

Chapter 7

Acquiring Information Technology and National Security Systems

7.0 CHAPTER OVERVIEW

7.0.1. Purpose

The goal of this chapter is to help program managers and Sponsors/Domain Owners implement DoD policies intended to achieve “fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space.” This chapter explains how the Department of Defense is using a net-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter provides descriptions and explanations of many of the associated topics and concepts.

This chapter also discusses many of the activities that enable the development of net-centric systems. However, not all activities are the direct responsibility of the Program Manager. Many activities reflect Department-level effort that occurs prior to or outside of the acquisition process. The detailed discussions of such a broad set of activities are presented here to help the Program Manager understand the context of the capabilities described in the Joint Capabilities Integration and Development System documents and required of the system under development.

7.0.2. Contents

This chapter contains 10 sections that present the Program Manager with a comprehensive review of topics, concepts, and activities associated with the acquisition of Information Technology and National Security Systems.

- [Section 7.1](#), “Introduction,” explains net-centricity in the context of the discussions and requirements outlined in the various other sections of this chapter.
- [Section 7.2](#), “Global Information Grid (GIG),” explains several important concepts that provide a foundation for acquiring net-centric Information Technology and National Security Systems. The overarching concept is that of the GIG as the integrated enterprise information technology architecture used to describe and document current and desired relationships among warfighting operations, business and management processes, and information technology. The integrated architecture products and artifacts:
 - Describe existing and desired capabilities;
 - Provide a basis for interoperability and supportability reviews and certifications;
 - Provide a component of the [Net-Ready Key Performance Parameter](#);
 - Provide required components of the Capability Development Document and Capability Production Document;
 - Develop and describe Key Interface Profiles; and
 - Document consistency with the GIG architecture and policies.

Section 7.2 continues with an explanation of compliance with the GIG architecture, and outlines eight requirements for compliance. It discusses a tool called the Net-Centric Operations and Warfare Reference Model (NCOW RM). (The NCOW RM helps

program managers and Sponsors/Domain Owners describe their transition from the current environment to the future net-centric environment. This will be a key tool during program oversight reviews.) The section defines what compliance with the NCOW RM means, and provides a method of assessing compliance with the model.

Finally, section 7.2 also introduces the DoD Net-Centric Data Strategy, the DoD Information Assurance Strategic Plan, and the GIG Enterprise Services Strategy, and relates each of these strategies to the NCOW RM.

The remaining sections elaborate on specific areas on which the Sponsors/Domain Owners and Program Managers should focus as they work to deliver and improve the reach, richness, agility, and assurance of net-centric capabilities:

- [Section 7.3](#), “Interoperability and Supportability of Information Technology and National Security Systems,” explains interoperability and supportability, outlines the use of the Net-Ready Key Performance Parameter in these processes, and describes the process of building an Information Support Plan.
- [Section 7.4](#), “Net-Centric Data Strategy,” provides guidance on implementing the Net-Centric Data Strategy and outlines important data tasks as they relate to the acquisition process.
- [Section 7.5](#), “Information Assurance,” explains the requirements for Information Assurance and provides links to resources to assist in developing an Information Assurance strategy.
- [Section 7.6](#), “Electromagnetic Spectrum,” offers help understanding the process of Spectrum Supportability.
- [Section 7.7](#), “Business Modernization Management Program,” provides important information for the Department’s business domains about the Business Modernization Management Program. The Business Modernization Management Program is developing an essential subset of the GIG architecture called the Business Enterprise Architecture. Section 7.7 also provides links to related websites and resources.
- [Section 7.8](#), “Clinger-Cohen Act,” helps program managers and Sponsors/Domain Owners understand how to implement the Clinger-Cohen Act and associated statutory and regulatory requirements.
- [Section 7.9](#), “Post Deployment Reviews,” discusses how the Department of Defense uses the Post Implementation Review to support Clinger-Cohen Act compliance. And finally,
- [Section 7.10](#), “Commercial, Off-The-Shelf (COTS) Solutions,” provides insight into Department guidance regarding acquisition of commercial-off-the-shelf (COTS) software products.

In summary, this chapter should help Program Managers and Sponsors/Domain Owners understand and apply the tools of the GIG architecture so that they can more effectively:

- Describe and measure the degree to which their programs are interoperable and supportable with the GIG;
- Ensure their programs employ and institutionalize approaches that make data visible, accessible, understandable, trusted, interoperable and responsive;

- Achieve the Department's objectives for Information Assurance;
- Ensure their programs will have assured, interoperable access to electromagnetic spectrum; and
- Achieve these goals within the constraints of the law and where possible, through the use of commercially available solutions.

7.1 INTRODUCTION

The [DoD Transformation Planning Guidance](#) defines the desired outcome of transformation as “fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space.” The goal of this chapter is to help Program Managers and Sponsors/Domain Owners implement the DoD policies that are intended to achieve this outcome. This introduction briefly explains net-centricity in context of the requirements outlined in the various other sections of this chapter.

Net-centricity is “the realization of a robust, globally networked environment (interconnecting infrastructure, systems, processes, and people) within which data is shared seamlessly and in a timely manner among users, applications, and platforms. By securely interconnecting people and systems, independent of time or location, net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Users are empowered to better protect assets; more effectively exploit information; more efficiently use resources; and unify our forces by supporting extended, collaborative communities to focus on the mission.”

The Department’s approach for transforming to net-centric operations and warfare aims to achieve four key attributes: reach, richness, agility, and assurance. This approach uses the Global Information Grid as “the organizing and transforming construct for managing information technology throughout the Department.” It envisions moving to trusted net-centric operations through the acquisition of systems and families-of-systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology infrastructure, to include National Security Systems. This Information Technology infrastructure includes data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.

The rest of this chapter describes the concepts, topics, and activities to achieve this transformation.

7.2 GLOBAL INFORMATION GRID (GIG)

7.2.1. Introduction

The Global Information Grid (GIG) is the organizing and transforming construct for managing information technology (IT) throughout the Department. GIG policy, governance procedures, and supporting architectures are the basis for developing and evolving IT capabilities, IT capital planning and funding strategies, and management of legacy (existing) IT services and systems in the DoD. In discussing the GIG and how a particular program interacts with, supports, or relies upon the GIG, it is useful to think of the GIG from three perspectives—its vision, its implementation, and its architecture.

7.2.1.1. The Global Information Grid (GIG) Vision

The GIG vision is to empower users through easy access to information anytime and anyplace, under any conditions, with attendant security. Program managers and Sponsors/Domain Owners should use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. The goal is to increase the *net-centricity* of warfighter, business, intelligence, DoD enterprise management, and enterprise information environment management operations by enabling increased *reach* among the GIG users, increased *richness* in the information and expertise that can be applied to supporting operational decisions, increased *agility* in rapidly adapting information and information technology to meet changing operational needs, and increased *assurance* that the right information and resources to do the task will be there when and where it is required.

7.2.1.2. The Implementation Component of the Global Information Grid (GIG)

The implementation component of the GIG is the existing, globally interconnected, end-to-end set of capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information. The GIG includes all Information Technology (IT) and National Security Systems (NSS) throughout the DoD, and their interfaces to allied and coalition forces, industry, and other Federal agencies. All DoD information systems that currently exist or that have been approved for implementation comprise the GIG. Every DoD acquisition program having an IT component is a participant in the GIG. Each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG. Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, and program managers should consider the existing and planned capabilities of the GIG that might be relevant as they develop their integrated architectures, Joint Capabilities Integration and Development System documentation (see CJCSI 3170.1), and related program requirements.

7.2.1.3. The DoD Enterprise Architecture

The DoD Chief Information Officer (CIO) plays the central role in the description, development, acquisition, and management of the Department's Information Technology (IT) capabilities. As the Secretary of Defense's principal staff assistant for IT and information resources management, the CIO develops, maintains, and uses the Department's enterprise IT architecture—the [Global Information Grid \(GIG\) Architecture and the Net-Centric Operations](#)

[and Warfare \(NCOW\) Reference Model](#) to guide and oversee the evolution of the Department's IT-related investments to meet operational needs.

