is written in accordance with references (a) through (q); definitions, concepts and interpretation are derived from these sources. This document provides guidance to support standardization of IA across the DON and should be tailored as necessary to support the program under development. If a system is an MAISP or MDAP and designated PIT, but is not required to adhere to the mandates of the DoD Acquisition Process, then that program should comply with reference (e).

1.3 Cancellation

This document supersedes reference (q).

1.4 References

(a) DoD Directive 5000.1, The Defense Acquisition System, May 2003
(b) DoD Instruction 5000.2, Operation of the Defense Acquisition System, Dec 2008
(c) Defense Acquisition Guidebook, Chapter 7, Dec 2004

(d) DoD Directive 8500.01E, Information Assurance Policy, Oct 2002
(e) DoD Instruction 8510.01 Information Assurance Certification and Accreditation Process (DIACAP), Nov 2007
(f) DoD Instruction 8500.2, Information Assurance Implementation, Feb 2003
(g) DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System, Jul 2004
(h) DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program, Dec 2005 (Change 1 incorporated May 2008).
(i) SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy, Dec 2004
(j) SECNAV M-5239.1 Department of the Navy Information Assurance Program, Information Assurance Manual, Nov 2005
(k) DON CIO Platform IT Policy Memorandum
(l) Navy CA Navy Certification Agent Qualification Standards and Registration Guidebook, Version 1.1 (Revision A), Feb 2008
(m) CJCSI 3170.01F Joint Capabilities Integration and Development System, May 2007
(n) Risk Management Guide for DoD Acquisition, Sixth Edition, Version 1.0, Aug 2006
(o) Naval SYSCOM Risk Management Policy, Jul 2008
(p) DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), Jun 2004
(q) Navy CA Platform IT Clarification Guidance, May 2007

1.5 Acronyms and Definitions

Refer to Appendix G.

2. Platform IT Designation

This chapter provides guidance to the PM and IAM intended to define terms and describes the process for obtaining a statement of exemption from the C&A process for IT systems and IT components designated as Platform IT (PIT). Per DoDD 8500.1, the C&A process (e.g., DIACAP) is applicable to all DON-owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of MAC, classification or sensitivity, except - per DoDD 8500.1 Paragraph 2.3 - IT that is considered Platform IT.

2.1 Stand-Alone Systems

Per DoDD 8500.1, systems having no external connections (stand-alone systems) are subject to the C&A process unless they have been designated as PIT. For stand-alone systems that have been designated as PIT, the processes outlined in this guidebook should be followed.

2.2 Actions Required of Program Managers

To obtain a designation of an IT system or IT component as Platform IT, the PM should follow the procedures in this guidebook. The system will be evaluated against the definition of Platform IT and the final designation statement will be issued by the Operational Designated Accrediting Authority (ODAA) or Marine Corps Enterprise Network Designated Accrediting Authority (MCEN DAA).

2.3 Process Steps

The PIT Designation Process is shown in Figure 1. To initiate the PIT Designation process, PMs need to submit the following information:

- Identify the special purpose system, including its Name, Acronym and Version Number
- Complete the Platform IT Determination Checklist provided in Appendix A
- Describe the special purpose system and its mission. In addition to a brief, textual description, include a high-level block diagram of the system that also depicts the PIT boundary. The diagram should allow the Certification Authority (CA) and DAA to clearly understand and identify the system's hardware, software and other components, as well as any interconnection with other systems, networks or IT. For systems with multiple variants, if the diagram accurately describes the variants then a single diagram may be submitted to cover multiple variants. The diagram should clearly identify the system and any variants it describes.
- The PM's justification and rationale should include supporting statements that describe how the system meets the criteria for PIT.
- Request evaluation to determine if the IT system or IT component is Platform IT.

The completed PIT Determination package is submitted to the cognizant Echelon II (EII) or Major Subordinate Command (MSC). EII/MSC will review the package to determine if the package is complete and if the system/component meets the PIT determination criteria. At this point, the EII/MSC will either:

(1) Return the request to the PM to address any identified package deficiencies

-or-

(2) Endorse and forward the request to the CA

If the package is forwarded to the CA, they will either:

(1) Return the request to EII/MSC to address any identified issues

-or-

(2) Endorse the request and forward it to the ODAA/MCEN DAA for final determination and designation of Platform IT

The ODAA/MCEN DAA will review the package and the CA's assessment, and issue a statement to the PM classifying the IT system or IT component as Platform IT, or the ODAA/MCEN DAA will explain why the system does not meet the criteria for Platform IT.

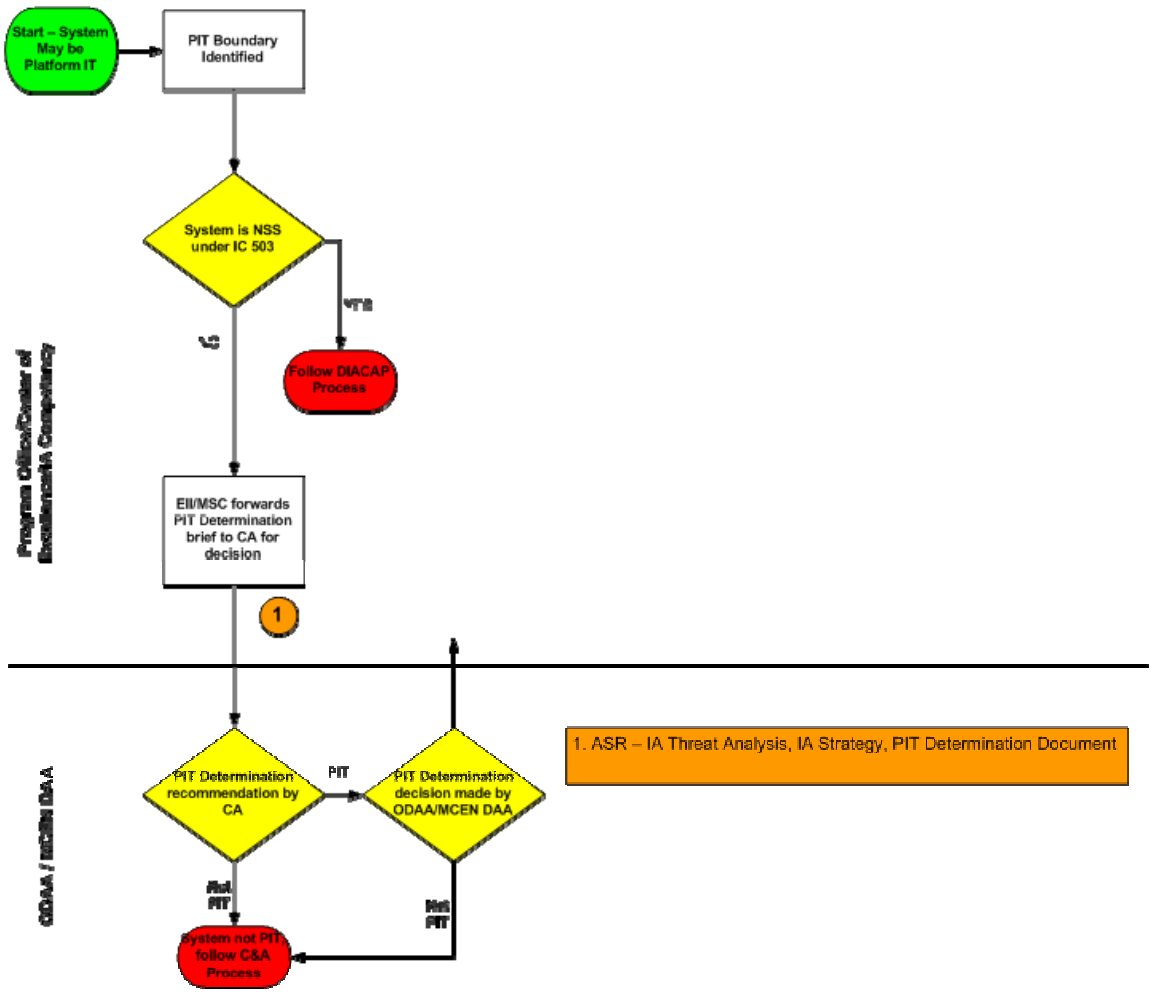


Figure 1 PIT Designation Process

3. Objectives and Implementation of IA into Platform IT Design

3.1 IA Objectives

The objective of this chapter is:

- to help the PM understand why he needs to consider information assurance principles during the development of his program strategy
- to help the PM and IAM/IAO understand where he needs to go to find information and guidance for developing an Information Assurance Strategy
- to help the PM and IAM/IAO understand the resources (in terms of funding and personnel) that are required to effectively implement information assurance.

PM's and Program Lead Systems Engineers who are unfamiliar with the details of the DoD IA regulations and policies may find it easier to consider the following five principles when trying to balance specific IA requirements with the other requirements that apply to their system:

- **Confidentiality** - Only authorized persons gain access to the information received, processed, stored or published by the system.
- **Integrity** of the information received, processed, stored or published meaning it has not been altered either by defect or malicious tampering.
- **Availability** of the information received, processed, stored or published to those who need it when they need it.
- **Non-repudiation** by those who gain access to the information received, processed, stored or published by the system so that they can not deny having interacted with the system or its information.
- **Authentication** of those who gain access to the information received, processed, stored or published by the system. Authentication takes confidence to the next level and imposes more specific and rigorous requirements for access.

Moreover, it is critical to understand that IA extends beyond the bounds of information security, to also include:

- Sound Engineering – include design features that promote stability and security
- Training and Awareness – should provide Fleet with proper training to ensure they are vigilant
- Response, Recovery, and Restoration - actively respond to internal and external malicious attacks, as well as recover from system failures caused by inadvertent operator error, internal and external malicious attack, and major calamities

3.2 IA Implementation

The first part of the IA Implementation Process is shown in Figure 2. Once a PIT determination has been issued for a particular system in writing by the ODAA/MCEN DAA, the PM is responsible for ensuring due diligence in meeting information assurance requirements throughout the lifecycle of the program. The process is intended to be tailored to the individual program, in

keeping with the resources available to the program. While the process assumes that the program is following the guidance provided in references (b) and (c), that does not imply that every PIT system is an ACAT program, or part of an ACAT program. For those systems that are not required to comply with references (a) through (c), the DIACAP artifacts (DIP, Scorecard, and POA&M) should serve as the reporting templates for tracking IA compliance for the delivered PIT system.

For the purposes of IA implementation into PIT programs, the Acquisition Process can be broken into three distinct sub-processes, each having specific documentation in which IA should be clearly articulated:

a) Requirements Generation (Joint Capabilities Integration and Development System – reference (o)): Identification of the required capabilities, key performance parameters (KPP) including the IA element of the Net-ready KPP (NR-KPP), as required, and key system attributes, which are included in the Initial Capabilities Document (ICD), the Capabilities Description Document (CDD)/ Capabilities Production Document (CPD), the Information Support Plan (ISP), and the Test and Evaluation Master Plan (TEMP); these documents are covered in more detail in Appendix C.

b) Acquisition and Program Management: Oversight of the key acquisition and program management processes and documentation, to include, but not limited to the Acquisition Strategy (AS), Acquisition Program Baseline (APB), Information Assurance Strategy (IAS), Contracts, Requests for Proposal (RFP), Training Plan, Integrated Logistics System (ILS), etc.; these documents are covered in more detail in Appendix C.

c) System Engineering: Implementation of a disciplined systems engineering process from requirements analysis through design, test, fielding, sustainment, and decommissioning. The system's functional design, including the information assurance design, will be captured in design documentation, such as the System Design Document (SDD) and other lower level technical specifications. All technical documentation will be reviewed during prescribed program technical design reviews governed by the System Engineering Technical Review (SETR) Process, which is discussed in paragraph 3.13 and Appendix E, in more detail.

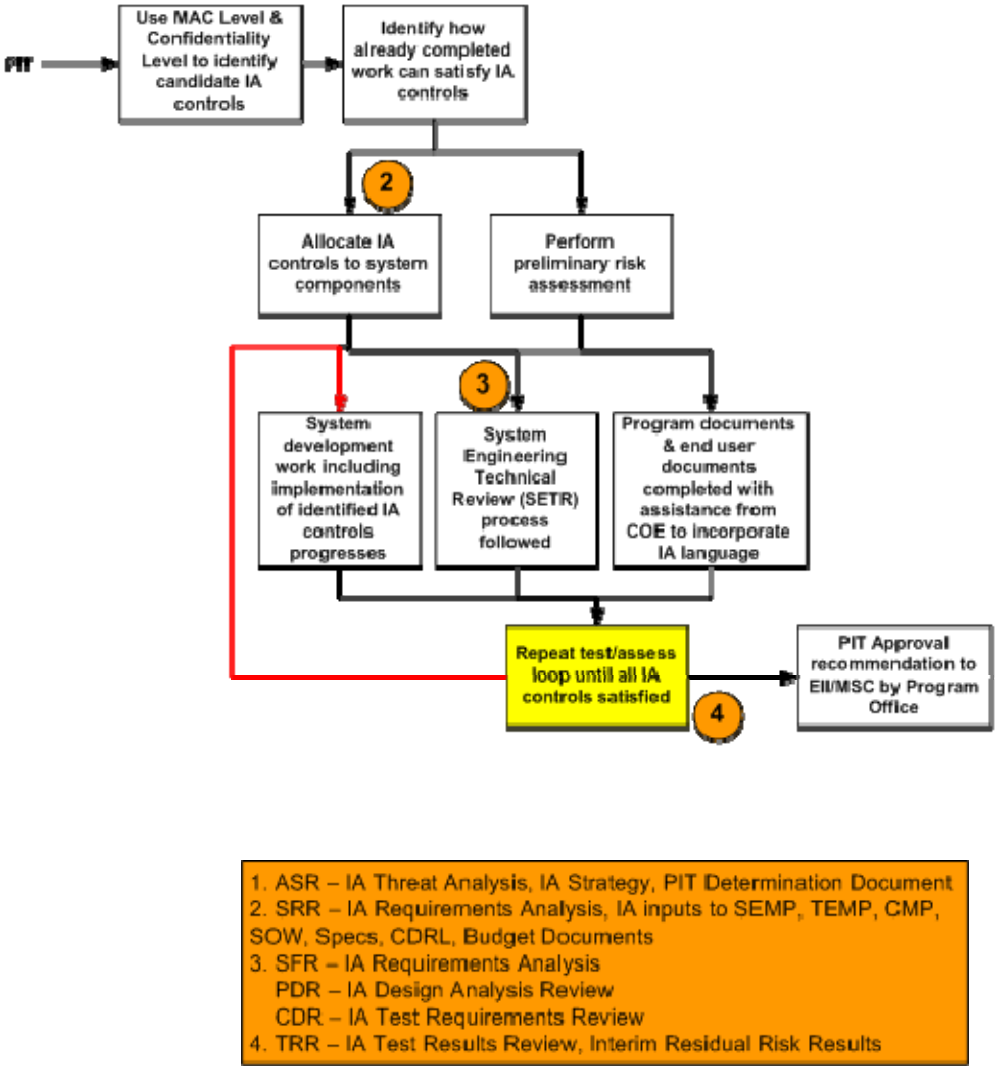


Figure 2 PIT IA Implementation Process Part 1

3.3 Program Manager (PM) Roles and Responsibilities IA Strategy Considerations for Program Acquisitions

In accordance with references (a) through (k), the PM is responsible for allocating and managing a budget sufficient to engineer information assurance requirements into the system alongside other system design requirements. DoD guidance specifically directs the PM to ensure "Information Assurance is traceable as a programmatic entity in the Planning, Programming, and Budgeting System (PPBS) and visibility extended into budget execution." This includes ensuring that appropriate types of funding are allocated (e.g., Research and development funds for system design, Operations & Maintenance for maintaining IA posture in the out-years, etc.). PMs should identify cost of integrating IA into the system design, to include, but not limited to the cost of:

- The cost of integrating IA into existing acquisition documentation

- Information Systems Security Engineering (ISSE) support, IA development/procurement, IA test & evaluation, and IA implementation into system architecture.
- Operations and maintenance related to maintaining the IA architecture and system security posture following fielding. (The PM may need to communicate these specific O&S costs to the appropriate resource stakeholders in order to ensure that the system will be operationally suitable.)
- Development, procurement, test, certification and accreditation, and maintenance of IA solutions

The PM is responsible for assigning an Information Assurance Manager that is qualified in accordance with reference (h). In accordance with reference (d), the IAM needs to be assigned in writing. The Program Manager or System Manager should ensure that the designated IAM has the support, authority, and resources to satisfy the responsibilities established in DoDD 8500.1.