The GIG Architecture is the Department's *IT architecture*. It describes the implementation component of the GIG, with integrated operational, systems, and technical views. The GIG Architecture fulfills, in part, the requirement to develop a Department-wide enterprise architecture. As defined by the Office of Management and Budget, *enterprise architecture* is the explicit description and documentation of the current and desired relationships among business and management processes and IT. The Enterprise Architecture describes the "current architecture" and "target architecture," and provides a strategy that will enable an agency to transition from its current state to its target environment. All DoD architectures, including warfighter, intelligence, business process, and enterprise management architectures, are part of the GIG Architecture. Versions 1 and 2 of the GIG Architecture are the current and target DoD IT architectures, respectively and describe the enterprise view of the GIG.

The NCOW Reference Model provides the means and mechanisms for the Department and its combat developers, sponsors, domain owners, and program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2).

7.2.1.4. Net-Centric Operations and Warfare Reference Model (NCOW RM)

The NCOW RM (see the [DoD Global Information Grid Architectures](#) website) represents the strategies for transforming the enterprise information environment of the Department. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the Department of Defense. Included in this description are the activities and services required to establish, use, operate, and manage this net-centric enterprise information environment. Major activity blocks include the generic user-interface (A1), the intelligent-assistant capabilities (A2), the net-centric service (core, Community of Interest, and enterprise control) capabilities (A3), the dynamically allocated communications, computing, and storage media resources (A4), and the enterprise information environment management components (A5). Also included is a description of a selected set of key standards and/or emerging technologies that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized.

Transforming to a net-centric environment requires achieving four key attributes: reach, richness, agility, and assurance. The initial elements for achieving these attributes include the Net-Centric Enterprise Services Strategy, the [DoD Net-Centric Data Strategy](#), and the DoD Information Assurance (IA) Strategy to share information and capabilities. The NCOW RM incorporates (or will incorporate) these strategies as well as any net-centric results produced by the Department's Horizontal Fusion pilot portfolio.

The NCOW RM provides the means and mechanisms for acquisition program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2). In addition, the NCOW RM will be a key tool during program oversight reviews for examining integrated architectures to determine the degree of net-centricity a program possesses and the degree to which a program can evolve to increased net-centricity. Compliance with the NCOW RM is one of the four elements that comprise the [Net-Ready Key Performance Parameter](#).

7.2.2. Mandatory Policies

[DoD Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003:](#)

- Requires the DoD Chief Information Officer (CIO) to “lead the development and facilitate the implementation of the Global Information Grid Integrated Architecture, which shall underpin all mission area and capability architectures.” ([See Section 3.2.1.2](#)).
- Requires DoD acquisition programs to demonstrate consistency with GIG policies and architectures, to include relevant standards, at Milestones A, B and Full Rate Production Decision Review (FRPDR) (or their equivalent). ([See Enclosure 4, Table E4.T1, Clinger-Cohen Act \(CCA\) Compliance Table](#)).

A number of **other DoD directives and instructions** provide policies relating to the GIG. These include:

[CJCS Instruction 6212.01, Interoperability and Supportability of Information Technology \(IT\) and National Security Systems, November 20, 2003:](#)

It is DOD policy that all IT and NSS and major modifications to existing IT and NSS will be compliant with the Clinger-Cohen Act, DOD interoperability regulations and policies, and the most current version of the DOD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DOD system is a continuous process that must be managed throughout the lifecycle of the system. The NR-KPP is comprised of the following elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), applicable Global Information Grid (GIG) Key Interface Profiles (KIP), DOD information assurance requirements, and supporting integrated architecture products required to assess information exchange and use for a given capability. ([See paragraph 5.a.](#))

[DoD Directive 4630.5, Interoperability and Supportability of Information Technology \(IT\) and National Security Systems \(NSS\), May 5, 2004:](#)

IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare. ([See paragraph 4.2.](#))

[DoD Directive 5000.1, The Defense Acquisition System, May 12, 2003, Enclosure 1, Additional Policy:](#)

[E1.9:](#) Information Assurance. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems.

[E1.10:](#) Information Superiority. Acquisition managers shall provide U.S. Forces with systems and families of systems that are secure, reliable, interoperable,

compatible with the electromagnetic spectrum environment, and able to communicate across a universal information technology infrastructure, including NSS, consisting of data, information, processes, organizational interactions, skills, analytical expertise, other systems, networks, and information exchange capabilities.

E1.13: Interoperability. Systems, units, and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units, and forces and shall effectively interoperate with other U.S. Forces and coalition partners. Joint concepts and integrated architectures shall be used to characterize these interrelationships.

[DoD Directive 8100.1, Global Information Grid Overarching Policy, September 19, 2002 \(Certified current as of November 21, 2003\)](#):

Addresses GIG Architecture compliance and includes the following requirements:

Section 4.3. [requires GIG assets to] *be interoperable, in accordance with approved requirements documents, and compliant with the operational, system, and technical views ... of the GIG architecture.*

Section 4.4.3. [requires development of] *an integrated DoD Architecture with operational, system, and technical views, [to be] maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate the accessibility and usability requirements of reference (k), and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities.*

Section 4.6. [The GIG Architecture] *shall be the sound and integrated information technology architecture required by [the Clinger-Cohen Act of 1996].*

7.2.3. Integration into the Acquisition Life Cycle

The following sections outline steps that the DoD Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, program managers, and/or other assigned managers should take to facilitate Global Information Grid (GIG) compliance and net-centricity when acquiring information technology-enabled capabilities that will interoperate within the GIG.

7.2.3.1. Before Milestone A

- Ensure that appropriate steps are taken to prepare or update an operational view (High-level Operational Concept Description, OV-1) of the integrated architecture for key mission areas and business processes using the DoD Architecture Framework and the guidance in [CJCS Instruction 6212.01, Enclosure E, paragraph 3](#). The Initial Capabilities Document should reflect this architecture work, as prescribed by [CJCS Instruction 3170.01](#) and in the format prescribed by [CJCS Manual 3170.01](#). It also supports analysis of alternatives, business process reengineering efforts, development of the acquisition strategy and information assurance strategy, and provides key artifacts that support development of the information support plan. Ensure that integrated architectures adhere to the three DoD net-centric strategies (Net-Centric Enterprise Services, Data, and Information Assurance Strategies) that have been incorporated into Net-Centric Operations and Warfare Reference Model.

- For systems in the scope of the [Business Management Modernization Program](#), architecture efforts should also align closely with the Business Enterprise Architecture.
- Develop an Initial Capabilities Document to describe capability gaps identified through analysis of joint concepts and integrated architectures. Use the criteria in [CJCS Instruction 6212.01, Enclosure E, Table E-1, “ICD Interoperability Standards Assessment Criteria.”](#) to ensure the Initial Capabilities Document and supporting OV-1 address required interoperability standards.

7.2.3.2. Before Milestone B

- Build or update the integrated architecture and supporting views (Operational View, Systems View, and Technical Standards View).
- Develop a Capability Development Document, as prescribed by [CJCSI 3170.01](#) and in the format prescribed by [CJCSM 3170.01](#), and a [Net-Ready Key Performance Parameter \(NR-KPP\)](#) that address the interoperability and Information Assurance requirements described in [CJCS Instruction 6212.01, Enclosure F, “Net-Ready Key Performance Parameter.”](#)
- Address issues associated with the updated integrated architecture, the Capability Development Document, and the Net-Centric Operations and Warfare Reference Model.
- Use the required integrated architecture products to support development of the [Information Support Plan](#). See [CJCS Instruction 6212.01, Table A-2, “JCIDS Documents/NR-KPP Products Matrix.”](#)
- Begin development of the Information Support Plan for Stage 1 Review. (See [section 7.3.6](#) for details.)
- Use the criteria in [CJCS Instruction 6212.01, Enclosure E, Table E-2, “Net-Centric Assessment Criteria.”](#) to guide the acquisition of net-centric capabilities.

7.2.3.3. Before Milestone C

- Update the integrated architecture and supporting views (Operational View, Systems View, and Technical Standards View) and ensure changes are reflected in the Capability Production Document, as prescribed by [CJCS Instruction 3170.01](#) in the format prescribed by [CJCS Manual 3170.01](#), and in the [Net-Ready Key Performance Parameter \(NR-KPP\)](#).
- If the program is entering the acquisition process at Milestone C, develop a NR-KPP using guidance in [CJCS Instruction 6212.01, Enclosure G, “Net-Ready Key Performance Parameter.”](#)
- Address any remaining issues associated with mapping to the [Net-Centric Operations and Warfare Reference Model](#), especially those related to Service-Level Agreements. A Service-Level Agreement defines the technical support, business parameters, and/or critical interface specifications that a service provider will provide to its clients. The agreement typically spells out measures for performance parameters and protocols used in interfacing, and consequences for failure.