Assignment of a qualified IAM is one of the most important steps and should be accomplished as early as possible to ensure that applicable IA requirements are addressed in the system architecture and detailed design.

The PM is responsible for the system security architecture in accordance with DoDI 5000.2 and DoDI 8500.2:

- When the program is Pre Milestone A, the PM's team should examine program and system characteristics to determine whether compliance with DoD Directive 8500.1 is recommended or required, and whether an acquisition IA strategy is required.
- When the program is Pre Milestone B, the PM should ensure that IA considerations are incorporated in the program's Acquisition Strategy.

The PM is responsible for ensuring that all appropriate Information Assurance (IA) policy and guidance is addressed in the Program's Information Assurance Strategy. Additional information on developing an Information Assurance Strategy can be found in Section 7.5.9.4 of reference (c).

The PM is responsible for ensuring that IA requirements are clearly communicated to offerors in the program's solicitations and contracts.

The PM is responsible for ensuring that IA requirements will be addressed throughout the system life cycle.

3.4 IA Manager (IAM) Roles and Responsibilities

Reference (h) provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce and should be used for selecting an IAM. As the PM's agent for ensuring compliance with DoD's information assurance policies and regulations, the IAM's roles and responsibilities include:

- Ensuring compliance with IA requirements in accordance with references (a) through (k)
- Supporting the PM in development of a program plan of action, milestones, and budget that addresses the implementation of information assurance requirements throughout the life cycle of the system

- Identifying an information assurance team
- Assigning and ensuring Certifier/Certification Agents are qualified in accordance with reference (h)
- Assigning IA responsibilities to qualified certifiers
- Ensuring that system security engineering processes are aligned to, and adequately documented in, the program's Systems Engineering Plan (SEP), and are executed with sufficient rigor to ensure required IA Controls are implemented, which culminates in the lowest level of residual risk to system operation.
- Ensuring that information assurance inputs to program acquisition documents are prepared. Section 7.5 of reference (c) provides specific detail on IA milestones
- Ensuring that the program's contractual documents, such as specifications, statements of work, or Contract Data Requirements Lists (CDRLs) incorporate appropriate Information Assurance language and requirements.
- Supporting Systems Engineering Technical Reviews by ensuring that entry and exit criteria include information assurance, that the IA entry and exit criteria are satisfied, and that design documentation meets the specified IA requirements
- Ensuring that information assurance controls and requirements are properly allocated and documented in design specifications, technical publications and manuals, etc.
- Ensuring information assurance controls and requirements are properly allocated and implemented in logistics or program planning documents
- Ensuring that information assurance controls and requirements have been communicated and appropriately resourced by program budget documents and are reflected in the program's requirements database.
- Ensuring that integrated logistics support documentation incorporate Information Assurance considerations throughout the life cycle of the system (see Appendix F).

3.5 IA Strategy Considerations for Program Acquisitions

An IA Strategy is mandatory for all mission critical and mission essential information systems as part of the Clinger Cohen Act Compliance certification/confirmation required for each program milestone. Mission Support systems as defined by reference (j) are not required to have an approved IAS.

The Program's IA Strategy is an integral part of the program's overall acquisition strategy, identifying the approach to integrating IA into the function design of the system under development. The IA Strategy should describe the program's strategy for complying with DoD and DON requirements, and provide a high level overview of the program's strategy to address integration, test, and certification of IA requirements in the normal system design and test regimen of the program. DON CIO has published a specific format for the IA Strategy, which is covered in greater detail in Appendix C.

3.6 Threat Analysis

For the purposes of IA, a "threat" is best defined as a tool, technique, or methodology that can be used to compromise or inflict damage to the information system or the information being processed. An IA threat analysis results in a specific list of tools, techniques, and methodologies that can be used to target the system under development. The PM should consider the risk of attack from these threats and provide a plan to counter these threats. If the PM is unable to counter these threats, ample justification in writing should be provided to and approved by the DAA.

In order to conduct an information assurance threat analysis, the engineer should start with a defined list of threats (i.e., methods, tools, and techniques) that can be used to attack the information system or the information being processed. This list may be held by the Joint Task Force – Global Network Operations (JTF-GNO), National Threat Operations Center (NTOC), Office of Naval Intelligence (ONI), Naval Information Operations Command (NIOC), Systems Command (SYSCOM) IA competency or other authoritative source. A PM may have to compile the list of threats from several authoritative sources. Each threat should be evaluated for applicability to the system or information being processed (i.e., Can the tool, technique, or methodology be used to attack the system or the information being processed by the sytem?), and if applicable, assigned a value of high, medium, or low. The finalized list of applicable threats should be included in the overall threat list for the system. The IA threats to the system should be continually reviewed and updated throughout the life cycle of the system. This list of applicable threats will be used to support IA risk assessments.

3.7 Mission Critical, Essential or Support Designation

The acquisition priority decision determining mission critical (MC) or mission essential (ME) has been delegated down to system owners, major claimants and program managers within DON. Mission Support (MS) is unique to DON and was introduced in reference (j). The IAM should assess the impact of the system designation as MC/ME/MS to the program's intended IA implementation. If IA implementation is significantly impacted by the system designation as MC/ME/MS, then the IAM should communicate that impact to the program manager via the program's risk management process.

3.8 Mission Assurance Category and Confidentiality Level

The determination of the Mission Assurance Category (MAC) and Confidentiality Level (CL) is described in Enclosures E2 and E4, respectively, of reference (f).

Mission Assurance Categories are defined as:

- **Mission Assurance Category I (MAC I)** Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

- **Mission Assurance Category II (MAC II)** Systems handling information that is important to the support of deployed and contingency forces.

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

- **Mission Assurance Category III (MAC III)** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.

The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

3.9 IA Requirements Analysis and Definition

DON policy requires all programs to implement IA. All programs should start with the minimum set of IA controls delineated in reference (f), based on MAC and CL. There are a number of factors that impact the selection of a system's high-level IA requirements:

- Results of IA Threat Analysis for the system under development
- MAC and CL determination for the system under development, as well as the sub-network and platform network into which the system under development will be integrated
- Functional decomposition and allocation of IA Controls delineated in reference (f) to the Objective Defense-in-Depth Architecture for the platform network, sub-network, or system into which another system is to be integrated
- System design features (key performance parameters and key system attributes) that promote stability and security
- Operating environment (i.e., platform) of the system under development
- Operational and procedural solutions that may mitigate threats to the system

The government retains the responsibility and authority for identifying, selecting, and approving the appropriate IA requirements for consideration in the system design; however, industry expertise may be called upon to evaluate the many factors impacting the IA design, and to make recommendations as to which IA requirements should be incorporated into the design of the system. To ensure IA requirements are considered in the functional design of the system, contracts, Statements of Work, and RFPs need to delineate specific tasks and deliverables in support of IA.

Once the high-level IA requirements have been identified, the finalized list should be included in the CDD/CPD. In parallel, the requirements should be captured in the program's requirements management database (e.g., DOORS) that permits development of a requirements traceability matrix (RTM).

In the case where the system under development is following non-SETR based process, the DoDI 8510.01 mandated DIACAP artifacts should be used to document the system's IA

requirements and compliance. Identification of IA requirements for a PIT system should be completed prior to the system completing its Material Solution Analysis Phase.

3.10 Functional Decomposition and Allocation of IA Requirements into System Requirements

The IA controls, key performance parameters and key system attributes, including IA design features, will be functionally decomposed and allocated to various elements within the system, the sub-network, and the platform network, as well as to the platform. (See a more detailed discussion of the Objective IA Defense-in-Depth architecture in Appendix B.) Even though an IA requirement will be inherited from the platform, the platform network, the sub-network, or system, it still needs to be documented in the requirements database so that the program RTM accurately reflects the IA requirements flow down from the objective Defense-in-Depth architecture to the system under development. The program RTM also needs to consider any PIT Interconnections (PITI) used to connect the PIT to non-PIT systems, as PITI are subject to C&A and may impose IA requirements on the PIT system.

In addition to the elements normally found in the RTM, IA unique tracking elements should be maintained within the RTM. These elements include the DoD 8500.2 IA Control Numbers, the IA Test Procedure Numbers, and the IA Test Procedure Names, as applicable. (These IA unique elements will support development of DIACAP artifacts, if needed.)

It is important to note that the IA elements in the RTM should not be treated as a separate set of requirements, but rather a sub-set of the program's RTM. The IAM should exercise caution to ensure that the IA sub-set of the RTM is always generated from the program's RTM. It is also important to ensure that IA requirements are updated using a single, authoritative requirements database that is under strict configuration management.

The program IAM needs to provide rationale for all IA requirements that cannot be met or are identified as not applicable.

3.11 Design and Development

System Engineers need to ensure that functional design considerations integrate IA functional requirements and that these requirements are included throughout the development process. The SETR process will incorporate IA entrance and exit criteria into the entrance and exit criteria for each design review. The Design Review Chairperson will validate that the IA technical requirements are included in design documentation and that all entrance and exit criteria, including the sub-set of entrance and exit criteria for IA, are satisfied. System trades will consider and prioritize IA requirements against all other system design requirements. Technical requirements (including IA) that cannot be met should be assessed for the risk to the program and risk to the performance of the system. Risk assessments should be conducted and the results brought to the attention of the PM and Resource Sponsor.

Commercial-Off-The-Shelf (COTS) IA products and IA-enabled products should be certified compliant with National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) by labs accredited 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, Government Off-The-Shelf

(GOTS) IA products or IA-enabled products employed by the system should be evaluated by the NSA or in accordance with National Security Agency (NSA) approved processes.

3.12 Configuration Management

Configuration Management is critical to ensuring a successful system design and development process. Controlling and documenting changes in design throughout the analysis, development, and testing process requires strict adherence to an established configuration management process. The configuration management process needs to include changes made to the IA configuration and associated documentation. Failure to include IA considerations in the configuration management and engineering change control processes could adversely affect the program's ability to integrate and maintain IA in the functional design of the system.

3.13 Risk Assessment

There are two kinds of risk assessment:

- Program Risk
- Risk to the Information Assurance posture of the platform or enterprise

Program risk is associated with cost, schedule and performance. Performance is often discussed in terms of technical risk, and, in fact, the terms "performance" and "technical" are interchangeable when discussing program risk. For the program risk, security and IA fall into the category of technical risk.

In accordance with reference (n), DoD has directed programs to develop a Risk Management Program, which the system commands have further refined by reference (o). The SYSCOM policy provides information on how to assess program risk. The following paragraphs will discuss how a program assesses the IA risk to the Defense-in-Depth architecture of the platform network. The analysis of IA risks, in addition to supporting the IA Program, should also support the Program's Risk Management Process and is utilized in the SETR. The IAM should be an active participant in the Risk Management Program.

Information Assurance risk assessment can be broken into two constructs:

1) Hardware and Software Functional Design Risk – design features and performance parameters, that are not, in of themselves security measures or related to security measures, but promote stability and security. For instance, information availability may be directly impacted by Operational Availability (A_o)

2) Security Risk – protective measures that reduce the risk from internal or external attack (malicious, accidental or natural); protective measures include firewalls, intrusion detection and protection systems, network analysis tool, access controls list, password implementation, etc.

The IAM provides the subject matter expertise to plan and execute IA risk assessment and structured testing that demonstrates satisfaction of IA requirements. These functions will be executed using established methods and procedures and industry best practices. The IAM needs to communicate the status of technical IA risk assessments to the PM as new risks are identified and old risks are retired.

A more detailed discussion of technical IA risk assessment is provided in Appendix F.

3.14 IA Validation and Test

3.14.1 IA Validation

In preparation for each technical review, the DAA will direct a technical risk assessment of IA, based on sound engineering judgment and incremental testing to validate implementation of IA controls, key system attributes, and performance parameters. Using the completed IA risk assessment, the DAA or his/her designated representative will validate the IA design of the system and report those findings to Milestone Decision Authority, the SYSCOM/PEO Technical Director, and the PM.

3.14.2 Integrated, Incremental IA Testing

Systems need to be tested for compliance with all IA controls - Administrative and Management Controls (AMC), Technical Controls (TC), and Operational and Procedural Controls (OPC) - as well as all performance parameters. There are a variety of test methods, to include, but not limited to: application of the automated tools/ Security Readiness Review Evaluation Scripts, such as the DISA Gold Disk and static code checker/scanner; manual tools to include DISA Security Checklists and Security Technical Implementation Guides (STIGs); test tools utilized to test network appliances and related device; software endurance tests; hardware reliability tests, etc.

However, due to the high cost of system testing associated with laboratory use and field/Fleet assets, it is essential that IA testing be integrated into routine test objectives and test plans flowing from the TEMP. IA operational and technical requirements should be integrated into standard test objectives and test plans alongside other key performance parameters and key system attributes, so as to leverage system time and execute efficient tests that demonstrate the required performance of the functional design.

Program Office compliance with AMCs will be validated by the appropriate higher authorities, such as the Acquisition Executive (AE)/Milestone Decision Authority (MDA) or their designated representatives, during normally scheduled program reviews. The Program Office is evaluated to ensure the key acquisition principles of sound planning, budgeting, and execution include Information Assurance throughout the life cycle of the system.

Platform or system compliance with AMC will be validated in the operational environment by, for example, Type Commanders, in conjunction with existing field/Fleet assessments. Evaluations in the operational environment will ensure the AMC for a given platform includes logical security, physical security, personnel security, CMS-H, TEMPEST, COMSEC, OPSEC, and TRANSEC procedures, as well as recovery and restoration procedures in the event of a casualty.

Incremental testing of TCs will occur in conjunction with routine engineering tests (ET), development test (DT), and operational test (OT) of the system's functional design, culminating, in many cases, in a technical evaluation (TECHEVAL), followed by an operational evaluation (OPEVAL). Testing of IA objectives during ET or DT can take place in a lab using modeling and simulation tools, emulated tactical code, or onboard the platform using prototype systems. Once an IA test objective has been satisfactorily demonstrated during testing, it need not be tested again, unless it is determined that changes in system design could impact the security posture or there is a need to demonstrate the objective in the higher level sub-networks or

platform network. In addition to TCs, there will be a number of design features and metrics that define system performance in the areas of Availability and Integrity. These performance parameters will also be tested in conjunction with routine ET and DT of the system's functional design. Test results from the testing of TC and IA performance parameters will be used as the basis of the IA Risk Assessment.

Incremental testing of OPCs will occur in conjunction with routine DT of the system's performance, as well as in an operational environment. Though an operational or procedural test objective may have been met in a lab environment, it may be necessary to check it again during OTs and/or OPEVAL onboard the platform.

Incremental testing of inherited controls may be partially demonstrated in a lab environment to validate that specific materiel solutions work as expected; however, all inherited controls need to be tested in the operational environment in order to verify that the Defense-in-Depth architecture protects the system. In the event of system upgrades that have no bearing on the IA posture of the platform network, sub-network, or system, it may be possible in some instances to justify that no additional testing of inherited controls is required.

3.14.3 Test Plans and Reports

All IA requirements identified in the RTM need to be traceable through the development process and validated during testing. This includes ensuring that IA requirements defined in the RTM are traceable to the program's incremental test plans. Early in the test planning process, the IAM should work with the T&E director to identify ET, DT, and OT events which will lend themselves to accomplishing IA test objectives in conjunction with scheduled testing. System test plans for routine testing will include IA test objectives and procedures to ensure an integrated test approach. Detailed test procedures will include, but not be limited to:

- Information Assurance Requirements
- Test Methodology
- Test Procedures
- Test Results
- Residual risk if no technical or procedural solution identified
- Risk Mitigation (primary, alternate, if available)
- Residual Risk once technical or procedural solution is applied

An example of a Test Report Format is shown in Figure 3.

Figure 3 Sample Test Report

The DIACAP Impact codes, indicated with an asterisk (*) in Figure 3, are:

High Impact Code. The absence or incorrect implementation of this IA Control may result in the loss of information resources, unauthorized disclosure of information, or failure

IA Control	Validation Procedure Number	Procedure Name	Procedure Objective	Procedure Preparation	Procedure Script	Expected Results	Actual Results	Impact Code (Risk)
DCSD-1	DCSD-1-2	IA Documentation Appointments	Ensure that all appointments to required IA roles (e.g., DAA and IAM) are documented in writing, to include assigned duties and appointment requirements criteria such as training, security clearance, and IT-designation.	1. Obtain a copy of all relevant system security documentation, or other documentation that identifies the required IA roles for the DoD information system. 2. Obtain a listing of all personnel currently assigned to IA roles within the system.	1. Review the system security or other documentation to ensure that all appointments to required IA roles are documented in writing. 2. Check to ensure that the documentation identifies assigned duties and appointment requirements criteria such as training, security clearance and IT-designation. 3. Record the results.	All appointments to require IA roles are established in writing and include assigned duties and appointment criteria.		High **(*)**

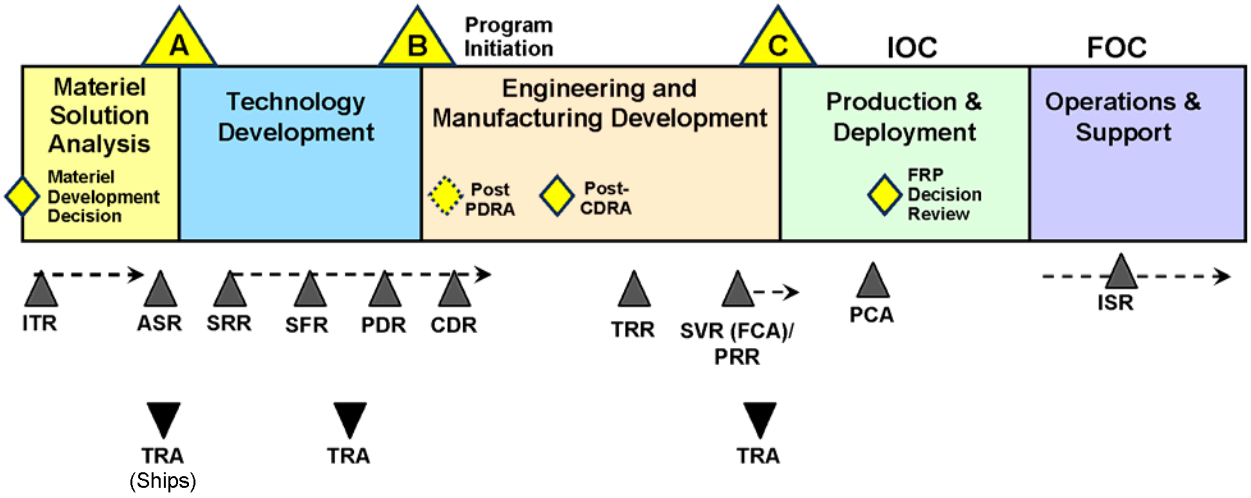
to maintain information integrity. Such exploitation may severely disrupt or impede situational awareness, management, and control; system operations; or user access.

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

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

3.15 System Engineering Technical Review (SETR) Process

The System Engineering Technical Review (SETR) process, as depicted in Figure 5, is an integral element of the Acquisition Process and life cycle management. Technical reviews coincide with, and support, key acquisition milestone decisions and gate reviews within the Acquisition Process, and provide an independent assessment of emerging designs against plans, processes, standards and specifications, and key knowledge points in the development process. One of the key objectives of the SETR process is to identify issues early in the design and development phase of acquisition and ensure that PMs are aware of the issues and have developed mitigation plans to resolve those issues.



- Initial Technical Review (ITR)
- Alternative Systems Review (ASR)
- Systems Requirements Review (SRR)
- System Functional Review (SFR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Post-PDR Assessment (Post-PDRA)
- Post-CDR Assessment (PCDRA)
- Test Readiness Review (TRR)
- System Verification Review (SVR)
- Functional Configuration Audit (FCA)
- Production Readiness Review (PDR)
- Operational Test Readiness Review (OTRR)
- Physical Configuration Audit (PCA)
- Technology Readiness Assessment (TRA)
- In-Service Review (ISR)

Figure 4 SETR Process

An integrated team of independent, subject matter experts conducts technical reviews. Engineering rigor, interdisciplinary communications, and competency insight are applied to the maturing design to assess and validate requirements traceability, product metrics, and technical adherence to standards and specifications. This team should include an IA professional having experience with the special purpose system under development. The IA professional will be tasked to evaluate the system design and artifacts against the pre-defined set of entrance and exit criteria for the specific review (i.e., ITR, ASR, SRR, etc.). Technical reviews support decisions to proceed with planned program events. Failure to pass the entrance and exit criteria of a SETR event usually results in immediate management attention on the un-satisfied criteria by both the government and contractor team.

A more detailed discussion of the SETR process, roles and responsibilities, entrance and exit criteria, and technical documentation is provided in Appendix E.

4. Platform IT Authority to Operate (ATO)

A PIT system will need to receive the authorization to operate from the appropriately designated PIT DAA. This section describes the documentation that will need to be submitted, and the process for submitting it to the PIT DAA.

4.1 Minimum Artifacts for PIT ATO

For systems following the acquisition process, the program should ensure that the PIT DAA is involved in the review of the acquisition documentation that includes relevant IA information, and that the PIT DAA (or their designee) participates in critical milestone and gate review decisions. When this has been the case, the minimum set of artifacts required to obtain an ATO should be the following:

- A diagram describing the Defense-in-Depth IA architecture of the platform network, sub-network, and system based on the actual installation configuration
- IA portions of TECHEVAL/OPEVAL Report for system, sub-network, and/or platform network
- IA Residual Risk Report
- IA Risk Mitigation Plan, if applicable

For those PIT systems that did not adhere to the acquisition process and did not generate the standard acquisition documentation products, the program should submit to the PIT DAA the standard DIACAP documentation based on implementation of reference (f) controls for the determined MAC and CL. The following set of information should be included in the set of artifacts:

- Designation of Mission Critical or Mission Essential Information System (IAW DoD 5000.2)
- MAC level (IAW DoDI 8500.2)
- Classification(s) of data (IAW DoDI 8500.2)
- IA Controls Compliance Status (IAW DoDI 8500.2)
    - IA Controls not applied should include rationale (e.g., restrictive architecture / negative system impact, etc.)
- POA&M for IACs not applied, if applicable

In summary, programs that have been designated PIT are only required to submit one set of IA artifacts: either the required acquisition process documentation as delineated in references (a) through (c) and modified by this guidebook, or the DIACAP artifacts, as specified in reference (e).

4.2 PIT DAA Authorization Process

The IAM should prepare the Risk Acceptance Letter and the PM will need to submit this request letter along with the minimum set of IA artifacts (listed above) to the PIT DAA.

Similar to how non-PIT systems are handled; the PIT DAA will review the IA artifacts and provide the PM with one of the following:

- PIT ATO (citing the conditions or limitations of operations, if necessary)
- PIT Interim Authorization to Operate (IATO) or PIT Interim Authorization to Test (IATT) (citing the period for which the PIT IATO/IATT is valid and the conditions and/or limitations on operations, if any)
- PIT ATO/IATO Rejection (citing the justification for rejection, any actions that need to be completed, and/or deficiencies that need to be corrected before and an ATO or an IATO will be granted)

4.3 Transition of Responsibility from PIT DAA to ODAA/MCEN DAA

TBD

5. Sustainment and Post-Implementation of PIT Systems

5.1 Introduction

Effective sustainment of PIT systems, including the Defense-in-Depth architecture, begins with the design and development of reliable and maintainable systems through the continuous application of a robust systems engineering methodology that focuses on total system performance. This applies to all PIT systems. Sustainment needs to occur in parallel with development, and end users need to be represented and provide feedback to the SETR process. Appendix F describes several of the key considerations for Integrated Logistics Support that IA professionals should take into account.

A conceptual sustainment process, which includes IA in the mix of other system engineering disciplines, is depicted in Figure 1 below. Note that the process aligns to the logistics analysis process for reliability, maintainability, and availability.

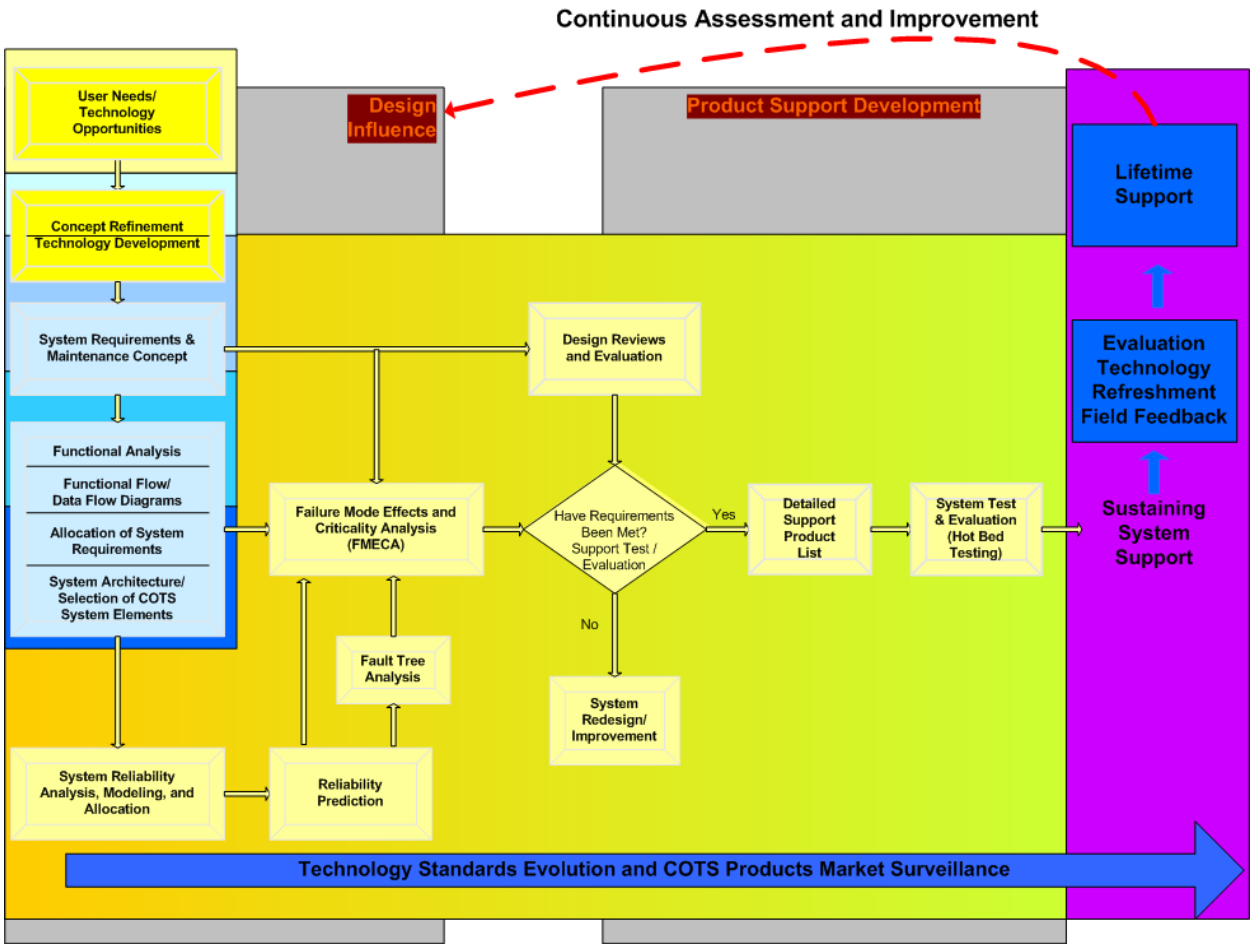


Figure 5 Sustainment Process

Sustainment, from the standpoint of IA, includes the ability to respond to threats that evolve, and vulnerabilities that might be discovered after the system has been fielded and that may impact the operation of the system and the information processed. IA reliability and probability of successful attack can be computed based on a number of approaches covered in the open literature. Fault tree analysis, from the IA perspective, is equivalent to developing attack trees. In turn, this can lead to Failure Mode, Effects, and Criticality Analysis (FMECA) conducted in the same manner as done for safety hazard analysis. Sustainment and post-deployment support are a recognized part of all SETR reviews from SRR onward.

5.2 Fleet Actions

Sustainment procedures for integrated combat support need to include IA operational and procedural guidelines to continually assure the protection of DON information systems and the information processed. These procedures should include regular threat briefing and vulnerability reports from US-CERT, GNOC, or equivalent bodies, to ensure the highest levels of training and awareness are attained.

Sustainment strategies should be refined throughout the life cycle, particularly during development of subsequent increments, modifications, upgrades, and re-procurement.

The PM and IAM are responsible for articulating outcome-based performance measures in the form of measures of effectiveness. Information assurance metrics should be used during development, as well as post-implementation and sustainment.

Fleet and field activity representatives should be involved in appropriate PIT development and sustainment IPTs and should be represented at SETR reviews for the PIT system.

The PM and IAM are responsible for planning the Post-Implementation Review (PIR). Working with Fleet and Field Activity IAMs, PMs and IAMs gather and analyze required IA data and assess the results. The primary recipient of the PIR report should be the Resource Sponsor who articulated the original objectives and outcome-based performance measures on which the PIT system development and/or deployment was based. For more information on the PIR, refer to section 5.3.4.

5.3 Program Management Office Actions

5.3.1 Supporting Fleet/Field Operations and Maintenance

The Program Manager's logistics team works with the users and the system engineering community to document support requirements into several integrated logistics support (ILS) documents. The most critical of ILS documents is the program's Maintenance Plan. The program's Maintenance Plan is the fundamental document used by logistics planners to determine supply support requirements, support equipment requirements, test equipment requirements, operator and maintainer manning and skill requirements, trainer and training support requirements, technical manual requirements, computer resource support requirements, facilities requirements, and design interface requirements. The program's Maintenance Plan begins concurrent with preparation for the program's SRR, and is continuously revised and updated through the program life cycle. See Appendix F for additional ILS considerations.

5.3.1.1 Information Assurance Vulnerability Management

Information Assurance Vulnerability Alerts (IAVA) and Information Assurance Vulnerability Bulletins (IAVB) will be made available to all organizations supporting the PIT system post-implementation. The Fleet and Field Activity IAM and the system program manager will collaborate on analyzing potential IAVA/IAVB impacts to the PIT system. See section 5.4 for how IAVA/IAVB fits into the PIT post-deployment process.

5.3.2 Engineering Change Support

5.3.2.1 System Modification and Modernization

All system modifications (ORDALTs, FCs, ECPs, etc.), whether installed to correct a deficiency, improve system performance, or to add new capability, should be analyzed for their impacts on information assurance and sustainment. This analysis needs to include whether the change to the system impacts the ability to quickly respond to newly discovered threats and vulnerabilities. IA and sustainment stakeholders should be permanent members of all change control boards associated with the given PIT system.

5.3.3 Demilitarization and Disposal

At the end of its useful life, a PIT system should be demilitarized and disposed in accordance with all legal and regulatory requirements and policy, to include all those related to IA. Program Managers will estimate and plan for the PIT system's demilitarization and safe disposal including, but not limited to, the destruction of hard drives and the wiping of all system memory following DoD and DON procedures.

5.3.4 Post Implementation Review (PIR)

The PIR provides an assessment of risk, readiness, technical status, and trends in measurable form. These assessments substantiate in-service support budget priorities. The PM and IAM should ensure that in-service IA design features meet the specified measures of effectiveness and suitability. IA issues are grouped by priority to form an integrated picture of in-service IA readiness, IA risk, and future in-service IA support requirements. With respect to IA, the PIR should provide:

- An overall system IA risk assessment
- An operational readiness assessment of the IA Defense-in-Depth architecture system IA issues
- Status of current system IA problem/discrepancy report inflow, resolution rate, trends, and updated metrics

Based on the PIR findings, a report should be prepared and recommendations provided to the PM. This report should highlight any IA deficiencies and/or recommendations for improvement. Typical success outcomes include:

- IA issues problems have been categorized to support the requirements generation process;
- IA issues have been integrated into and prioritized against other issues in program budgets
- Current and future levels of operational IA risk and system readiness have been quantified to support program budgets.

5.3.5 Guidelines for Reassessing Platform IT Designation Decisions

It may be appropriate to reconsider a system's designation as Platform IT if either of the following occur:

- There are changes to any responses in the system's PIT determination checklist
- There are changes to the PIT designation boundary to include, but not be limited to, the addition or withdrawal of an external interface

5.3.6 Budget Considerations

The PIT system's budget should include sufficient funds to support sustainment throughout the lifecycle of the system. As a minimum, budget allocations should consider support of the following IA activities:

- IAM and associated IA professionals
- Modernization of the IA Defense-in-Depth architecture and associated solutions

- IA regression testing
- IAVA/IAVB Management
- Training
- Sustainment

Regarding Sustainment, a program's Maintenance Plan is one of the key documents used by the Navy & Marine Corps readiness account managers (e.g.,. OPNAV(N4), HQMC(AS), HQMC(LS)) when setting sustainment account funding. The program's Maintenance Plan is also key to helping the PM determine those elements of the program which should be individually resourced and funded by the program's budget lines.