- Ensure the program delivers capabilities responsive to the Capability Production Document and meets interoperability and Information Assurance requirements reflected in the updated NR-KPP.
- Use the criteria in [CJCS Instruction 6212.01, Enclosure G, Table G-3, “Net Centric Assessment Criteria.”](#) to ensure services and data products delivered by the acquisition align with the Department’s objectives for net-centricity.
- Prepare and submit the Information Support Plan for final Stage 2 Review. (See [section 7.3.6](#) for details.)
- Address all information exchange requirements as part of the Information Support Plan Interoperability Requirements Certification and the Information Technology and National Security Systems Interoperability Certification processes.

7.2.3.4. After Milestone C and the Full-Rate Production Decision Review,

- Continue life-cycle compliance with the [Information Support Plan Interoperability Requirements Certification](#) and the Information Technology and National Security System Interoperability Certification.
- Continue life-cycle compliance with Information Assurance Certification and Accreditation.

7.2.4. Global Information Grid (GIG) Architecture-Related Guidance

The following paragraphs describe the major sources of guidance and tools related to the GIG Architecture and supporting DoD strategies for implementing the architecture in Information Technology and National Security Systems programs. Program managers and Sponsors/Domain Owners should use the guidance, tools, and strategies outlined below throughout a program’s life-cycle to meet a variety of statutory and regulatory requirements.

7.2.4.1. DoD Architecture Framework (DoDAF)

The [DoDAF](#) provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions to ensure a common denominator for understanding, comparing, and integrating architectures. An integrated architecture consists of multiple views or perspectives (Operational View (OV), Systems View (SV), Technical Standards View (TV) and All View (AV)) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

- The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.
- The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.
- The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.
- The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture.

Typically the Combat Developer (or Domain Owner/Sponsor) will be responsible for the architecture description prior to Milestone B with the program manager taking on the responsibility subsequent to the approval at Milestone B.

(See <https://pais.osd.mil/enterprisearchitectures>)

7.2.4.2. DoD Information Technology (IT) Standards Registry (DISR)

The Joint Technical Architecture (JTA)—Version 6.0 is a minimal set of primarily commercial IT standards. These standards are used as the “building codes” for all systems being procured in the Department of Defense. Use of these building codes facilitates interoperability among systems and integration of new systems into the [Global Information Grid \(GIG\)](#). The Department of Defense is beginning to move the JTA 6.0 into a new capability, called the [DoD IT Standards Registry \(DISR\)](#). The JTA 6.0 will continue to be in effect until the DISR capability is fully established. Key net-centric elements that program architectures should focus on include:

- Internet Protocol – Ensure data packets are routed across network, not switched via dedicated circuits. Focus on establishing IP as the convergence layer.
- Secure and Available Communications – Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service. Focus is on Black (encrypted) Transport Layer to be established through the Transformational Communications Architecture implementation.
- Assured Sharing – trusted accessibility to net resources (data, services, applications, people, devices, collaborative environment, etc). Focus on assured access for authorized users and denied access for unauthorized users.
- Quality of Service – Data timeliness, accuracy, completeness, integrity, availability, and ease of use. This is envisioned as being measured through the [Net-Ready Key Performance Parameter](#). Focus on Service Level Agreements and service protocols with quality and performance metrics.

7.2.4.3. Core Architecture Data Model (CADM)

Provides a common approach for organizing and portraying the structure of architecture information, and is designed to capture common data requirements. The CADM facilitates the exchange, integration, and comparison of architecture information throughout the Department of Defense, improving joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance interoperability.

7.2.4.4. Global Information Grid (GIG) Capstone Requirements Document

The GIG Capstone Requirements Document provides the broad, overarching requirements for any system that will become a part of the GIG. In the Analysis of Alternatives, the Sponsor/Domain Owner or program managers should identify approaches to mitigate the inability to meet the GIG Capstone Requirements Document requirements, especially those that directly conflict with their program requirements, and identify any resulting impacts from not meeting such requirements.

7.2.4.5. DoD Net-Centric Data Strategy

The [Data Strategy](#) provides the basis for implementing and sharing data in a net-centric environment. It describes the requirements for inputting and sharing data, metadata, and forming dynamic communities to share data. Program managers and Sponsors/Domain Owners should comply with the explicit requirements and the intent of this strategy, which is to share data as widely and as rapidly as possible, consistent with security requirements. Additional requirements and details on implementing the DoD Data Strategy are found in [section 7.4](#). Specific architecture attributes associated with this strategy that should be demonstrated by the program manager include:

- Data Centric – Data separate from applications; applications talk to each other by posting data. Focus on metadata registered in DoD Metadata Repository.
- Only Handle Information Once – Data is posted by authoritative sources and made visible, available, and usable (including the ability to re-purpose) to accelerate decision-making. Focus on re-use of existing data repositories.
- Smart Pull (vice Smart Push) – Applications encourage discovery; users can pull data directly from the net or use value added discovery services. Focus on data sharing, with data stored in accessible shared space and advertised (tagged) for discovery.
- Post in Parallel – Process owners make their data available on the net as soon as it is created. Focus on data being tagged and posted before processing.
- Application (Community of Interest (COI) Service) Diversity – Users can pull multiple applications (COI Services) to access same data or choose same applications (Core and COI Services) for collaboration. Focus on applications (COI service) posting and tagging for discovery.

7.2.4.6. DoD Information Assurance (IA) Strategy

This Departmental strategy provides the focus, enduring goals, and strategic objectives for establishing assured information capabilities within the Department of Defense. These goals are the following:

- Goal 1: Protect Information – to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust commensurate with mission needs.
- Goal 2: Defend Systems & Networks – by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense.
- Goal 3: Provide IA Situational Awareness/Command and Control (C2) – integrate the IA posture into a User-Defined Operational Picture synchronized with NETOPS and emerging Joint C2 Common Operating Picture programs to provide decision makers and network operators at all command levels the tools for conducting IA/CND operation in Net-Centric Warfare.
- Goal 4: Transform and Enable IA Capabilities – innovatively by discovering emerging technologies, experimentation, and refining the development, delivery and deployment processes to improve cycle time, reduce risk exposure and increase return on investment.

- Goal 5: Create an IA Empowered Workforce – that is well equipped to support the changing demands of the IA/information technology enterprise.

7.2.4.7. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document (CDD)

The GIG ES CDD is currently focused on nine core enterprise services to be provided by the Net Centric Enterprise Services (NCES) Program. These services are the foundation for the initial net-centric capabilities to be provided by the Defense Information Systems Agency. The CDD describes the overall set of services in detail.

The NCES program will develop the core enterprise services incrementally. The NCES Program Plan describes the increments and their anticipated schedule. Each program that is dependent upon the core services being developed by the NCES program should address the impact of the incremental NCES schedule on their program. The Net-Centric Operations and Warfare Reference Model (NCOW RM) provides a basis for discussing issues associated with these core services. Table 1 shows the relationship of the nine Core Services articulated in the GIG ES CDD to the services articulated in the NCOW RM.