5.4 PIT Post-Implementation IA Assessment Process

A system begins the Post-Implementation IA Assessment Process when a system modification is required and it is determined that the modification will impact the IA posture of the system, sub-network, and/or the platform network.

The Post-Implementation IA Assessment Process depicted in Figure 6 combines with the sustainment process in Figure 5 at the point where continuous assessment and improvement feeds from lifetime support back to design influence.

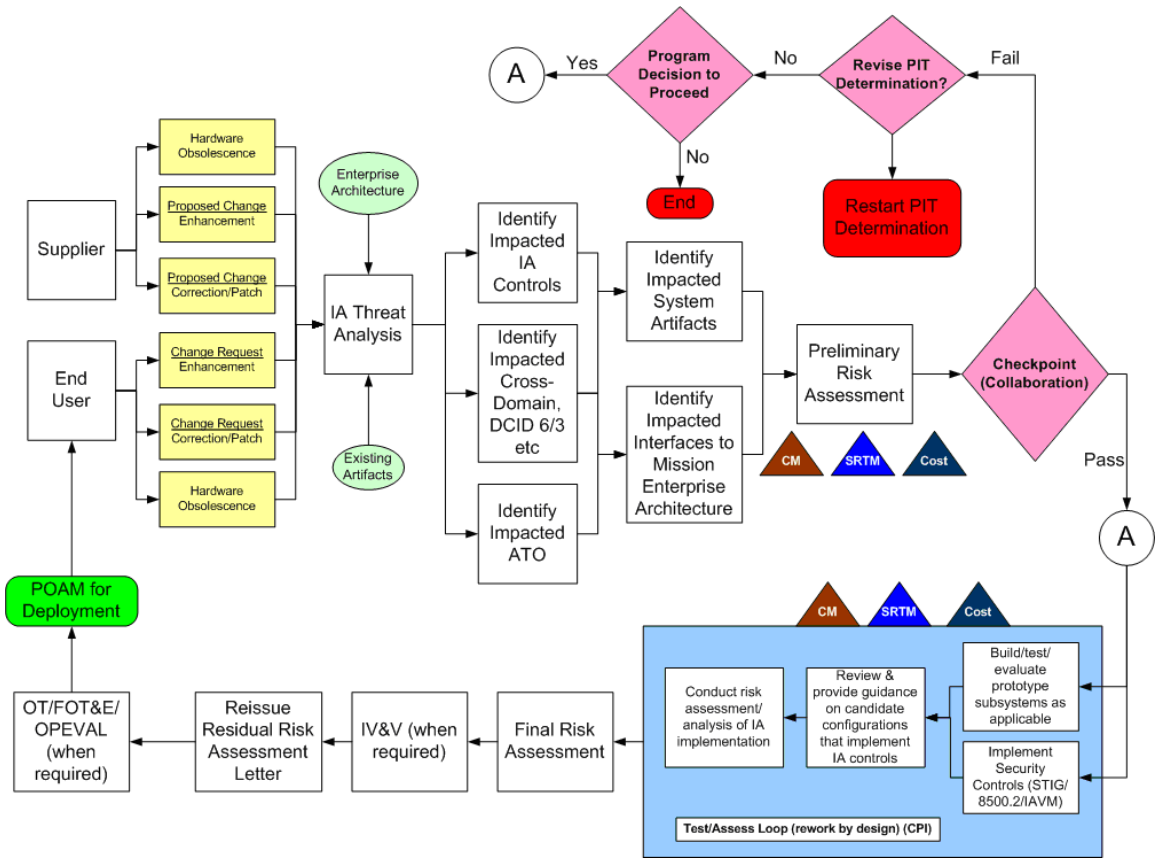


Figure 6 Post-Implementation IA Assessment Process

5.4.1 Process Description

When a system modification is proposed and sufficient design information is available, an IA threat analysis is conducted using the existing PIT system artifacts and the relevant system, sub-network, and platform network architecture diagrams. The results of the threat analysis are used to assess the risk to the IA Defense-in-Depth posture of the platform network. The risk assessment is then used to specify needed changes to IA posture of platform network, sub-system, and/or system. After the preliminary risk assessment is completed, a checkpoint meeting should be held to review the preliminary risk assessment, the updated IA sub-set of the RTM, and the supporting analyses to review and validate the proposed changes to the IA posture.

Once the system modifications are complete, IA regression testing will be conducted in conjunction with normal system regression testing of the modification, to ensure the integrity of the IA posture has been maintained. The PIT system documentation will be updated as needed to ensure configuration control of the changes proposed. Once the cognizant DAA is satisfied that the risk to the system has been reduced to an acceptable level, an updated ATO can be issued.

5.4.2 Key IA Considerations During System Modification

Strict configuration control of both the installed PIT system, proposed design changes and all documentation is mandatory to avoid introducing additional risk from poor CM.

The checkpoint meeting is the main opportunity for all affected stakeholders to learn of proposed IA enhancements, patches, or new threats and their associated workarounds. Sufficient time should be allotted for comprehensive feedback.

In the rare case where the PIT system might have to be re-classified as a non-PIT system, or the PIT system accreditation boundary has to be redrawn, the end users should be given sufficient advanced notice to allow appropriate workarounds to be implemented.

Appendix A
How To Complete the Platform IT Determination Checklist

Download or obtain a current copy of the PIT Determination Checklist from the DON CIO website:

http://www.doncio.navy.mil/

Enable Macros: The PIT Determination Checklist now uses macros to streamline this process. To obtain full functionality, macros must be enabled at Medium or Lower security. To check macro options, go to Tools>Macro>Security. Use of macros is not mandatory.

Note: Use of this form is for pre-evaluation only. The IT system or component is not designated PIT until an authorized DAA officially designates it.

Instructions using Macros:

PIT Question A: Determine if the system or component is subject to implementation..

PIT Question B: Determine whether the system or component may be a PIT candidate.

These questions will be filled automatically as you fill out the rest of the PIT Determination Checklist.

Question 1: Candidate System Information:

In the space provided, enter the date of drafting this document, system name and its acronym.

Question 2: IA Characteristics:

With respect to DoD and DON information determine what the candidate system does (IE Receive, Transmit, Process, Store, Display). Check all that apply.

Question 3: Platform IT Characteristics:

Of the three options provided, determine what statements describe the system. Check all that apply.

Question 4: General Services Characteristics:

Determine whether the candidate system performs any general services (IE email or networking) for one or more non-platform IT systems or business functions?

Note: Exclusively Tactical email and chat may be used by platform IT systems. Click “yes” or “no” accordingly.

Question 5: Special Purpose Mission or Function:

Determine and check all the special purpose missions/functions that apply to the candidate IT system or component?

Instructions without Macros:

PIT Question A: When asked whether the statement, “This IT system or component is subject to IA Implementation”, is true or false, enter “yes” for true and “no for false.

PIT Question B: When asked whether the statement, “This IT system or component may be a Platform IT candidate”, is true or false:

To enter “yes”:

Question 2 must have one or more of the responses checked.

Question 3 must have one or more of the responses checked.

Question 4 must have “No” checked.

Question 5 must have on or more of the major section boxes checked.

All of these criteria must be satisfied to enter yes. If a candidate system does not, then the answer is no.

Appendix B

Additional Information Assurance Principles

1. Objective Defense-in-Depth Architecture

Each domain (air, surface, subsurface, C4I, ground, facilities, supply, R&D, etc.) will be responsible for establishing an objective Defense-in-Depth architecture for the end-to-end information system, or "platform network", installed in each platform type (ship, aircraft, submarine, humvee, shore facility, etc.) The objective Defense-in-Depth architecture needs to provide protection against both external and internal malicious attacks, inadvertent operator error, and major calamity, whether natural or man-made.

The platform network generally consists of multiple segments, or "sub-networks". Sub-networks will be based on an aggregation of systems with similar functionality, mission, and/or the same level of security classification and with a need to exchange information. A sub-network will generally have its own communications capability (router, switch, network interface card, etc.) that permits communications with other sub-networks within the platform network or to other platforms outside the boundary of the platform network. Some examples of sub-networks based on like-functionality include C4I sub-networks, the Aviation sub-networks, the Hull, Mechanical, and Electrical (HM&E) sub-networks, and Utility Energy Management (UEM) sub-networks. These types of sub-networks will generally be organized and managed under a single PEO or SYSCOM lead. Examples of sub-networks based on the same level of security classification include Unclassified, Secret, and Top Secret sub-networks, which will usually be segregated using high assurance guards (HAG), Cross Domain Solutions, or high assurance internet protocol encryption (HAIPE) devices. These types of sub-networks will generally be organized and managed under a single PEO or SYSCOM lead for the specific platform.

The term "system" refers to a collection of information technology components (processors, displays, input/out consoles, software, etc.) organized to perform a specific mission. The term "application", refers to the software and/or firmware that implement the functions of a special purpose system in support of its mission. The term "processor" refers to the hardware on which the application executes. The term "processing environment" refers to the processor, operating system, and middleware configuration that supports the applications. A system, therefore, consists of applications and the processing environment.

As described above, the platform network consists of multiple sub-networks. Those sub-networks that provide access to networks outside of the platform boundary are at the first level in the platform network and will be referred to as a Level 1 sub-network or simply Level 1. (Note: Due to the unique nature of Tactical Data Links and Sensor and Weapons Networks, segregated tactical data networks are not considered platform boundary sub-networks.) The Level 1 sub-network serves as the first line of defense against external attacks; as such Level 1 sub-networks are in the position to provide the most robust defense against external attacks. There may be several Level 1 sub-networks existing at the platform boundary. Level 2 sub-networks connect to Level 1 sub-networks. The Level 1 sub-network serves as a buffer between the platform boundary and the Level 2 sub-network and the level 1 sub-network needs to provide a certain degree of protection to the level 2 sub-network. Level 3 sub-networks will connect to Level 2 networks; both the Level 1 and Level 2 sub-networks serve as a buffer between the platform

boundary and the Level 3 sub-network and both the Level 1 sub-network and the Level 2 sub-network provide a certain degree of protection to the Level 3 sub-network. Subsequent sub-network levels can be identified for each platform network. The System level, the Application level, and the Processor level, in that order, will serve as the last three levels in the Defense-in-Depth architecture for the platform network. See Figure B-1 for a graphic representation of Levels 1-3, System level, Application level, and Processor level.

To protect against internal threats, the protective measures implemented at the System level, Application level, and Processor level should be sufficiently robust to delay or deny access to the special purpose system and the information being processed, while still permitting data exchange and information flow. In order to understand what protective measures to implement at each of these levels, it will be necessary to carefully evaluate the various tools, techniques, and methodology that could be used to attack the system. Figures 2 and 3 depict surface ship examples of possible levels in a Defense-in-Depth architecture.

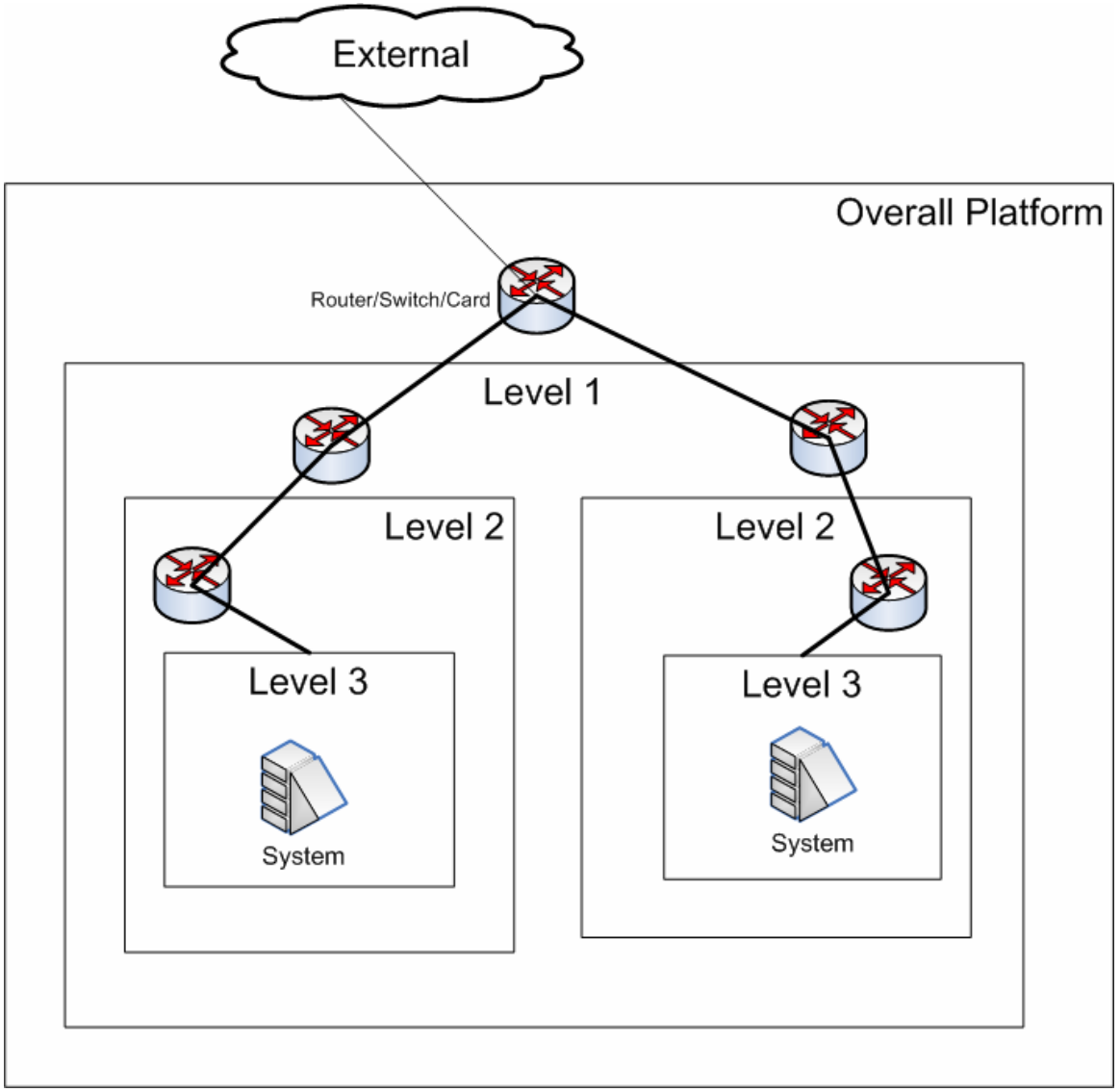


Figure B-1 Generic Defense-in Depth Architecture Example

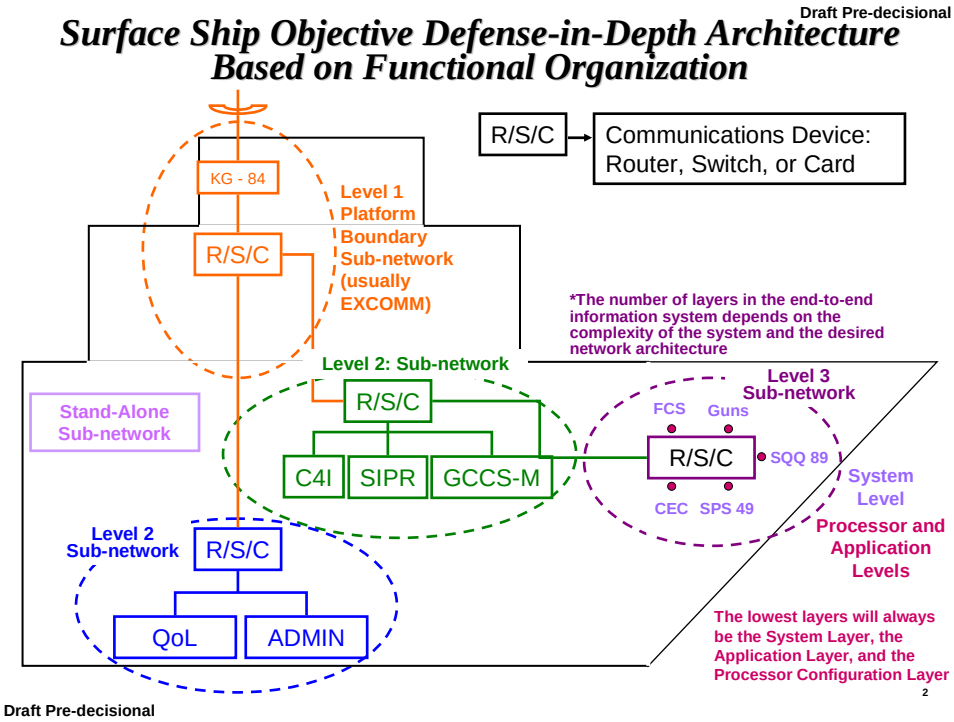


Figure B-2 – Shipboard Example #1

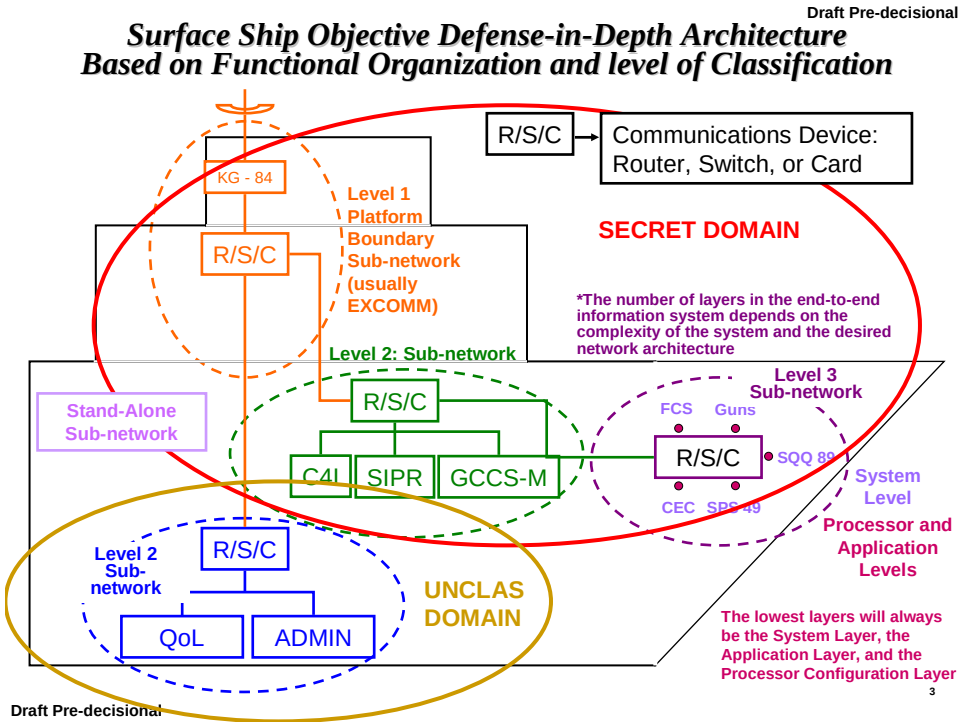


Figure B-3 – Shipboard Example #2

2. Selecting the Right IA Security Requirements

It is important to note that DoD guidance directs all systems to implement IA to enforce the protection of information to be processed by the system within their operational environment, regardless of whether the system is determined to be PIT or non-PIT.

The identification of the IA requirements starts with the list of approved IA controls found in DoDI 8500.2. There are three basic types of IA controls, discussed in more detail below.

- Administrative and Management Controls (AMC) – These controls are implemented by the Program Office and by the platform's personnel, under the cognizance of the IAM, to ensure an information assurance program is properly established, funded and managed.
- Technical Controls (TC) – These controls provide system requirements to ensure the functional design includes information assurance throughout the entire life-cycle, from early requirements definition, through design and development, and into life cycle support and decommissioning. TCs should be interpreted, functionally decomposed, and allocated to the functional design of the platform network, sub-networks and systems by the Program Office system engineering team.
- Operational and Procedural Controls (OPC) – These controls provide requirements that affect the operation of the system in the environment in which the system will be used, and take two basic forms: system set-up and configuration, and system operator interaction. OPCs include actions performed by the operators to manage the system and to respond to problems, to ensure the availability, integrity, and confidentiality of information processed by the platform network, sub-networks, and systems. While the OPCs largely depend on the system IA configuration of the platform network, there are a number of standing OPCs that should be folded into the platform network operations manual to ensure IA awareness and training are complete.

It is necessary to develop and maintain of a set of standing IA tools that establish the Defense-in-Depth architecture for each platform type. The IA tools can include, but not be limited to:

- Objective Information Assurance Requirements Traceability Matrix for the specific platform type
- Objective Platform Network Defense-in-Depth architecture diagram that identifies the location of the functionally decomposed controls within the platform network
- Objective Platform Network Defense-in-Depth architecture diagram that translates the TCs into generic materiel solutions (i.e., passwords, firewalls, access control lists (ACL), VPN tunnels, etc.) for each location at which a control is to be implemented

The IA controls from DoDI 8500.2, as well as other security requirements considered critical to achieving the Defense-in-Depth architecture, should be functionally decomposed and allocated to the IT components comprising the system, based on MAC and CL. This functional decomposition and allocation of requirements should be captured in the platform type RTM. Management of the platform type RTM may occur at the SYSCOM level.

3. Selecting the Right IA Design Features

Since the DoDI 8500.2 IA Controls do not necessarily provide comprehensive protection, the following design features and performance parameters should be considered since they significantly contribute to the stability and security of the platform network and are critical to attaining the IA objectives of availability and integrity:

1. Networking Capabilities
    a. Internal Platform Communications vs. External Platform Communications
    b. Communications Devices/Interfaces - Routers vs. switches vs. network interface cards vs. point-to-point connections
    c. Protocols and Messages - TCP/IP vs. TDP vs. specially designed protocols and messages (Link 11, Link 16, Data Distribution System (DDS), etc.)
    d. Communications Architectures – Time division, multiple access (TDMA) vs. commercial division, multiple access (CDMA) vs. time division, pair wise access (TDPA) vs. publish and subscribe vs. query and response
    e. Communications Path – terrestrial land line vs. mobile; radio communications; interface cards
    f. Encryption Requirements
    g. Cross-domain Information Exchange Requirements
    h. Anti-jam Features
    i. Anti-tamper Features
    j. Interoperability
    k. Latency
2. Hardware Reliability, Maintainability, and Availability (RM&A) Measures of Effectiveness
    a. Operational Availability (A_o)
    b. Mean Time Between Failure Hardware ($MBTF_{HW}$)
    c. Mean Time Between Operational Mission Failure Hardware ($MTBOMF_{HW}$)
    d. Mean Time to Repair (MTTR)
    e. Automated Network Configuration Set-up
    f. Automated Troubleshooting and Repair (e.g., built-in-tests)
    g. Fault Detection and Isolation
    h. False Alarm Rate
3. Software Reliability
    a. Software Endurance
    b. Software Fault Detection and Tolerance

c. Probability of Message Error

d. Propagation Loss

e. Data Integrity

f. Data Latency

g. Mean Time Between Operational Mission Failure Software ($MTBOMFs_W$)

h. Interoperability – Track File Consistency and other SIAP Metrics

The list of parameters provided above do not constitute a comprehensive list, but does provide a starting point for design engineers to begin evaluating measurable and testable parameters for the system under development.

Appendix C
Documentation

C.1 Requirements Generation Documentation

Requirements Generation Process

In accordance with reference (m), there are four key documents in the requirements generation process: ICD, CDD/CPD, ISP, and TEMP. The ICD provides a high-level overview of the capabilities required by the system under development. The capabilities identified in the ICD will then be translated into the Net-Ready KPP (NR-KPP), as well as into measures of effectiveness and suitability (operational performance requirements and key system attributes) for inclusion in the Capability Development Document (CDD) and the Capability Production Document (CPD) for the system being developed. The NR-KPP documents the IA requirements for the system. The ISP documents the IA architecture that supports the NR-KPP, and the TEMP focuses on the overall structure, major elements, and objectives of the Test and Evaluation (T&E) program. The system performance parameters and key system attributes are eventually decomposed functionally and allocated to the various elements and components and captured in the SDD and the lower level specifications.

Initial Capabilities Document (ICD)

Because the ICD is the first document in the requirements generation process, it is critical to ensure that IA capabilities are included. At a minimum, the following language is recommended for inclusion into the ICD:

(*System) requires the capability to effectively protect the information and information system from inadvertent operator error, internal and external malicious attack, and natural and man-made major calamities (hurricane, fire, flooding, etc.)*

(System) requires the capability actively respond to internal and external malicious attacks, as well as recover from system failures caused by inadvertent operator error, internal and external malicious attack, and natural or man-made major calamities

Capability Development Document (CDD)/Capability Production Document (CPD)

Most programs are required to provide a Net-Ready Key Performance Parameter (NR-KPP) in the CDD/CPD. One element of the NR-KPP is Information Assurance. In addition to the IA requirements that make up the NR-KPP, each program should include in the CDD/CPD those IA requirements, based on DoDI 8500.2, common criteria, and other IA requirements deemed appropriate, and in keeping with the objective Defense-in-Depth architecture for the platform network or sub-network into which the system will be integrated. In the event that a NR-KPP is not required, it is still necessary to provide the IA requirements in the CDD/CPD.

Section 3 of Appendix B provides the minimum list of design features/measures of effectiveness that support the IA objectives of availability and integrity, as well as the IA element of the NR-KPP, and should be considered for inclusion in the CDD/CPD.

The IA elements of the NR-KPP are progressively detailed at each step of the acquisition process, and are assessed as part of the certification of the CDD beginning with entry to Milestone A (if

the program is initiated at Milestone A) or Milestone B (if the program is initiated at Milestone B) and are most robust at the entry of Milestone C. Items 5.1 through 5.26 of the CJCSI-6212.01D Appendix C to Enclosure D, Interoperability and Supportability Assessor's Checklist constitute the factors used to evaluate the IA component of the NR-KPP. It should be noted that this assessment of the NR-KPP is broad in scope and encompasses both program management and engineering accomplishments, but is not technical. The NR-KPP is certified in the ISP where technical detail is decomposed and documented and typically is found in DoD Architectural Framework (DoDAF) artifacts such as OV-5 Operational Activity Model), SV-1 (Systems Interface description), SV-2 (Systems Communications Description), SV-4 (System Functionality Description), SV-5 (Operational Activity to Systems Function Tractability Matrix) and SV-6 (Systems Data Exchange Matrix).

Information Support Plan (ISP)

DoDI 4630.8 provides guidance for developing the ISP, while ASN RDA CHSENG has promulgated a template for submission of Navy ISPs. Section 2.12 is titled Information Assurance. All DON systems (ACAT, non-ACAT, and fielded systems) that are required to submit an ISP should provide the following additional information in section 2.12 of the ISP:

a) Provide an overview of the Defense-in-Depth strategy for the system, to include a discussion of the materiel solutions - protective measures and design solutions - to be implemented in the system under development, as well as those to be inherited from the end-to-end information system installed in the platform. Identify requirements for modeling, simulation and or special training systems required for development and/or support of the system.

b) Develop, as a minimum, two architecture diagrams to supplement the discussion in paragraph a) above: 1) the overall Defense-in-Depth diagram for the platform, which clearly demonstrates the individual system's connections to the end-to-end information system along with the inherited protective measures; 2) a system diagram that clearly demonstrates the protective measure and inherent design features that protect the system from both internal and external threats.

Note: There is currently no DoDAF guidance for development of operational or system views to depict the IA architecture for a system, sub-network or platform network; however, a program may adapt DoDAF architecture products, as necessary, to depict the IA Defense-in-Depth architecture.

c) Provide an overview of the security training required of maintenance technicians and platform's personnel in accordance with reference (h).

d) Provide a list of the materiel solutions, whether protective measures (e.g., FW, IDS/IPS, passwords, etc.) or design features (e.g., common criteria, segregated networking, firmware solutions, etc.), where in the system the solution has been implemented (e.g., platform boundary, internal networking boundary, system level, application level, etc.), whether the materiel solution has been approved for use and by which agency (i.e., NIST or FIPS processes); if the materiel solution is not yet approved for use, when will it be brought through the approval process; if not, why not.

e) Provide an overview of the test strategy and key test events during which security objectives will be tested; test strategy should include the incremental testing approach and aggregation of results and how it will support platform certification.

f) Provide an overview of the sustainment of the security posture of the system, to include CM of the security architecture.

g) Provide a more detailed discussion of the NR-KPP (if applicable) documented in the CDD/CPD.

Test and Evaluation Master Plan (TEMP)

The TEMP focuses on the overall structure, major elements, and objectives of the T&E program and it should be consistent with the acquisition strategy, approved CDD or CPD, System Threat Assessment, and the ISP. The TEMP should also be consistent with and complementary to the Systems Engineering Plan. Section 9.10 of the Defense Acquisition Guidebook provides a recommended TEMP format. The IAM is encouraged to participate in the development of the TEMP. Section 3 of Appendix B provides a list of design features/measures of effectiveness that support the IA objectives of availability and integrity, as well as the IA element of the NR-KPP, and should be considered for inclusion in the TEMP.

In accordance with the Commander Operational Test and Evaluation (OT&E) Force Operational Test Director's Manual (COMOPTEVFORINST 3980.1), Section IV of the TEMP must include the IA Critical Operational Issue (IA COI) and the IA Measure(s) of Effectiveness. The IA COI will be validated using IA Effectiveness Test, as further defined by the DOT&E memorandum, Policy for Operational Test and Evaluation of Information Assurance in Acquisition Programs. The TEMP must also provide an OT&E strategy for IA assessment addressing the test process, identification of required IA test resources and funding, and a reference to appropriate threat documentation.

C.2 Acquisition Documentation

Contract Language

All programs should ensure contract language clearly articulates IA requirements throughout the life cycle of the program, to include, but not limited to: Contract Deliverable Requirement List (CDRL); inclusion of IA performance parameters and key system attributes in system design documents and architecture products, Requests for Proposal (RFP) and Statements of Work (SOW) for both manufacturer and program office support contracts.

The solicitation may require the offeror propose an acceptable approach to selecting IA controls starting from the baseline set of DoDI 8500.2 b commensurate with the system's MAC and Confidentiality Level or may identify these IA controls as part of the solicitation. Also, the task of proposing the MAC and confidentiality level may be part of the offeror's proposal.

Acquisition Strategy

Defense Acquisition Guidebook (DAG) paragraph 7.5.9.5 provides a recommended format for integrating IA into the Acquisition Strategy and highlighting any IA considerations that may impact the acquisition of the program under development. All programs should follow this format, as a minimum, but may provide additional information to highlight any impacts not specifically covered by DAG paragraph 7.5.9.5.

Acquisition Program Baseline

The program manager derives the Acquisition Program Baseline (APB) from performance, schedule and cost goals consistent with program resources. Capabilities documents (CDD and CPD) are used to derive performance goals and these goals are documented as Key Performance Parameters (KPPs). In the APB, program goals are translated and documented as the KPPs for the system under development. Typically, KPPs are few in number and are focused on issues that are so important that the continuance of the program may be questioned if they are not achieved. Once approved, the APB becomes the criteria against which the milestone decision authority measures program success. KPPs are developed in accordance with reference (m).

Information Assurance Strategy

Acquisition programs for IT systems designated as having an acquisition priority of Mission Critical and Mission Essential are required by reference (b) to:

- Develop a formal IA Strategy using the DON Chief Information Officer (CIO) IA Strategy template.
- The IAS or update to the IAS is required to be approved prior to entering the next Milestone review.
- The IAS is submitted as an element of the CCA Compliance package. The IAS is required to be signed by the PM and the EII/MSC DAA.
- The final IA Strategy is required to be submitted to the DON CIO 90 days prior to the milestone. Acquisition programs for IT systems that are MC/ME and ACAT III or lower (including AAPs) are required to submit IASs to the Command IOs. Command IOs require 30 days (prior to submission to DON CIO) before approving and forwarding higher level IASs to DON CIO and 30 days for approval of IASs under their cognizance.

Acquisition programs for IT systems that have an acquisition priority of Mission Support, as defined in reference (j), may not be required to develop an IA Strategy; however, higher authority may determine that an IA Strategy is required for ACAT I and II IT Mission Support programs or programs designated as "special interest".

DON CIO has published a template at http://www.doncio.navy.mil/, (Click "Browse Topic Areas"; click "Clinger Cohen Act Compliance", cursor down to "Information Assurance Strategy Guidance Template".) and its use is mandatory for all Mission Critical and Mission Essential information systems.