GIG ES CDD/NCES	NCOW RM Activity
Application	A316 (Provide Applications Services)
Collaboration	A312 (Provide Collaboration Services)
Discovery	A311 (Perform Discovery Services)
Enterprise Services Management/NetOps	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Information Assurance/ Security	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Mediation	A314 (Perform Information Mediation Services)
Messaging	A313 (Provide Messaging Services)
Storage	A315 (Perform Information Storage Services)
User Assistance	A2 (Perform User Agent Services)

Table 1. Mapping of Global Information Grid Enterprise Services/Net Centric Enterprise Services Core Services to Net-Centric Operations and Warfare Reference Model Services

7.2.5. Compliance with the Global Information Grid (GIG)

Compliance with the GIG means an information technology-based initiative or an acquisition program, throughout its lifecycle:

1. Meets the [DoD Architecture Framework \(DoDAF\)](#) requirements in producing architectural products. This requirement is met by producing a complete integrated architecture using the specified products described in the DoDAF and having it assessed for accuracy, consistency, and sufficiency with respect to its intended use (e.g., capability definition, process re-engineering, investment decisions, and integration engineering).
2. Meets the Core Architecture Data Model (CADM) requirements for using/reusing architecture data. This requirement is met through reuse of CADM data in a program's integrated architecture and through contributing new reusable architecture data (if any) to the CADM.
3. Meets the [Joint Technical Architecture \(JTA\) v6.0/DoD Information Technology Standards Registry \(DISR\)](#) requirements in selecting technologies and standards. This requirement is met by defining and implementing capabilities, based on technologies and standards contained within the JTA/DISR. Meeting this requirement should be validated at every milestone.
4. Meets the [DoD Net-Centric Data Strategy](#) requirements and intent. Make explicit the data that is produced and used by the program's implemented operations. Provide the associated metadata, and define and document the program's data models. This requirement is met by:
 - a. Describing the metadata that has been registered in the DoD Data Metadata Registry for each data asset used and for each data asset produced (i.e., data for which the program is the Source Data Authority).
 - b. Providing the documented data models associated with the program.
5. Explicitly addresses net-centricity and determine the program's net-centric correspondence to key net-centric criteria (e.g., concepts, processes, services, technologies, standards, and taxonomy). (See and follow the Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance Assessment Methodology (Draft) – [found](#) on the [GIG Architecture](#) website). An important aspect of this is the program's mapping of its operational, systems, and technical view content to the NCOW RM key net-centric criteria. This correspondence shall describe—in terms of the programs content—operational, systems, and technical view—what the program provides, what the program dependencies are, and what the program gaps are. The correspondence shall also provide additional information related to the NCOW RM and its emerging technologies and standards, and a transition roadmap (when gaps are identified). Additionally, the program shall provide an explicit evaluation of risk with respect to achieving net-centricity at each program milestone.
6. Meets the broad requirements set forth in the GIG Capstone Requirements Document. This requirement is met by describing the program elements that address each requirement and by expressing an overall degree of conformance to the GIG Capstone Requirements Document. Where conformance cannot be achieved, appropriate rationale and associated risks (near, mid, and/or long term) should be presented.

7.2.6. Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM)

The [NCOW RM](#) is focused on achieving net-centricity. Compliance with the NCOW RM translates to articulating how each program approaches and implements net-centric features. Compliance does not require separate documentation; rather, it requires that program managers and Sponsors/Domain Owners address, within existing architecture, analysis, and program architecture documentation, the issues identified by using the model, and further, that they make explicit the path to net-centricity the program is taking.

To this end, the material below will help program managers and Sponsors/Domain Owners in this articulation. It describes the features of net-centricity, key strategies in attaining net-centricity, and how to use the NCOW RM as a common basis for discussing program architectures and corresponding implementations with respect to these DoD net-centric strategies.

7.2.6.1. Features of Net-Centricity

Transforming to a net-centric environment requires satisfying four key features: *reach*, *richness*, *agility*, and *assurance*.

- *Reach* can be operationally defined in terms of space-time where “distance is not a factor,” but recognizing that the integration of spatially disconnected capabilities costs time (i.e., there is a minimum delivery time). Time is the dominant limitation in success!
- *Richness* can be operationally defined in terms of the total set of expertise, information, and/or capabilities that can be brought to bear, within a unit of time, to effect a decision or an action subsequent to a decision. Richness contributes to driving the margin of uncertainty in a decision or action downward.
- *Agility* can be operationally defined in terms of the number of effective adaptations that can be accomplished per unit of time. Thus, highly agile capabilities are those that can anticipate or react and successfully adapt to changes in the environment faster than less agile capabilities.
- *Assurance* can be operationally defined in terms of achieving expected levels of operational and systems performance within a specified context, including an adversarial force in a specified timeframe. Adversarial force (i.e., counters to assurance) is measured in terms of work-factors (time to accomplish a condition or effect) and probabilities (likelihood of occurrence). Note that this is a broad definition of assurance that includes the general concept of information assurance. Assurance should:
 - Provide the capability to deter an adversarial force.
 - Prevent adversarial force from succeeding within a specified time and/or detect an adversarial force when it is being applied in time to provide mitigating responses to counter such a force application.
 - Provide the capability to recover in a timely fashion from an adversarial force, given that the application of such a force has succeeded to some degree.

Assurance can be directly related to the time-value of mission operations. That is, the time-value related to mission might be assessed by the following types of questions:

- Can the mission succeed within the resources/unit time expected?
- Can mission performers respond to operational and systems failures, and still succeed within some time boundary?
- Can operational or system resources be reconstituted, upon catastrophic failure, in time to still enable mission success?

7.2.6.2. Key Strategies for Achieving Net-Centricity

The initial means for attaining these net-centric features include implementing the Net-Centric Enterprise Services (NCES), Net-Centric Data, and Information Assurance (IA) Strategies to share information rapidly and widely.

- The NCES Strategy focuses on achieving a set of Net-Centric Enterprise Core Services (NCES—being developed by Defense Information Systems Agency) that can be dynamically shared and used by everyone in conjunction with selectable sets of Community of Interest (COI) services to rapidly assemble information capabilities and integrate processes as needed. Core services may be developed within a program, when it is determined that the core services of the NCES Program cannot meet program needs and then made available to the Enterprise for reuse. COI services, as identified by a program, are expected to be developed and registered by every program that contributes to the evolution of the [Global Information Grid \(GIG\)](#). Environment Control services, as expressed in the Net-Centric Operations and Warfare Reference Model are expected to be provided through DoD GIG End-to-End IA Initiative and through other programs contributing to the GIG. Reuse of registered services is strongly encouraged. This service-oriented approach enables flexibility in reuse of service modules and a more loosely coupled infrastructure that can be adapted more readily to changing operational needs.
- The [Net-Centric Data Strategy](#) focuses on more rapid, widespread, and agile data sharing through the establishment of dynamic COIs, and includes concepts such as Only Handle Information Once; Task, Post, Process, and Use; and the use of descriptive metadata tagging.
- The IA Strategy (See DoD IA Strategy and [section 7.4](#) of this chapter) focuses on assuring information processing, transport, storage, and the dynamic sharing of information within and across DoD boundaries. Tagging is also central to the IA strategy.

7.2.6.3. How to Use the Net-Centric Operations and Warfare Reference Model (NCOW RM)

These strategies have been captured in the [NCOW RM](#) and program managers and sponsors/ domain owners can use the NCOW RM to help describe how they are implementing these strategies in their programs.

NCOW RM objectives include:

- Providing a model that guides the development of net-centric architectures throughout the Department.
- Supporting the identification, description, and evolution of enterprise information technology capabilities required for operating in the net-centric environment.

- Providing a model that can be used to support oversight and governance of [Global Information Grid \(GIG\)](#) net-centric transformation.

Conformance to the NCOW RM means that a program:

- Uses NCOW RM definitions and vocabulary
- Incorporates NCOW RM capabilities and services (or demonstrates equivalence) in its materiel solution, including those represented by the:
 - Net-Centric Enterprise Services Strategy
 - Net-Centric Data Strategy
 - Net-Centric Information Assurance Strategy
- Incorporates NCOW RM Information Technology and National Security Systems standards in the Technical View products developed for its materiel solution.

7.2.6.4. A Step-By-Step Approach

Compliance does not require separate documentation; rather, it requires that the Combat Developers, DoD Agencies, or program managers address, within existing architecture, analysis, and program documentation products, the issues identified by using the model and further they make explicit the path to net-centricity the program is taking. Using the model consists of the following steps:

1. Establishing the categorical positioning of the program with respect to the overall DoD enterprise. This is accomplished by articulating the domain decomposition in which the program exists by describing its domain and “portfolios of capabilities.”
 - For example, the Warfighter Domain may consist of Joint Command and Control (C2), Force Application, Force Protection, Focused Logistics, or Battlespace Awareness Sub-Domains.
 - If the program is associated with a platform (e.g., Joint Strike Fighter), it may belong primarily in the Force Application Sub-Domain, but have “portfolios of capabilities” in the Joint C2, Battlespace Awareness, and Force Protection Sub-Domains.
 - More specifically, the Joint Strike Fighter may have communication (e.g. TADIL, IP, etc) links that cover several Sub-Domains, it may have integrated test capabilities that support the Focused Logistics Sub-Domain, and it may have integrated avionics, navigation, targeting, and fire control that support the platform itself and its weapons, within Force Application Sub-Domain.