The IAS is an executive level document and should provide salient information of a strategic nature, at a high level. Each subject required by the template must be sufficiently addressed for executive decision and may be supplemented by referral to other sources or program documents. Each subject represented by a header (or issue) in the template requires an explicit answer or an explanation as to why it does not apply. When the program has not matured sufficiently to answer, an explanation is required including a statement as to when the answer will be provided. The strategy outlined in the IAS is used to frame the planning that will define the program. Based on the nature of each program, in addition to the required information in the template, some topics should be amplified and other topics that are strategic in nature should be considered for inclusion in the IAS. Some examples are:

- How security system engineering is integrated into the program's systems engineering approach and how IA related updates to Systems Engineering Technical Review (SETR) entry and exit requirements to incorporate appropriate Information Assurance risk assessments and controls are used. Describe how the IAM is expected to determine the entry and exit criteria for SETR events, the role of the IAM in providing detailed IA requirements to be addressed at each review.
- How updates to technical interface documents, technical publications, training, etc. will be managed to incorporate appropriate Information Assurance controls.
- How updates to logistics or program planning documents will be managed to incorporate appropriate Information Assurance controls selected from reference (f).
- How the program identifies and manages budget resources for IA is required by the template, but is often not easily identified in financial data. This section should be done carefully so that there is an approved strategic purpose that forms a foundation for plans and to identify appropriate funding levels for the IA portion of the program. Updates to budget planning documents to ensure appropriate funding of Information Assurance requirements should also be described.

Cost Analysis Requirements Description (CARD)

ACAT 1 and ACAT 1A acquisition programs are required to define program and system parameters in accordance with the Cost Analysis Requirements Description (CARD) as described in DoD 5000.4M. The basic CARD technical and programmatic guidance, tailored to suit the scope and complexity of the program, should be followed to ensure that all pertinent technical cost drivers are addressed which should include cost drivers for Information Assurance such as security design features, and IA supportability and maintenance cost drivers. The term CARD-like document is used in the System Engineering Technical Review (SETR) Handbook to

describe the minimum technical description required to achieve the objectives of the SETR Initial Technical Review (ITR).

The success of the ITR also depends on independent subject matter expert review of each of the identified cost drivers. Therefore it is critical that an IA subject matter expert review the CARD-like document to assess the completeness and accuracy from an IA perspective.

Systems Engineering Plan (SEP)

DAG paragraph 2.3.7 states the purpose of the SEP is to document the program's System Engineering Strategy to include the overall technical approach, including processes, resources, and metrics, and applicable performance incentives. The SEP Preparation Guide, Version 2.01 provides specific guidance for completion of the SEP; however, it does not specifically call out Information Assurance, but instead refers to security. Therefore, it is essential to the functional design of the system to highlight how the program will integrate IA into the normal system design and test regimen, to include system engineering processes, the system engineering technical review process, entrance and exit criteria for each technical review, validation and test, as well as how these processes feed key acquisition documents.

The IAM by participation in the development of the SEP, ensures that system engineering processes adequately document required IA requirements and considerations.

Configuration Management Plan

Configuration management is critical to program success. The program's CM plan should include procedures and tools for verifying and validating the configuration of the IA Defense-in-Depth architecture of the platform network; the specific IA materiel solutions that have been implemented in the platform network, the sub-networks, and the systems; the configuration of software at the system, application, and processor configuration. It is of equal importance to ensure CM of program and system IA documentation. The program's CM plan should also require assessment of the impact of all system modifications (Ordnance Alterations (ORDALTs) Field Changes (FC), Engineering Change Proposals (ECP), etc.) on IA as a factor for approval of installation of the modification.

C.3 Design Documentation

Requirements Database

Each program will capture operational and technical requirements in a requirements database, such as DOORS, which will be used to support documentation of requirements flow down. The database should capture all requirements levied on the system. One sub-set of this database will be the Information Assurance requirements for the system.

Requirements Traceability Matrix (RTM)

The IA requirements should not be captured in a separate RTM. Instead, they should be included as a subset of the program's overall RTM. The RTM should include all high-level IA requirements identified in the CDD as those requirements are decomposed and allocated to the various system elements and technical documents.

System Design Document (SDD) and Lower-level Specifications

The SDD may have numerous sub-specifications and different titles, but in effect captures the technical specifications to which a system will be designed. The IA technical requirements from the progam’s RTM and if applicable from the objective Defense-in-Depth architecture for the given platform, should be included as detailed design criteria and performance parameters in the SDD and other lower level specifications. Though captured in the RTM, the list of IA requirements captured in the SDD and lower level specifications should be limited to only those that apply to the system under development. Inherited controls should not be included in the SRD and lower level specifications, as these documents are intended to be used by the engineers to design the system.

Appendix D

Risk Management

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The objective of performing risk management is to enable the system to accomplish its mission(s):

1. by better securing the system components that store, process, or transmit information;
2. by enabling program management to make well-informed risk management decisions to justify expenditures on IA;
3. by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Risk assessment is the process which includes identification and evaluation of risks and risk impacts, and concludes with recommended risk-reducing measures. It is used to determine the extent of the potential threat and the risk associated with a system throughout its development. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the mission of the system.

Risk mitigation is the process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the output of the risk assessment process.

The evaluation and assessment process is used to determine whether the remaining residual risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the system for operation.

During the Design and Development Phase of the Acquisition Process, the Security Engineer should assess the IA risk to a system, sub-network, and platform network before, during, and after IA design work occurs. When assessing risk to the platform network, sub-networks, or systems, the security engineer should first answer a simple question: "What is the risk to the system under development from an internal or external malicious attack, inadvertent operator error, or major calamity?" In order to determine a common methodology for assessing risk across disparate systems installed onboard a platform, the Security Engineer should start with the tools, techniques, and methodology that can be used to attack the platform network from an internal workstation or a remote, external site.

The next step is to design the system to meet the IA requirements identified in the Defense-in-Depth architecture for the specific platform network, as well as for the those sound system engineering design features that ensure the system works as designed in a benign environment. Once the specific IA configuration (i.e., the system design) is complete and it incorporates both security solutions and design features that promote security (including availability, integrity, and confidentiality), the Security Engineer should evaluate the residual risk.

Risk assessment should occur at each individual level in the Defense-in-Depth architecture, but it is possible to conduct the risk assessment at the sub-network level and at the platform network level, if the engineering of each system in the sub-network have closely coordinated with the other systems in the sub-network.

For more detailed guidance on how to perform risk management and risk assessments, refer to NIST Special Publication 800-30 “Risk Management Guide for Information Technology Systems”.

Appendix E

System Engineering Technical Review (SETR) Process

1. Introduction

There are a myriad of factors that impact the SETR process, chief among these is the maturity of the technical designs and associated documentation. As such, the SETR process should be tailored for each program. The lead Systems Engineer advises the Program Manager regarding the technical reviews that should be accomplished and what documentation should be reviewed at each technical review. The technical reviews are documented in the program's Systems Engineering Plan (SEP), approved by the program's Milestone Decision Authority.

OSD(AT&L) maintains Technical Review Checklists online at https://acc.dau.mil/ (ACC Practice Center > Systems Engineering.> Policy & Guidance > OSD SE Guidance > Technical Review) These checklists present a series of generic questions that provide the IAM a solid starting point from which to understand the key issues to be discussed in the technical review and how they relate to IA. Additionally, the Naval Systems Engineering Guide, published by NAVAIR, and the Technical Review Manual, published by PEO IWS are two sources of detailed guidance on the preparation and conduct of Technical Reviews, the information and documentation that should be reviewed, entrance and exit criteria for each specific review, and systems engineering processes used in support of the acquisition of systems. These documents have been recommended as the starting point for the ASN RDA CHSENG initiative to establish a single authoritative document on the SETR process.

2. IA Roles and Responsibilities in the SETR Process

2.1 SETR Panel Composition

In addition to the normal composition of the SETR Panel, the PIT DAA should serve on the SETR Panel as the competent IA authority. The PIT DAA may delegate this responsibility to a command IAM or an IA Technical Warrant Holder, or other authoritative IA professional that is independent of the program under review.

2.2 SETR Chairperson

In addition to the normal duties and responsibilities for executing a technical review, the SETR Chair person will ensure that IA entrance and exit criteria are included in the technical review entrance and exit criteria and that a competent IA authority, independent of the program under review, is assigned.

2.3 PIT DAA

The PIT DAA, as a member of the SETR Panel, is responsible for:

- Validating the IA technical review
- Validating that entrance and exit criteria have been satisfied
- Identifying any IA technical issues

- Validating IA issue mitigation is ongoing
- Recommending whether a program should proceed or delay, based on the findings of the IA technical review
- Assigning a lead IA Review Team Member

The PIT DAA has a critical role throughout SETR events to ensure that the system will be able to function in the operational environment with an acceptable level of risk.

2.4 IA Manager

The IAM, as the program's IA subject matter expert, is responsible for:

- Coordinating technical review of IA design considerations by requesting support of either the IA Technical Warrant Holder or the SYSCOM IA Competency, whichever is applicable.
- Ensuring that all information assurance requirements are appropriately captured, documented, and assessed in the Program's system requirements traceability matrix
- Ensuring critical IA technical information and risks are provided to the review team to support the technical review timeline (identified risks should include: the probability of occurrence, the severity of impact if it occurs, and a plan for mitigation or resolution)
- Ensuring that the appropriate SETR checklist has been reviewed for Information Assurance considerations
- Ensuring that technical review's entry criteria have been met
- Ensuring risks are conveyed in a clear and concise manner to the Program's Lead Systems Engineer, the Program Manager, PIT DAA, and to the Technical Review Team
- Ensuring concerns from information assurance stakeholders, and in particular, from the intended Fleet user/maintainer/operator community, have been captured, identified, mitigated or elevated during the review.
- Ensuring that technical issues related to IA are resolved

The IAM should avoid identifying new issues solely to support a SETR event. As soon as sufficient data indicates an IA technical issue exists, the issue should be brought to the attention of the program leadership team.

2.5 IA Technical Expertise

In order to support the guidelines and processes for IA implementation, EII/MSC leadership may establish an IA competency organization and empower the PIT DAA and/or IA Technical Warrant Holder to coordinate IA resources across programs to ensure standardization of IA implementation and consistency within platforms.

The PIT DAA should assign the requisite IA expertise to conduct the technical review. As such the IA technical expertise is responsible for

- Ensuring that IA technical assessment has been completed to meet the timeline for technical review

- Ensuring critical technical information and risks are conveyed to the program's IAM, PM and PIT DAA

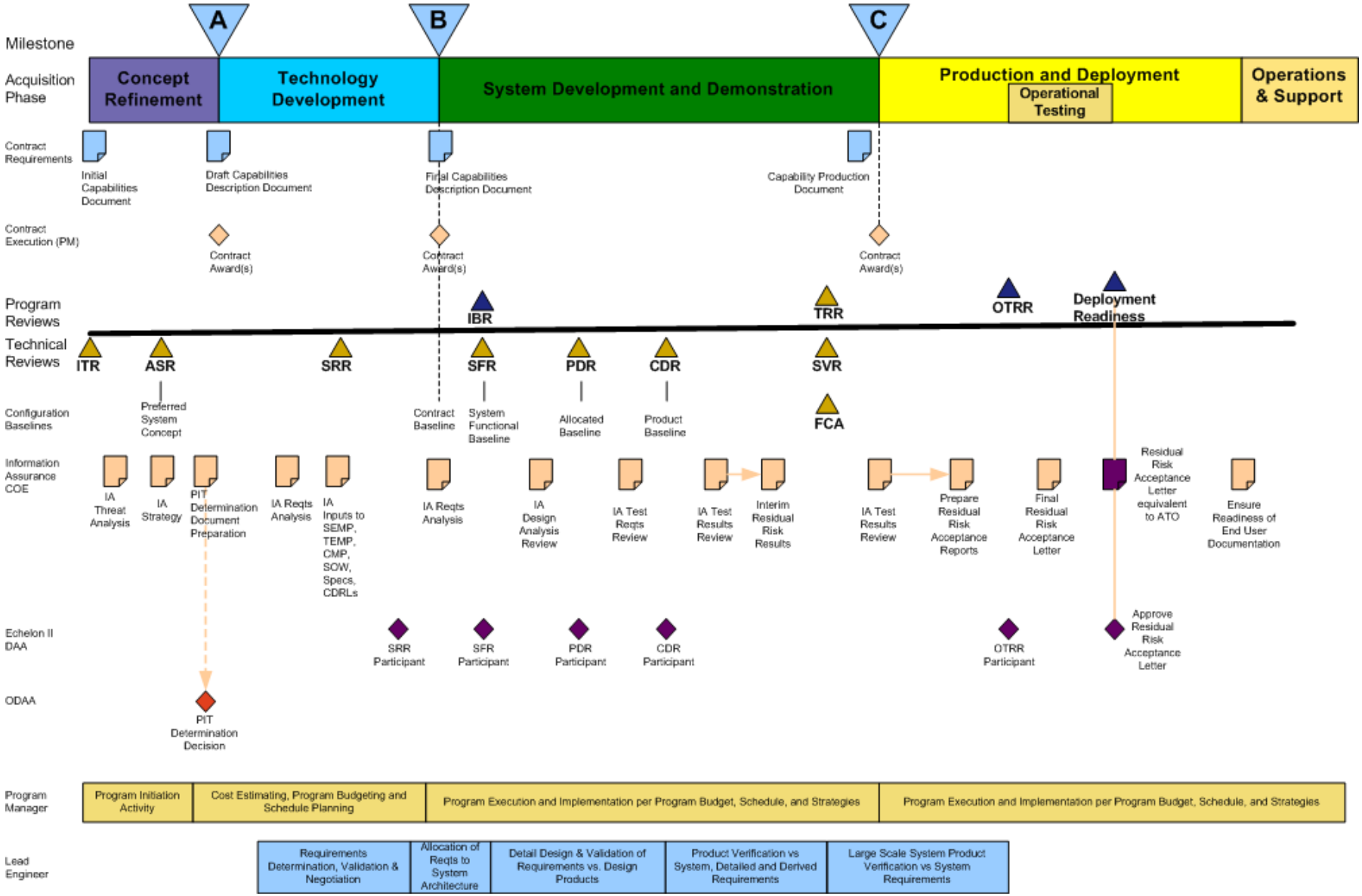


Figure E-1 Information Assurance PIT Process Aligned with SETR Process

3. SETR Events, Entrance and Exit Criteria

As shown in Figure E-1, the Systems Engineering Technical Reviews typically included on a program schedule are:

- Initial Technical Review (ITR)
- Alternate System Review (ASR)
- Technology Readiness Assessment (TRA)
- Systems Requirements Review (SRR)
- Integrated Baseline Review (IBR)
- System Functional Review (SFR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- System Verification Review (SVR)
- Physical Configuration Audit (PCA)
- In-Service Review (ISR)
- Post-Implementation Review (PIR)

Other technical reviews that may also be required (depending on where the program originates) is the Production Readiness Review (PRR) and the Operational Test Readiness Review (OTRR). In addition, Naval Air Systems Command will conduct a Flight Readiness Review (FRR), if applicable to the program. Individual SYSCOMs may have specific guidance covering any additional technical reviews.

With the concurrence of the program's MDA, SETRs may be tailored to suit individual program scope and complexity. Tailoring of reviews is usually documented in the Program's acquisition schedule and in the program's SEP. However, SRRs, PDRs, CDRs and SVRs are normally conducted on all non-ACAT acquisition programs.

For more information on Systems Engineering Technical Reviews, a high level summary of SETR can be found in Chapter 4.5.8, of reference (c).

ITR – Initial Technical Review

The ITR is a multi-disciplined technical review to support a program's initial Program Objective Memorandum (POM) submission. This review is intended to ensure that a program's technical baseline is of sufficient rigor to support a valid (acceptable cost risk) cost estimate and enable an independent assessment of that estimate by cost, technical and program management subject matter experts. The ITR assesses the envisioned requirements and conceptual approach of a proposed Program and verifies that the requisite research, development, test, engineering, logistic, and programmatic bases for the program reflect the complete spectrum of technical challenges and risks.

IA Entry Criteria

- Determine if an acquisition IA strategy is required
- A properly certified program IAM has been identified.
- High level system IA requirements are understood and documented.
- IA system capability specific requirements have been identified and documented in the appropriate acquisition documents.
- A determination on whether the Net-Ready KPPs are required. If required, the derived IA requirements from the Net-Ready KPPs have been identified and documented appropriately.
- The MAC and Confidentiality Level of the system concepts are understood and documented.

IA Completion/Exit Criteria

- All entrance criteria have been met and documented in the appropriate program acquisition documents.

ASR – Alternative Systems Review

The ASR is a multi-disciplined product and process assessment to ensure that the resulting set of requirements agrees with the customers needs and expectations, to ensure that the system concepts align with the external environment (systems, information networks, and infrastructure), and to ensure the system under review can proceed into the Technology Development phase. ASRs are typically completed prior to Milestone A.

IA Entry Criteria

- See criteria for the ITR.
- Acquisition IA strategy is in draft development (if required).
- External IA environmental factors and threats for the preferred system concepts have been identified and documented.
- All relevant IA stakeholders for the preferred systems concepts have been identified and all of their requirements have been documented in the appropriate acquisition documents.

IA Completion/Exit Criteria

- IA capabilities of the preferred system concepts have been specified and documented in the appropriate acquisition documents.
- The recommended set of DoDI 8500.2 IA controls for the preferred systems concepts have been identified and requirements statements have been derived and documented in the appropriate acquisition documents.
- The preferred system concepts, as disclosed, can satisfy any IA CDD or ICD specific requirements.
- All IA derived requirements for the preferred concepts have been identified and documented in the appropriate acquisition documents.
- All IA requirements can be met or satisfied by the preferred system concepts.
- The IA events in the program schedule are executable from the standpoint of technical and cost risk within acceptable margin and probability of estimate
- The program is properly staffed appropriately with trained and certified IA personnel.

SRR – System Requirements Review

The SRR is a multi-disciplined product and process assessment to ensure that the system under review can proceed into the System Development and Demonstration (SDD) phase, and that all system and performance requirements derived from the CDD are defined, aligned with the external environment (systems and infrastructure), and consistent with cost (program budget), schedule (program schedule), risk, and other system constraints.

IA Entry Criteria

- Appropriate IA elements are included in the following technical products:
  1. System specification, to include a description of interoperability and/or distributed services requirements,
  2. System architecture (hardware, software, IA, human, material as necessary) complete with details regarding partitioning rationale and approach to architecture development,
  3. System software functionality description,
  4. System/Subsystem Design Specification,
  5. CARD (i.e., IA cost elements are appropriately captured),
  6. The preferred system solution definition addresses which controls will be met technically, operationally, or administratively.
  7. The IA technical risk assessment is complete and mitigation plans are appropriately identified and resourced.
  8. SEP includes appropriate IA control elements.
  9. The Software Development Plan (SDP), when available, addresses the appropriate IA controls.
  10. Integrated system architecture and supporting views.
- IA is appropriately resourced by the program budget to cover the cost of developing, procuring, testing, certifying and accrediting, and maintaining the posture of system IA solutions. Appropriate types of funds are allocated (e.g. Operations & Maintenance for maintaining IA posture in out years.
- IA controls have been properly addressed by specific Contract language (Specifications, CDRLS, SOW, etc.)
- IA controls have been properly identified and documented by requirements statements that are managed and tracked in the program's system requirements management system. At a minimum, the DoDI 8500.2 controls have been addressed.
- If system(s) have been determined as Platform IT candidates, then Platform IT designation is to be acquired from the ODAA/MCEN DAA.
- The Draft ISP has been reviewed and appropriate IA controls have been identified and documented by requirements statements in the program's system requirements management system.

- The Draft NR-KPP has been reviewed and appropriate IA controls have been identified and documented by requirements statements in the program's system requirements management system.

IA Completion/Exit Criteria

1. System requirements are sufficiently detailed and understood to enable system functional definition and functional decomposition
2. There is an approved system specification that addresses the appropriate IA controls.
3. The derived information assurance requirements from the Family of Systems (FoS) or System of Systems (SoS) are properly allocated and approved.
4. Adequate IA processes and metrics are in place for the program to succeed
5. The IA risks are known and manageable for design and development
6. The IA elements of the program schedule are executable (technical/cost risks)
7. The program is properly staffed or supported with IA personnel.
8. The IA elements of the program are executable within allocated budget
9. The IA elements in the preliminary CARD are consistent with the approved system specification
10. The required IA software functionality in the system specification is consistent with the software sizing estimates and the resource-loaded schedule.

TRA – Technology Readiness Assessment

The TRA is a regulatory information requirement per DoD Instruction 5000.2. The TRA is a systematic metrics-based process that assesses the maturity of Critical Technology Elements (CTEs) and is a requirement for all acquisition programs. The TRA may be conducted concurrent with other technical reviews, specifically SRR, CDR, SVR, and/or PRR.

IA Entry Criteria

- Any critical technology elements necessary to achieve the desired IA solution for the preferred concept have been identified.

IA Completion/Exit Criteria

- All IA specific CTE's can achieve the TRA level required for the appropriate Acquisition Milestone, (ie. TRL = 5 at Milestone A, TRL = 6 at Milestone B, and TRL = 7 at Milestone C).

IBR – Integrated Baseline Review

IA Entry Criteria

- Update system specifications with IA requirements
- Identify IA risks
- Further develop schedule and cost plans for IA activities
- Update IA Strategy

IA Completion/Exit Criteria

- Executable IA schedule
- Known and manageable IA risks

SFR – System Functional Review

The SFR is a multi-disciplined product and process assessment to ensure that the system under review can proceed into preliminary design, and that all system requirements and functional performance requirements derived from the CDD are defined, aligned with the external environment (systems and infrastructure) and consistent with cost (program budget), schedule (program schedule), risk, and other system constraints.

IA Entry Criteria

- SFR technical products listed below for both hardware and software system elements with IA concerns appropriately addressed
    1. Updated system specification, to include a description of interoperability and/or distributed services requirements
    2. Preliminary functional baseline (with supporting trade-off analyses and data),
    3. Preliminary system software functional requirements
    4. CARD changes (if any)
    5. SEP changes (if any)
    6. Updated risk assessment
    7. Software Test Plan ready to be placed under configuration management
    8. Software Requirements Documents ready to be placed under configuration management
    9. Interface Requirements Specifications ready to be placed under configuration management
    10. Identified software and interface requirements to be implemented in each incremental build and/or release
- Secure resources for IA. Include IA in program budget to cover the cost of developing, procuring, testing, certifying and accrediting, and maintaining the posture of system IA solutions. Ensure appropriate types of funds are allocated (e.g. Operations & Maintenance) for maintaining IA posture in out years
- Contract language specifies IA/security requirements
- DoD Information Technology Portfolio Repository – DON (DITPR-DON) registration of system(s) completed
- Initiate C&A process. If systems have been determined to be Platform IT candidates, then Platform IT designation is required from the ODAA/MCEN DAA
- Draft Information Support Plan
- Net-Ready KPP
- Detailed IA/security design
- Integrated system architecture and supporting views

IA Completion/Exit Criteria

IA concerns have been addressed as part of the following overall exit criteria:

1. The system functional requirements, as disclosed, can satisfy the CDD
2. The system functional requirements are sufficiently detailed and understood to enable system design to proceed
3. Adequate processes and metrics are in place for the program to succeed
4. The risks are known and manageable for design and development
5. The program schedule is executable (technical/cost risks)
6. The program properly staffed
7. The program with the approved functional baseline is executable within the existing budget
8. The updated CARD is consistent with the approved functional baseline
9. The updated cost estimate fits within the existing budget?
10. The System Functional Baseline has been established to enable preliminary design to proceed with proper Configuration Management (CM)
11. All appropriate documents have been updated and put under CM control?
12. The software functionality is in the approved functional baseline consistent with the updated software metrics and resource loaded schedule

PDR – Preliminary Design Review

The PDR is a multi-disciplined product and process assessment to ensure that the system under review can proceed into detailed design, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.

IA Entry Criteria

An IA preliminary design and test plan, both tracing back to the CDD, should be available.

PDR technical products for each system hardware and software configuration item – containing appropriate IA discussion - have been made available to the cognizant PDR participants prior to the review:

1. Updated system specification, to include a description of interoperability and/or distributed services requirements along with IA impacts
2. Preliminary subsystem design specifications for each configuration item (hardware and software), with supporting tradeoff analyses and data, as required. The preliminary software design specification should include a completed definition of the software architecture, and a preliminary database design description is applicable. The approach to writing secure code and developing secure architecture also needs to be available.
3. Confidence that the preliminary design has been reflected in the software estimated cost to complete
4. Updated risk assessment to include both security risk and overall program risk
5. SEP changes (if any)
6. CARD changes (if any)
7. Updated integrated system architecture and supporting views
8. If appropriate, an indication of whether the ISP has been entered into the Joint C4I Program Assessment Tool - Empowered (JCPAT-E)

IA Completion/Exit Criteria

1. The proper competencies were represented at the review
2. The status of the technical effort and design (including IA design) indicates OPEVAL success (operationally suitable and effective)
3. The preliminary design (including Defense-in-Depth and IA controls), as disclosed, can satisfy the CDD
4. The system allocated baseline has been established and documented to enable detailed design to proceed with proper configuration management
5. Adequate processes and metrics are in place for the program to succeed
6. The risks are known and manageable for developmental test/operational test (DT/OT), including Security Test and Evaluation
7. The program schedule is executable (technical/cost risks)
8. The program is properly staffed, including IA personnel

9. The program is executable with the existing budget and with the approved system allocated baseline
10. The software estimated cost to complete is consistent with the preliminary design approved at the PDR
11. The updated cost estimate (including IA cost) fits within the existing budget
12. The preliminary design is producible within the production budget
13. The updated CARD is consistent with the approved allocated baseline
14. The software functionality in the approved allocated baseline is consistent with the updated software metrics and resource-loaded schedule
15. Verification that the integrated architecture System and Technical Views support, and are consistent with, the appropriate Operational architecture, the CPD, the Information Support Plan (ISP) and Net-Ready Key Performance Parameter (NRKPP)
16. Verification (where appropriate) that system data has been entered/updated in the FORCEnet Implementation Baseline (FIBL).

CDR – Critical Design Review

The CDR is a multi-disciplined product and process assessment to ensure that the system under review can proceed into system fabrication, demonstration, and test, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.

IA Entry Criteria

- IA test procedures developed, including validation procedures for DoDI 8500.2 IA Controls
- Updated IA schedule and budget
- Updated IA risks
- Detailed IA design
- The following items, including all relevant IA design details, are available:
    1. Updates to the systems specification and functional specification
    2. Product specifications for each hardware and software configuration item, along with supporting trade-off analyses and data
    3. Current risk assessment – both IA risk and program risk
    4. SEP changes (if any)
    5. CARD changes (if any)
    6. Software Design Document complete and ready to be placed under configuration management
    7. Software Interface Design Document complete and ready to be placed under CM
    8. Preliminary Test Procedures for Software Integration and Systems testing available for review
    9. Integrated architecture System and Technical Views supporting and consistent with the Operational architecture and the CPD and NR-KPP
    10. The data in the FIBL has been updated, whenever this is required

IA Completion/Exit Criteria

- Detailed IA design satisfies the CDD
- IA schedule is executable
- IA risks are known and manageable
- Other criteria involving IA design and execution:
    1. The proper competencies were represented at the review
    2. The status of the technical effort and design indicates OPEVAL success (operationally suitable and effective)
    3. The detailed design, as disclosed, satisfies the CDD, and CPD, if available

4. The system product baseline has been established and documented to enable hardware fabrication and software coding to proceed with proper configuration management
5. Adequate processes and metrics are in place for the program to succeed
6. The risks are known and manageable
7. The program schedule is executable (technical/cost risks)
8. The program is properly staffed, including IA personnel
9. The program is executable with the existing budget and the approved product baseline
10. The software estimated cost to complete is consistent with the critical design approved at the CDR
11. The detailed design is producible within the production budget
12. The updated CARD is consistent with the approved product baseline
13. Critical Safety Items and Critical Application Items (and their security equivalents) are identified
14. The updated cost estimate fits within the existing budget
15. The software functionality in the approved product baseline is consistent with the updated software metrics and resource-loaded schedule
16. The program is compliant with the program's approved FORCEnet category FIBL, where this is applicable

TRR – Test Readiness Review

The TRR is a multi-disciplined product and process assessment to ensure that the subsystem, system, or systems of systems under review is ready to proceed into formal test.

IA Entry Criteria

IA testing, and analysis of test results (including residual risk assessment) are included in the following:

a. Configuration of system under test has been defined and agreed to. All software in the system under test have been placed under configuration management or have been defined in accordance with an agreed to plan and a Version Description Document has been made available to TRR participants (minimum of 7 working days prior to the review). All software in the system under test is frozen. All interfaces are under configuration control. All Ports, Protocols and Services are tentatively defined.

b. All applicable functional, unit level, subsystem, system integration, and qualification testing has been conducted successfully.

c. Test Requirements have been documented and are fully traceable to system, engineering, operational or program requirements.

d. All TRR specific materials such as test plans, test cases, and procedures have been available to all participants prior to conducting the review (minimum of 7 working days).

e. All test certifications or flight approvals, if required, have been obtained or will be completed prior to the beginning of the testing.

f. All known system discrepancies have been identified and dispositioned in accordance with an agreed to plan.

g. All previous design review exit criteria and key issues have been satisfied in accordance with an agreed to plan.

h. All required test resources (people, facilities, test articles, test instrumentation) have been identified and are available to support required tests. For IA, this will include applicable IA test planning documentation.

i. Roles and responsibilities of all test participants are defined and agreed to.

IA Completion/Exit Criteria

IA test plans are completed and approved. Identification and coordination of required IA test resources is completed. In addition, IA impacts will be included in the following criteria:

a. Test requirements are traceable, documented and approved. Adequate test plans based on these traceable requirements are completed and approved for the system under test.

b. Adequate identification and coordination of required test resources is completed

c. Previous component, subsystem, system test results form a satisfactory basis for proceeding into planned tests.

d. Risk level identified and accepted by Program/Competency leadership as required.

e. Testers have a high degree of confidence that the system under test will pass the testing successfully and agree that the anomalies, limitations, and vulnerabilities will not impact this.

f. The developers are aware of the testers' plans and have a high degree of confidence that the system under test will pass the testing successful.

Appendix F
Integrated Logistics Support

F.1 Information Assurance Operations and Sustainment Considerations

Part of the IAM's responsibilities throughout the program's life cycle is to consider the types of deliverables (both data and product) that should be supplied to the operators, maintainers, administrators, fleet IAM/IAO's and integrating Engineering Support Activities and to effectively identify those deliverable requirements to the PM's team. Starting with the program's systems Production and Deployment Phases, and continuing over the Operations and Sustainment Phases of acquisition, these deliverables are generally grouped under the heading of Integrated Logistics Support (ILS).

As shown in Figure F-1 below, by the time the program enters these phases, most major decisions about support considerations for a system will have already been established. Program managers or IAM's who wait until the O&S phase to begin thinking about how to support the information assurance posture of the system will face significant challenges.

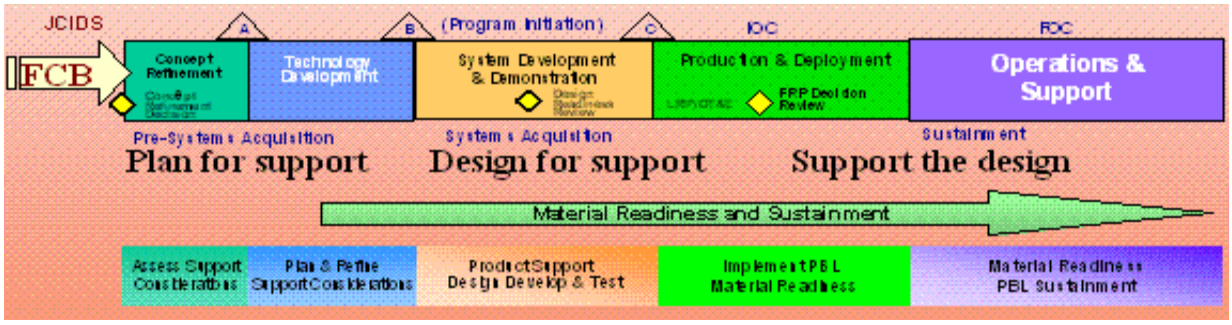


Figure F-1

Readiness to deploy a system, whether that deployment is to a Developmental or Operational Test environment, or to the final intended fleet operational environment requires that the appropriate logistics elements listed in Figure F-1 have been addressed from an IA perspective.

F.2 Logistics Elements

This section outlines the IA elements associated with each logistics element. Additional descriptions of the logistics elements can be found in the DAG.

F.2.1 Maintenance Planning

Maintenance planning activity usually begins when requirements are being formalized during the program's SRR timeframe, and continues throughout the lifecycle of the program. The program's Maintenance Plan (sometimes called the ILS Plan) uses the program's Requirements Traceability Matrix (RTM) as a primary source for determining logistics support requirements. The maintenance plan establishes maintenance concepts and requirements for the life of the system. It includes, but is not limited to: levels of repair, repair times, testability requirements, support equipment needs, manpower skills, facilities, interservice, organic and contractor mix of repair responsibility, and site activation. This element has a great impact on the planning, development, and acquisition of other logistics support elements.

This document is a key document that provides source information to the other logistics support elements. Many IA issues can be resolved by working with the PM's logistics team to ensure that the IA requirements have been properly incorporated into the maintenance planning.