It is the program’s set of operational functions, activities, applications, services, and interface descriptions that are categorized into these portfolios that is of interest. These portfolios will be referenced in establishing the set of program-provided “Community of Interest (COI) Services” with respect to the Net-Centric Operations and Warfare Reference Model (NCOW RM).

2. Determining the program architecture’s degree of NCOW RM correspondence by activity mapping. This requires orientation of the program’s architecture to the NCOW RM activity decomposition. (Note – Additional guidance and specific

examples of mapping to cover services/systems or technical views will be provided in the next release of the DoD Acquisition Guidebook.)

- The landmark for activity mapping orientation is the NCOW RM COI Services and more specifically, the categorical portfolios established in step one, (e.g., Domain--Warfighter, Business, Intelligence, Enterprise Management, and/or Enterprise Information Management) are placed within the A321 or A322 blocks of COI Services. Examples (for illustration only) might include:
 1. A321 - Warfighter: Joint Future Combat System: (JTF) Engagement Execution Control.
 2. A321 - Warfighter: Army Future Combat System: (Unit of Action) Tactical Execution Control.
 3. A321 - Business: BEA: Provide Educational Benefits: Application for Benefits.
 4. A321 - Business: BEA: Provide Educational Benefits: Determine Eligibility.
 5. A322 - Modeling & Simulation: Warfighter Joint: Theater Engagement Modeling.
 6. A322 - Training: Enterprise Information Environment Management: NetOps: Global (Tier 1) Joint: Assess Threats: CND Watch Officer.
- Mapping Correspondence to NCOW RM. By placing the program's operational activity model (i.e., its portfolio of COI Services) into the NCOW RM 's COI Services, a PM can map the program's "similarity" and/or identify the specific use of NCOW RM Activities (e.g., Core Services and Environmental Control Services).
 1. COI Services export to the User Interaction Activity a set of Capability Interfaces (i.e., the program's user interactions). These are specializations of the generic capabilities identified in the NCOW RM User Interaction Activity. A program may have both specialized and generic interfaces, but is not expected to have just the NCOW RM generic interfaces.
 2. If the program utilizes the concept of a User Assistant, it will map to it. If not, it will indicate that it is currently not applicable (i.e. a potential future gap).
 3. If the program is dependent upon Net-Centric Enterprise Services (NCES) for its Core Services, it should indicate that fact and detail any issues associated with incremental deployment of the DoD's NCES program. If it is providing its own set of core services, it should describe the correspondence of their core service set to the NCOW RM Core Services.

4. The program must map its policies and controls to the Environment Control Services. That is, all program policies associated with implementing and integrating Enterprise Information Environment control must be made explicit. Enforcement issues (e.g., where and/or how a policy is to be enforced) should be raised, especially if enforcement is dependent upon other Global Information Grid (GIG) participants. These policies might be needed within the program to ensure a specific quality of service, a specified condition of maintaining confidentiality while sharing information, or the least privilege aspects of a given role being instantiated through the program. The controls might identify specific parameters and mechanisms that the program will need to enable and enforce such policies. For example, the adaptive encryption controls within a software-based radio may provide for the needed confidentiality in using shared space.
5. The program must identify the computing, communications, and storage resources it will use, especially those to provide a wider sharing of information. Policies associated with use dynamics and resource allocation must be made explicit. The physical resources (e.g., computing, communications, and storage) the program is providing must be identified with explicit sharing policies.
6. The program must address its approach to managing its information environment and how that approach integrates with the overall approach for managing the GIG (e.g., NetOps). The Manage Enterprise Information Environment Activity represents a set of services associated with Enterprise Information Environment (EIE) Management and Operations. Each program must articulate its local, regional, and global EIE management aspects, identifying what it provides and what it is dependent upon.
7. Finally, the program mapping must show (a) what activities the program depends upon from the GIG (e.g., [GIG Enterprise Services](#)); (b) what activities the program provides to the GIG (e.g., new control policies, new control mechanisms, new services); and (c) activity gaps—where the source of fulfilling the program requirement cannot be readily identified (e.g., Identity Management), or a required component will not be readily available when needed (e.g., tactical-level core services).
 - A capabilities roadmap should be derived from this mapping. This roadmap should be part of the Capability Development Document.
 - Service-Level Agreements should be established and incorporated into the Capability Production Document.
 1. A service-level agreement should be made with each provider of a supporting capability to assure accountability for each external dependency. The Capability Production Document should address these agreements.

2. A service-level agreement should be made with each program consumer of a supported capability to assure accountability for each dependency upon the program. The Capability Production Document should address these agreements.
 - The Program Manager should address the risk of not achieving the net-centric strategies represented in the Reference Model and gap mitigation in the [Analysis of Alternatives](#), and in the Initial Capabilities Document, Capability Development Document, and Capability Production Document.
3. Identifying information producer and consumer relationships that the program serves (e.g., those that are currently known and those for which data may be re-purposed). Specifically identify all producer/consumer relationships that originate external to the GIG (e.g., allies, coalition partners, commercial business, and other Federal Government). These relationships are part of the integrated architecture and should be addressed in the Capability Development Document.
4. Identifying the requirement for close-coupled relationships and those relationships that can be more loosely coupled. Address in the Capability Development Document.
5. Identifying the metadata for all data assets created in the program's implemented operations and aligning those assets with similar data assets within the program's domain(s). These data assets must be registered in the [DoD Metadata Repository](#) in accordance with the DoD Data Strategy.
6. Identifying the data assets to be used or consumed in the program's implemented operations and ensuring that such assets have been identified with metadata and that this metadata is registered in the DoD Metadata Repository in accordance with the DoD Data Strategy.
7. Identifying all policy needs of the program that must be incorporated or accommodated by the Environment Control Services (e.g., authentication, authorization, fault-tolerance, continuity of operations, qualities of service). These are both policy-enabling activities and policy enforcing activities. Policy, and its associated parameters, should be made explicit and not left implicit. Identify the differences between enterprise-level policies and program-level policies. This should be addressed in the Capability Development Document and in the integrated architecture.
8. Identifying the emerging technologies and standards that will (might) be used in the program's implementation. This should be addressed in the Capability Development Document and in the integrated architecture. In this identification, both the utility expected and the risks to be mitigated should be addressed. Planned upgrades and migration strategies should be addressed in the Capability Development Document.

7.2.7. Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance Assessment Methodology

Compliance evaluation, or assessment, will be performed by inspection and analysis of a program's documentation against specific criteria related to the [NCOW RM](#). These criteria are

No Product Requirements															
DODI 5000.2															
No Product Requirements															
DODD 4630.5															
No Product Requirements															
DODI 4630.8															
ISP	X	1	X	X		X	X	X	X		X	X	X		X
ISP NR-KPP	X			X		X	X	X			X	X	X		X
CJCSI 3170.01															
No Product Requirements															
CJCSM 3170.01															
ICD			X												
CDD	X			X		X	X	X			X	X	X		2
CPD	X			X		X	X	X			X	X	X		3
CRD			4		4		4								
CJCSI 6212.01															
ICD			X												
CDD NR-KPP	X			X		X	X	X			X	X	X		X
CPD NR-KPP	X			X		X	X	X			X	X	X		X
CRD (I-KPP)			4		4										
CRD (NR-KPP)			4				4								
DODAF															
Integrated Architecture	X	X		X	X		X		X						X

Table 2. Policy-Based Architecture Product Requirements

Legend:

X – Required Architecture Product

1 – Acronym List

2 – Draft Information Technology (IT) Standards Profile generated by DoD IT Standards Registry (DISR)

3 – Final IT Standards Profile generated by DoD IT Standards Registry (DISR)

4 – Required for legacy Capstone Requirements Documents and Capstone Requirements Document updates directed by the Joint Requirements Oversight Council.

Policy-based Products:

- [DoD Directive 5000.1](#), [DoD Instruction 5000.2](#), [DoD Directive 4630.5](#), and [CJCSI 3170.01](#) do not show requirements for architecture products.
- [DoD Instruction 4630.8](#)
- ISP – Information Support Plan (Replaces C4I Support Plan - C4ISP)
- NR-KPP – [Net-Ready Key Performance Parameter](#)
- ISP NR-KPP – NR-KPP for an ISP
- ICD – Initial Capabilities Document

- CDD – Capability Development Document
- CPD – Capability Production Document
- CRD – Capstone Requirements Document
- CDD NR-KPP – NR-KPP for a CDD
- CPD NR-KPP – NR-KPP for a CPD
- CRD (I-KPP) – CRD based on an Interoperability KPP
- CRD (NR-KPP) – CRD based on a NR-KPP
- Policy References do not show requirements for OV-6b, OV-6a, OV-7, SV-3, SV-7, SV-8, SV-9, SV-10a, SV-10b, SV-11, or TV-2.

7.2.9. DoD Chief Information Officer (CIO) Use of the Global Information Grid (GIG) Architecture

The DoD CIO uses the [GIG Architecture](#) in all three of the major decision processes of the Department (see [Chapter 1](#)).

The DoD CIO uses the GIG architecture throughout the processes included in operating the Joint Capabilities Integration and Development System to:

- Advise the Joint Requirements Oversight Council.
- Provide the basis for the development and refinement of joint integrated architectures by the Joint Staff and other DoD Components in support of the JCIDS.
- Develop assessments and provide recommendations to the JROC; the GIG Architecture, including its concepts, products, data, conclusions, and implications provides a key source for these assessments.

The DoD CIO uses the GIG architecture throughout the Planning, Programming, Budgeting, and Execution process to:

- Review and provide recommendations for development of the Strategic Planning Guidance and the Joint Programming Guidance.
- Provide recommendations to the Senior Level Review Group relating to Information Technology, National Security Systems, interoperability, and information assurance.
- Review and evaluate Program Change Proposals and Budget Change Proposals relating to Information Technology, National Security Systems, interoperability, and information assurance.
- Provide recommendations for Program Objective Memorandum planning and programming advice.

Finally, the DoD CIO uses the GIG Architecture throughout the Defense Acquisition Process to:

- Provide the basis for clear and comprehensive guidance in Information Technology Acquisition Decision Memoranda.
- Form and support his decisions and recommendations as a member of the Defense Acquisition Board, the lead for the Information Technology Acquisition Board, and the Milestone Decision Authority for Acquisition Category IA programs.

- Identify and specify Information Technology and National Security Systems implications associated with systems acquisition.
- Assess interoperability and supportability during the Overarching Integrated Product Team process.
- Review Information Support Plans and evaluate the interoperability, interoperability key performance parameters, and information assurance aspects of those plans.

7.2.10. Net-Centric Attributes

A checklist, available from ASD(NII), is being developed to address net-centric attributes and net-centric capabilities. Combat Developers, DoD Agencies, and program managers can use this checklist as an additional net-centric assessment aid.

[Net-Centric Checklist](#)

[NCOW RM](#)

[NCOW RM Compliance Methodology v1.1](#)

Table 3 outlines the major characteristics of net-centricity. Combat Developers, DoD Agencies, and program managers should ensure acquisition programs adhere to the policies, standards, and design tenets outlined below. For a more detailed discussion, see [CJCS Instruction 6212.01, Enclosure E, Table E-2, “Net Centric Assessment Criteria and the NCOW RM”](#).

Title	Description	Metric	Source
Internet Protocol (IP)	Data packets routed across network, not switched via dedicated circuits	IP as the Convergence Layer Net-Centric Operations and Warfare Reference Model (NCOW RM), Technical View compliant with JTA v6.	NCOW RM, GIG Arch v2, IPv6 Memos (9 Jun 03 and 29 Sep 03), JTA Memo 23 Nov 03 , JTA v6.0
Secure and available communications	Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service	Black Transport Layer Transformational Communications Architecture (TCA) compliance; Technical View compliant with JTA v6.0/DISR	TCA; IA Component of Assured GIG Architecture; JTA Memo 23 Nov 03 , JTA v6.0
Only handle information once (OHIO)	Data posted by authoritative sources and visible, available, usable to accelerate decision making	Reuse of existing data repositories	Community of interest policy (TBD)
Post in parallel	Business process owners make their data available on the net as soon as it is created	Data tagged and posted before processing NCOW RM, Technical View compliant with JTA v6.0/DISR	NCOW RM, DoD Net-Centric Data Strategy (9 May 03) JTA Memo 23 Nov 03 , JTA v6.0
Smart pull (vice smart push)	Applications encourage discovery; users can pull data directly from the net or use value-added discovery services	Data stored in public space and advertised (tagged) for discovery NCOW RM, Technical View compliant with JTA v6.0/DISR	NCOW RM; DoD Net-Centric Data Strategy (9 May 03); JTA Memo 23 Nov 03 , JTA v6.0
Data centric	Data separate from applications; apps talk to each other by posting data	Metadata registered in DoD Metadata Registry NCOW RM, Technical View compliant with JTA v6.0/DISR	NCOW RM; DoD Net-Centric Data Strategy (9 May 03); JTA Memo 23 Nov 03 , JTA v6.0
Application diversity	Users can pull multiple apps to access same data or choose same app (e.g., for collaboration)	Apps posted to net and tagged for discovery NCOW RM, Technical View compliant with JTA v6.0/DISR	NCOW RM; JTA Memo 23 Nov 03 , JTA v6.0
Assured Sharing	Trusted accessibility to net resources (data, services, apps, people, collaborative environment, etc.)	Access assured for authorized users; denied for unauthorized users	Security/IA policy (TBD); IA Component of Assured GIG Architecture; JTA Memo 23 Nov 03 , JTA v6.0
Quality of service	Data timeliness, accuracy, completeness, integrity, and ease of use	Net-ready key performance parameter	Service level agreements (TBD); JTA Memo 23 Nov 03 , JTA v6.0

Table 3. Net-Centric Characteristics

7.3 INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

7.3.1. Interoperability and Supportability

Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and National Security Systems interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle, and it should be balanced with information assurance.

Supportability for Information Technology systems and National Security Systems is the ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capability(ies).

7.3.2. Mandatory Policies

[DoD Directive 4630.5, Interoperability and Supportability of Information Technology \(IT\) and National Security Systems \(NSS\)](#)

4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate.

4.3. IT and NSS interoperability and supportability needs, for a given capability, shall be identified through:

- The Defense Acquisition System (as defined in the DoD 5000 series issuances); <link>*
- the Joint Capabilities Integration and Development System (JCIDS) process; <link>*
- and the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) change recommendation process (see CJCSI 3180.01, Joint Requirements Oversight Council (JROC) Programmatic Processes For Joint Experimentation And Joint Resource Change Recommendations <link>).*

4.5. IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be

completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.

4.8. *Interoperability and supportability needs shall be balanced with requirements for Information Assurance (IA)*

DoD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

E3.1.5. *A Net-Ready Key Performance Parameter (NR-KPP), consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. A NR-KPP shall be defined for all IT and NSS defense acquisition and procurement programs and shall be specified to a level of detail that allows verification of interoperability throughout a system's life. The defined NR-KPP shall be developed in such a way that it can be reliably measured, tested and evaluated.*

E3.1.6. *IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an Information Support Plan (ISP). For all DoD Acquisition Category (ACAT) programs and non-ACAT acquisitions and procurements, an Information Support Plan (ISP) shall be produced and used to analyze interoperability and supportability requirements specified in the NR-KPP.*

Note: [Paragraph 7.3.6.7](#) of this guide provides detailed guidance on ISPs.

6.2.3.6.1. *All IT and NSS, regardless of ACAT, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC). IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions. Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.*

6.2.3.6.2. *IT and NSS interoperability testing can occur in multiple stages. Evolutionary acquisitions or procurements, and normal life-cycle modifications, result in a progressively more complete capability. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested and certified. However, all critical interfaces, identified in the NR-KPP, which have been tested, must be successfully certified for interoperability prior to fielding. When appropriate (e.g., between successful completion of operational testing and the fielding decision), the DISA (JITC) shall issue interim interoperability certification letters specifying which of the system's interoperability needs have been successfully met and which have not. The DISA (JITC) shall issue an overall system certification once the system successfully meets all requirements of the NR-KPP validated by the Chairman of the Joint Chiefs of Staff. The DISA (JITC) shall provide interoperability certification letters to the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the DOT&E the Chairman of*

the Joint Chiefs of Staff, and the Commander, USJFCOM, as well as to the OTA and program manager, as applicable.