The IAM should ensure that IA requirements are appropriately considered by the maintenance plan. The IA requirements that should be addressed include any specific requirements for IA-enabled products, frequency and mean time to update data associated with IAVA and IAVB (when applicable), physical security requirements for depot and other repair facilities, personnel clearance requirements (from the program's DD-254), and IA personnel training requirements for personnel at depot and repair facilities (per DoD 8570.1-M).

F.2.2 Supply Support

Supply support consists of all management actions, procedures, and techniques necessary to determine requirements to acquire, catalog, receive, store, transfer, issue and dispose of spares, repair parts, and supplies. Included are requirements for provisioning for initial support, as well as acquiring, distributing, and replenishing inventories. In layman terms, this means having the right spares, repair parts, and supplies available, in the right quantities, at the right place, at the right time, at the right price. The process includes provisioning for initial support, as well as acquiring, distributing, and replenishing inventories. Key supply support requirements are derived based on analyses conducted during the development of the program Maintenance Plan. These analyses may start in the period between System Requirements Review and Preliminary Design Review, but intensify following Critical Design Review.

IAM inputs to supply support include provisioning issues related to IA products and IA-enabled products.

F.2.3 Support and Test Equipment

Support and Test Equipment is made up of all equipment (mobile or fixed) required to support the operation and maintenance of a system. This includes ground handling and maintenance equipment, tools, metrology and calibration equipment, and manual and automatic test equipment. Support and Test Equipment requirements are usually being formalized during the program's SRR timeframe, and new requirements are usually identified during the program's System Development and Demonstration phase. Support and Test Equipment may also be completely separate program developments. Program managers are expected to decrease the proliferation of support equipment into the inventory by minimizing the development of new support equipment and giving more attention to the use of existing government or commercial equipment.

Program support and test equipment requirements are derived based on analyses conducted during the systems engineering development of the system, and analyses conducted during the development of the program Maintenance Plan.

IAM's should ensure that appropriate IA controls have been incorporated into Support Equipment and Test Equipment interface documents and specifications, as well as ensuring that appropriate IA language is included into Support and Test Equipment acquisition contracts and source selection criteria.

F.2.4 Manpower and Personnel

Manpower and Personnel involves the identification and acquisition of personnel (military & civilian) with the skills and grades required to operate, maintain, and support systems over their lifetime. Early identification is essential. If the needed manpower is an additive requirement to existing manpower levels of an organization, a formalized process of identification and justification should be made to higher authority. Add to this the necessity to train these persons, new and existing, in their respective functions on the new system, and the seriousness of any delays in the accomplishment of this element becomes apparent. In the case of military requirements, manpower needs can, and in many cases do, ripple all the way back to recruiting quotas.

Manpower & support requirements for sustaining the IA of a system will be addressed by the manpower & support analyses derived from the Maintenance Plan.

F.2.5 Training and Training Support

Training and Training Support consists of the policy, processes, procedures, techniques, training devices, and equipment used to train civilian and military personnel to acquire, operate and support a system. This includes individual and crew training, new equipment training, initial, formal, and on-the-job training. Though the greatest amount of training is accomplished just prior to the fielding of a system, it should be remembered that in most programs, a large number of individuals will need to be trained during system development to support the system test and evaluation program.

Training and Training Support requirements are derived based on analyses conducted during the systems engineering development of the system, and analyses conducted during the development of the program Maintenance Plan. Training system requirements may begin being formalized during the program's SRR timeframe, and new requirements can be identified during the program's System Development and Demonstration phase. Training support requirements are generally developed after a program's CDR. From an IA perspective, training includes instruction on use of IA products and IA-enabled products, as well as related IA duties, such as incident response and dealing with IAVAs. Refresher training, such as that required to keep security certifications current, should be addressed here as well. The IAM should coordinate with the logistics planners to ensure that training plans and support concept of operations address these requirements.

Training systems (such as simulators) are sometimes separate program developments by themselves. IAM's should ensure that appropriate IA controls have been incorporated into Training System and Training Equipment interface documents , specifications as well as ensuring that appropriate IA language is included into Training System acquisition contracts and source selection criteria..

F.2.6 Technical Data

From a logistics perspective, Technical Data represents recorded information of scientific or technical nature, regardless of form or character (such as manuals and drawings). From the IT perspective, technical data comprises the manuals and drawings that provide instructions on how

to operate and maintain the system. Thus software documentation (including requirements documents, user guides, release notes, and the like) is considered technical data while the computer programs themselves are not. The IA portions of requirements documentation and user guides, along with such items as the Security Features User Guide and system administrator manuals, are examples of technical data that will require the IAM's attention.

Technical manuals and engineering drawings are the most expensive and probably the most important data acquisitions made in support of a system. It is the technical manuals that provide the instructions for operation and maintenance of a system. A **costly and frequent** oversight of many programs stems from the failure to properly identify and contract for technical data. IA professionals should pay special attention during the development of contract documentation to ensure that appropriate technical data are identified on the contracts deliverable requirements list, the contract's statement of work, and that the data delivery requirements are appropriate to support the program's schedule.

The documents listed in Table F-1 are common types of Technical Data that IA professionals might consider procuring or developing organically. The program IAM/IAO should plan to acquire or develop during the acquisition of the Platform IT system. Whether the choice is to acquire them from the system OEM or develop them, these documents will need to be verified and reviewed throughout the SETR process.

F.2.7 Computer Resources Support

Computer Resources Support encompass the facilities, hardware, software, documentation, manpower, and personnel needed to operate and support mission critical computer hardware/software systems. It is in this area that the IAM needs to be the most effective; the analysis and documentation discussed in earlier sections can be reused to great effect here.

Many large programs, such as those marked as ACAT 1, will have some form of computer resource working group (it may be called by various names and it may be viewed as its own Integrated Product Team) to accomplish the necessary planning and management of computer resources support. If such a group exists, the IAM should actively engage with it.

F.2.8 Facilities

Facilities consists of the permanent and semi-permanent real property assets required to support a system, including studies to define types of facilities or facility improvements, location, space needs, environmental requirements, and equipment. Physical security and network requirements (including physical wiring, conduits, man traps, and the like) are some of the IA issues relevant to facilities.

Like many of the other logistics elements, facilities requirements are derived during the maintenance planning process. While many considerations about facilities may be made even during the concept definition stage, the actual facilities engineering details typically begins after CDR. Since last minute decisions to deploy a system to a different locale might lead to costly delays, the IAM should engage with the logistics team early in the facility planning process to ensure that all IA-related facility issues are addressed.

F.2.9 Packaging, Handling, Storage and Transportation (PHS&T)

PHS&T is the combination of resources, processes, procedures, design, considerations, and methods to ensure that all system, equipment, and support items are preserved, packaged, handled, and transported properly, including environmental considerations, equipment preservation for the short and long storage, and transportability. IA issues associated with PHS&T include:

- Transporation and handling of classified hardware
- Shipment of software and software updates, mainly if CDs, portable hard drives or flash drives are being considered. Shipment of software over networks should be treated under computer resources support (section F.2.7).

PHS&T requirements generally begin to be addressed in detail during the program's PDR and CDR timeframes, particularly during sub-system and component reviews leading up to the program's main PDR and CDR.

F.2.10 Design Interface

Design Interface is the relationship of logistics-related design parameters to readiness and support resource requirements. Logistics-related design parameters include the following:

- Reliability and maintainability (R&M)
- Human factors
- System safety
- Survivability and vulnerability
- Hazardous material management
- Standardization and interoperability
- Energy management
- Corrosion
- Nondestructive inspection
- Transportability

This area of ILS is included here to highlight certain logistics disciplines whose methods may be tailored and reused to achieve IA requirements (such as system safety, standardization and interoperability). Some elements of reliability and vulnerability analysis (including Poisson curves associated with probability of infection and mean time between infections) may also be relevant.

Table F-1 Typical Data Needed by End Users of Platform IT Systems

IAM End User	Engineering Support Activity*	Operator End User	Maintenance / SysAdmin
Tech Pubs and Operating Reports	Tech Pubs and Operating Reports	Tech Pubs and Operating Reports	Tech Pubs and Operating Reports
Training Guide	Training Guide	Training Guide	Training Guide
Risk Mitigation Guidance and Training	Risk Mitigation Guidance and Training	Risk Mitigation Guidance and Training	Risk Mitigation Guidance and Training
System CONOPS incl Security CONOPS**	System CONOPS incl Security CONOPS	Operational CONOPS	System CONOPS incl Security CONOPS
Residual Risk Report	Residual Risk Report	CPUG	Residual Risk Report
Review of IA Controls	Summary of IA Portion of OPEVAL report		Review of IA Controls
Multi Level Security Device Settings	Multi Level Security Device Settings		Multi Level Security Device Settings
Firewall Ports Protocol Services (where applicable)	Firewall Ports Protocol Services (where applicable)		Firewall Ports Protocol Services (where applicable)
Access Control Lists	Access Control Lists		Access Control Lists
SFUG/CPUG			SFUG/CPUG
PIT Determination Letter			
Residual Risk Acceptance Letter from PIT-DAA	Residual Risk Acceptance Letter from PIT-DAA	Residual Risk Acceptance Letter from PIT-DAA	Residual Risk Acceptance Letter from PIT-DAA
* The Engineering Support Activity is the cognizant engineering support organization for the system or facility where the PIT system			
** A Security CONOPS should include IAVM implementation			

Appendix G
Definitions / Acronyms

This appendix defines PIT related terms for IT networks, systems and IT components within the Department of the Navy (DON). It is based primarily on Department of Defense (DoD) Instruction 8500.1 and Secretary of the Navy (SECNAV) Instruction SECNAVINST 5239.3A. Definitions, concepts and interpretation are derived from these sources. This appendix also provides a list of definitions for the acronyms used in this document.

G.1 DEFINITIONS

GENERAL PURPOSE

A system used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications. General purpose systems are normally not built for a unique application, and do not fall outside the definition of special purpose systems as defined by DoD 8500 series guidance.

GLOBAL INFORMATION GRID (GIG)

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel.

PLATFORM

A vehicle, structure or person that performs a mission in support of US National Security policy; and aboard or in which a DoD national security system may be installed to support assigned missions. Generally, the term “platform” includes, but is not limited to, Aircraft, Ship, Submarine, Shore Facility (such as NOC, JIC, Command Center, Hospital, Base Power Plants), Ground Vehicle (such as HMMWVs, Tanks, Strykers), Remotely Operated Vehicle (such as UAV, USV, UUV), and a Sailor or Marine in the field.

PLATFORM IT

Derived from DoDD 8500.1, Paragraph E2.1.16.4, Platform IT:

1. REFERS TO computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. PIT does not include general purpose systems.

2. MAY:
   a. Reside aboard or on a platform
   b. Be stand-alone
   c. Have an interconnection to other Platform IT (known as a “Platform IT-to-Platform IT Interconnection”)

d. Have a Platform IT Interconnection (see DoDI 8500.1) to other IT that is not Platform IT (e.g., a general-use ship's network, such as ISNS, or a non-Platform IT system)

BOUNDARY

The physical and/or logical limit of a platform or the physical and/or logical limit of the information system as determined by the system description.

CONNECTION

The physical or logical interface that allows data to flow between components in a system, between systems within a system-of-systems, or between information systems installed onboard different platforms.

1. **Platform IT Interconnection (PITI)**:
   a. A physical or logical connection at or crossing the boundary between a Platform IT system and a non-Platform IT system

2. **Platform IT to Platform IT Interconnection (PTPI)**:
   a. A physical or logical connection at or crossing the boundary between a Platform IT system and another Platform IT system

REAL-TIME

Systems in which the correctness of the system depends not only on the logical result of computations, but also on the time at which the results are produced or the sense of urgency of the systems information processing and the information processed by the system to completion of the platform's mission.

SPECIAL-PURPOSE SYSTEM

Derived from DoDD 8500.1, Paragraph E2.1.16.4.

System or platform that employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or necessary in real time for the performance of the system's mission. Examples of special purpose systems include weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric.

G.2 ACRONYMS

Acronym	Definition
A	
ACAT	Acquisition Category
ASN (RDA)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ASR	Alternative Systems Review
ATO	Authorization To Operate
C	
C&A	Certification and Accreditation
CA	Certification Authority or Certification Agent
CAD	Component Advanced Development
CARD	Cost Analysis Requirements Description
CDD	Capability Development Document
CDP	Capabilities Development Package
CDR	Critical Design Review
CDRL	Contract Data Requirements Lists
CI	Configuration Item
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
COE	Center of Excellence
COTS	Commercial-Off-The-Shelf
CPD	Capability Production Document
CPUG	Control Panel User Guide
CSCI	Computer Software Configuration Item
CT&E	Certification Test and Evaluation
CTE	Critical Technology elements
D	
DAA	Designated Accrediting Authority
DAG	Defense Acquisition Guidebook
DCID	Director of Central Intelligence Directive
DFARS	Defense Federal Acquisition Regulation Supplement
DIACAP	DoD Information Assurance Certification and Accreditation Process
DITPR-DON	DoD Information Technology Portfolio Repository - Department of the Navy
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
DT	Development Test

E

ERB	Executive Review Board
ECP	Engineering Change Proposal
EII	Echelon II
ESI	Enterprise Software Initiative
EVM	Earned Value Management

F

FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act
FOT&E	Follow-on Operational Test and Evaluation
FRP	Full Rate Production
FRR	Flight Readiness Review
FY	Fiscal Year

G

GIG	Global Information Grid
GOTS	Government Off-The Shelf

I

IA	Information Assurance
IAC	Information Assurance Controls
IAM	Information Assurance Manager
IAS	Information Assurance Strategy
IATF	Information Assurance Technical Framework
IATO	Interim Authorization To Operate
IATT	Interim Authorization To Test
IA TWH	Information Assurance Technical Warrant Holder
IAVA	Information Assurance Vulnerability Advisory
IAVB	Information Assurance Vulnerability Bulletin
IBR	Integrated Baseline Review Process
ICD	Initial Capabilities Description
ILSMT	Integrated Logistics Management Team
IOT&E	Initial Operational Test & Evaluation
IP	Internet Protocol
IRR	Integration Readiness Review
IRS	Interface Requirements Specification
ISP	Information Support Plan
ISR	In Service Review
ISSE	Information System Security Engineering
ISSEP	Information Systems Security Engineering Professional
IT	Information Technology
ITR	Initial Technical Review
IV&V	Independent Verification and Validation

J

JCIDS	Joint Capabilities Integration and Development System

K

KPP	Key Performance Parameters

L

LRIP	Low Rate Initial Production

M

MAC	Mission Assurance Category
MAIS	Major Automated Information Systems
MC	Mission Critical
MCEN DAA	Marine Corps Enterprise Network Designated Accrediting Authority
MDA	Milestone Decision Authority
ME	Mission Essential
MNS	Mission Needs Statement
MS	Milestone
MSC	Major Subordinate Commad

N

NAVAIR	Naval Air Systems Command
NAVAIRINST	Naval Air Systems Command Instruction
NIST	National Institute of Standards and Technology
NR-KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy

O

ODAA	Operational Designated Accrediting Authority
O&M,N	Operation and Maintenance, Navy
OPEVAL	Operational Evaluation
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT	Operational Test
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review

P

PCA	Physical Configuration Audit
PCR	Physical Configuration Review
PDR	Preliminary Design Review
PEO	Program Executive Officer
PII	Personally Identifiable Information
PIT	Platform Information Technology *also* Platform IT
PITI	Platform Information Technology Interconnections
PM	Program Manager
PMO	Program Management Office

POAM	Plan of Action and Milestones
POM	Program Objective Memorandum
PPS	Ports, Protocols and Services
PR	Program Review
PRR	Production Readiness Review
PTPI	Platform IT to Platform IT Interconnection

R

RTM	Requirements Traceability Matrix

S

SDD	System Development and Demonstration
SECNAVINST	Secretary of the Navy Instruction
SEMP	Systems Engineering Master Plan
SETR	Systems Engineering Technical Review
SEP	Systems Engineering Plan
SFR	System Functional Review
SFUG	Security Features User Guide
SIRD	Software Interface Requirements Description
SOO	Statement of Objectives
SOW	Statement of Work
SRD	System Requirements Document
SRR	Systems Readiness review
SSEP	System Security Engineering Plan
SSR	Software Specification Review
SSWG	System Safety Working Group
ST&E	Security Test and Evaluation
SVR	Systems Verification Review
SwRS	Software Requirements Specification

T

TDP	Technical Data Package
T&E	Test and Evaluation
TEMP	Test and Engineering Master Plan
TRA	Technology Readiness Assessment
TRB	Technical Review Board
TRL	Technology Readiness Levels
TRR	Test Readiness Review