6.2.3.7. Interoperability Reviews. *IT and NSS shall be subject to interoperability reviews over the life of a system to determine if interoperability objectives are being met. The Interoperability Senior Review Panel (ISRP) comprised of senior officers from the following DoD Organizations: the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DOT&E, the DPA&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM; reviews and assesses interoperability to identify IT and NSS interoperability deficiencies. Multiple sources may be used to identify IT and NSS interoperability deficiencies including JCIDS documents; ISPs; TEMPs and operational test plans; and observation of tests and exercises by the DOT&E and the OTAs, the USJFCOM interoperability priority list, the Joint Warfighting Capability Assessments, program management offices, the MCEB, the MIB, DISA, DoD Component interoperability testing organizations, and the Joint C4ISR Battle Center. Identified IT and NSS interoperability deficiencies may pertain to both the technical exchange of information and the end-to-end operational effectiveness of that exchange required for mission accomplishment.*

Note: The Interoperability Senior Review Panel maintains an Interoperability Watch List (IWL). DoD Instruction 4630.8, [paragraph 6.2.3.8.1](#), discusses procedures for placing programs with significant interoperability deficiencies on the IWL. Program managers should be aware of the process and the criteria for nominating programs to the IWL.

DoD Directive 5000.1, The Defense Acquisition System, Enclosure 1

Paragraph E1.10. Establishes the requirement to acquire systems and families of systems that are interoperable.

Paragraph E1.11. States the requirement that test and evaluation shall assess interoperability.

Paragraph E1.16. Cites interoperability as a primary reason for acquisition managers to consider and use performance-based strategies for acquiring and sustaining products and services.

DoD Instruction 5000.2, Operation of the Defense Acquisition System, Enclosure 5

Paragraph E5.4.9 states that “All DoD MDAPs, programs on the OSD T&E Oversight list, post-acquisition (legacy) systems, and all programs and systems that must interoperate, are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. For IT systems, including NSS, with interoperability requirements, the Joint Interoperability Test Command (JITC) shall provide system interoperability test certification memoranda to the Director, Joint Staff J-6, throughout the system life cycle and regardless of ACAT.”

Paragraph E5.5 states that “During Developmental Test and Evaluation (DT&E) the materiel developer shall:

E5.5.4. Assess technical progress and maturity against critical technical parameters, to include interoperability, documented in the TEMP.

E5.5.8. In the case of IT systems, including NSS, support the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Joint Interoperability Certification (JIC) process.”

CJCS Instruction 6212.01, Interoperability And Supportability Of Information Technology And National Security Systems provides implementing instructions and checklists to the DoD Directive 4630.5 and DoD Instruction 4630.8.

7.3.3. Interoperability and Supportability Integration into the Acquisition Life Cycle

Figure 1 is a chart from CJCS Instruction 6212.01 that depicts the relationship between key interoperability and supportability activities and the Joint Capabilities Integration and Development System and Defense Acquisition processes:

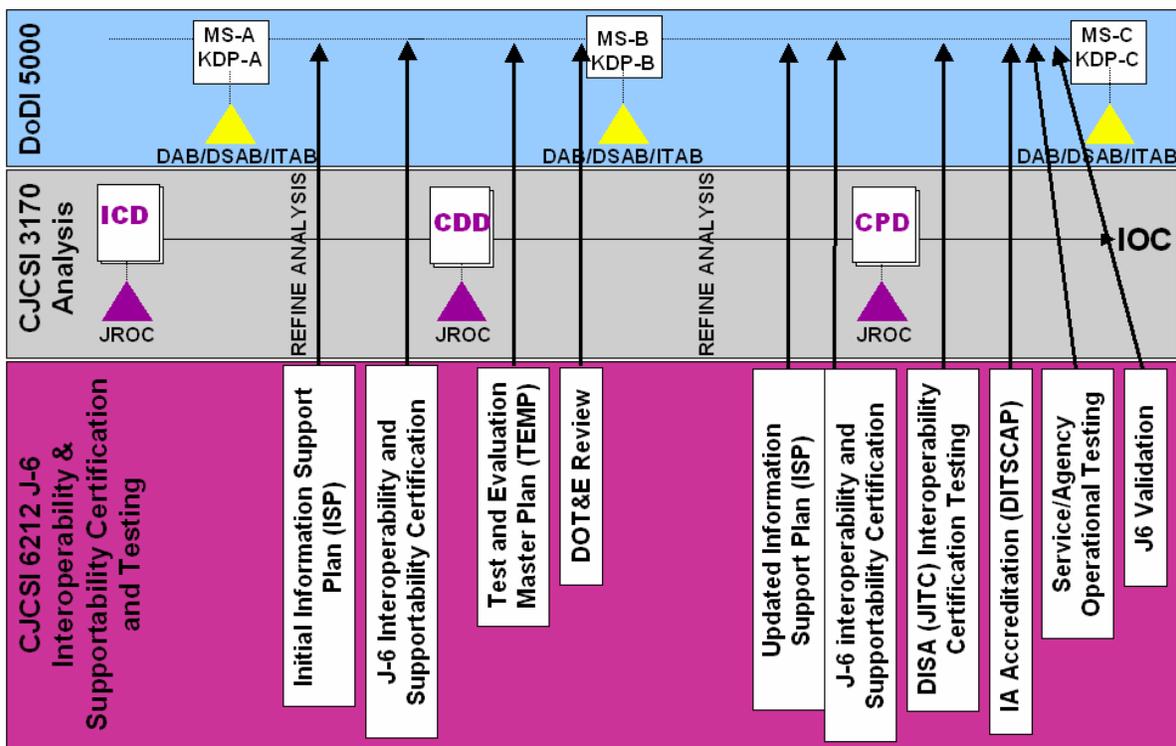


Figure 1. J-6 Interoperability and Supportability Certification, Testing and Validation Process for ACAT Programs

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

The NR-KPP has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving Information Technology (IT) and National Security Systems (NSS) interoperability and supportability. The NR-KPP assists Program Managers, the test community, and Milestone Decision Authorities in assessing and evaluating IT and NSS interoperability.

The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. Program managers will use the NR-KPP documented in Capability Development Documents and Capability Production Documents to analyze, identify, and describe IT and NSS interoperability needs in the Information Support Plan and in the test strategies in the Test and Evaluation Master Plan. The following elements comprise the NR-KPP:

- [Compliance with the Net-Centric Operations and Warfare Reference Model.](#)
- [Compliance with applicable Global Information Grid Key Interface Profiles.](#)
- [Compliance with DoD Information Assurance requirements.](#)
- [Supporting integrated architecture products.](#)

7.3.4.1. Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM)

The [NCOW RM](#), Figure 2, describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (i.e., core services, Community of Interest services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid are realized.

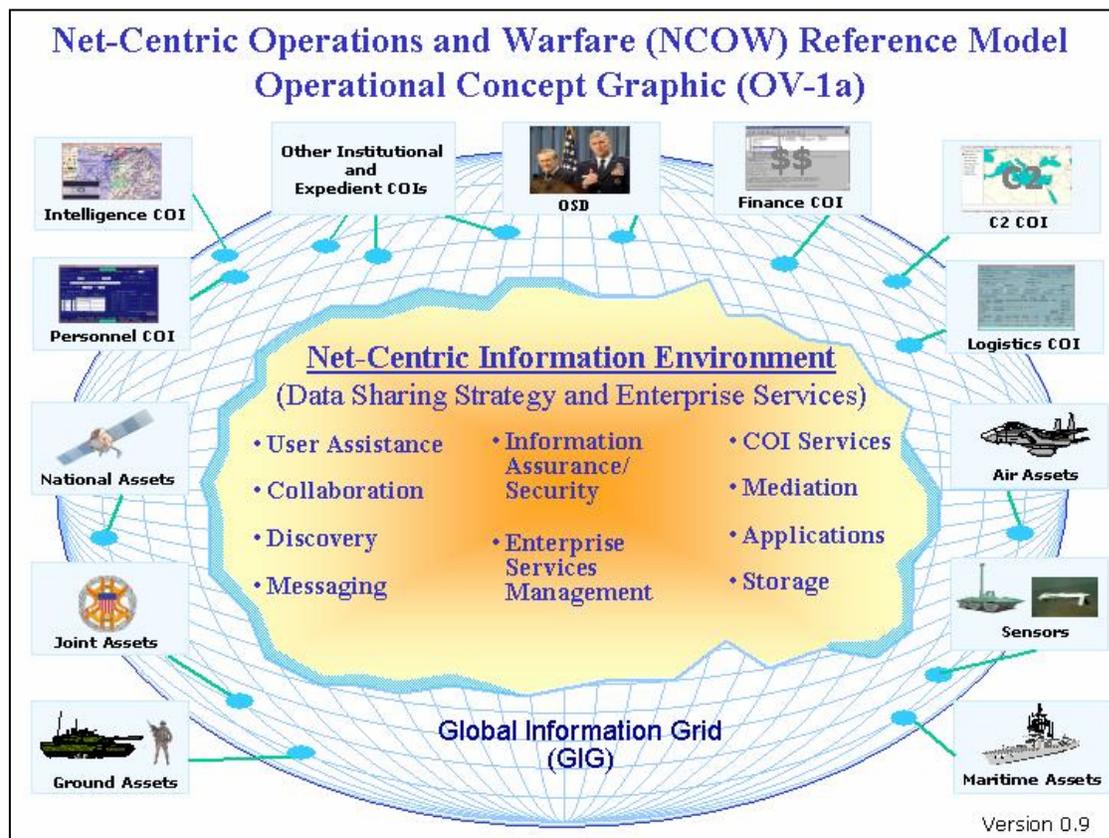


Figure 2. Depiction of the Net-Centric Operations and Warfare Reference Model (NCOW RM)

Program manager compliance with the NCOW RM is demonstrated through inspection and analysis of a capability's:

- Use of NCOW RM definitions and vocabulary;
- Incorporation of NCOW RM Operational View capabilities and services in the materiel solution;
- Incorporation of NCOW RM Technical View Information Technology and National Security Systems standards in the Technical View products developed for the materiel solution.

See [section 7.2.6](#) for a description of how program managers show compliance with the NCOW RM. In addition, [CJCS Instruction 3170.01](#) and [CJCS Instruction 6212.01](#) for detailed discussions of the inspection and analysis processes.

7.3.4.2. Compliance with Applicable Global Information Grid (GIG) Key Interface Profiles (KIPs)

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Refined Operational View <input checked="" type="checkbox"/> Refined System View <input checked="" type="checkbox"/> Interface Control Specifications -- Interface Control Document (ICD) <input checked="" type="checkbox"/> Technical View & SV-TV Bridge <input checked="" type="checkbox"/> Configuration Management Plan <input checked="" type="checkbox"/> Procedures for standards conformance and interoperability testing utilizing reference implementations <input checked="" type="checkbox"/> Engineering Management Plan 	<table border="1"> <thead> <tr> <th colspan="2"><i>Communications KIPs</i></th> </tr> </thead> <tbody> <tr><td>1.</td><td>Logical Networks to DISN Transport Backbone</td></tr> <tr><td>2.</td><td>Space to Terrestrial Interface</td></tr> <tr><td>3.</td><td>JTF to Coalition</td></tr> <tr><td>4.</td><td>JTF Component to JTF Headquarters</td></tr> <tr><td>5.</td><td>Teleport (i.e., deployed interface to DISN)</td></tr> <tr><td>6.</td><td>Joint Interconnection Service</td></tr> <tr><td>7.</td><td>DISN Service Delivery Node</td></tr> <tr><td>8.</td><td>Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)</td></tr> <tr><td colspan="2"><i>Computing KIPs</i></td></tr> <tr><td>9.</td><td>Application Server to Database Server</td></tr> <tr><td>10.</td><td>Client to Server</td></tr> <tr><td>11.</td><td>Applications to COE/CCP (NCES/GES)</td></tr> <tr><td colspan="2"><i>Network Operations KIPs</i></td></tr> <tr><td>12.</td><td>End System to PKI</td></tr> <tr><td>13.</td><td>Management Systems to (integrated) Management Systems</td></tr> <tr><td>14.</td><td>Management Systems to Managed Systems</td></tr> <tr><td>15.</td><td>IDM to Distribution Infrastructure</td></tr> <tr><td>16.</td><td>Information Servers to IDM Infrastructure</td></tr> <tr><td colspan="2"><i>Applications</i></td></tr> <tr><td>17.</td><td>Application Server to Shared Data - FIOP (SADI)</td></tr> </tbody> </table>	<i>Communications KIPs</i>		1.	Logical Networks to DISN Transport Backbone	2.	Space to Terrestrial Interface	3.	JTF to Coalition	4.	JTF Component to JTF Headquarters	5.	Teleport (i.e., deployed interface to DISN)	6.	Joint Interconnection Service	7.	DISN Service Delivery Node	8.	Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)	<i>Computing KIPs</i>		9.	Application Server to Database Server	10.	Client to Server	11.	Applications to COE/CCP (NCES/GES)	<i>Network Operations KIPs</i>		12.	End System to PKI	13.	Management Systems to (integrated) Management Systems	14.	Management Systems to Managed Systems	15.	IDM to Distribution Infrastructure	16.	Information Servers to IDM Infrastructure	<i>Applications</i>		17.	Application Server to Shared Data - FIOP (SADI)
<i>Communications KIPs</i>																																											
1.	Logical Networks to DISN Transport Backbone																																										
2.	Space to Terrestrial Interface																																										
3.	JTF to Coalition																																										
4.	JTF Component to JTF Headquarters																																										
5.	Teleport (i.e., deployed interface to DISN)																																										
6.	Joint Interconnection Service																																										
7.	DISN Service Delivery Node																																										
8.	Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)																																										
<i>Computing KIPs</i>																																											
9.	Application Server to Database Server																																										
10.	Client to Server																																										
11.	Applications to COE/CCP (NCES/GES)																																										
<i>Network Operations KIPs</i>																																											
12.	End System to PKI																																										
13.	Management Systems to (integrated) Management Systems																																										
14.	Management Systems to Managed Systems																																										
15.	IDM to Distribution Infrastructure																																										
16.	Information Servers to IDM Infrastructure																																										
<i>Applications</i>																																											
17.	Application Server to Shared Data - FIOP (SADI)																																										

Figure 3. GIG Key Interface Profiles (KIPs)

GIG KIPs, Figure 3, provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. A KIP is the set of documentation produced as a result of interface analysis which: designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Systems Engineering Plan, Configuration Management Plan, Technical Standards View (TV-1) with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant GIG KIPs, for a given capability, are documented in the Capability Development Document and Capability Production Document. Compliance with identified GIG KIPs are analyzed during the development of the Information Support Plan and Test and Evaluation Master Plan, and assessed during Defense Information Systems Agency (Joint Interoperability Test Command) joint interoperability certification testing. An interface is designated as a key interface when one or more the following criteria are met:

- The interface spans organizational boundaries.
- The interface is mission critical.
- The interface is difficult or complex to manage.
- There are capability, interoperability, or efficiency issues associated with the interface.
- The interface impacts multiple acquisition programs.

Program manager compliance with applicable GIG KIPs is demonstrated through inspection of Joint Capabilities Integration and Development System documentation and test plans, and during JITC interoperability certification testing (see CJCS Instruction 3170.01 <link> and [CJCS Instruction 6212.01](#) for detailed discussions of the process).

7.3.4.3. Compliance with DoD Information Assurance (IA) Requirements

Requirements for DoD information assurance certification and accreditation are specified in [DoD Directive 8500.1](#), [DoD Instruction 8500.2](#), [DoD Directive 5200.28](#), and [DoD Instruction 5200.40](#). Satisfaction of these requirements results in IA compliance verification of the capability with previously agreed to security requirements. See [section 7.5](#) for details.

Framework Product	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational nodes, operational activities performed at each node, connectivity and information exchange needlines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational Activities, relationships among activities, inputs and outputs. Overlays can show cost, performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing - traces actions in a scenario or sequence of events and specifies timing of events
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture

Table 4. Architecture Products Required to Assess Information Exchange and Use

7.3.4.4. Supporting Integrated Architecture Products

In accordance with the DoD 4630 Series, integrated architecture products defined in DoD Architecture Framework Version 2.0 (and described in Table 4 and Figure 4) shall be used to assess information exchange and use for a given capability. The functional proponent, domain owner, PSA, and Program Manager use the supporting integrated architecture products in developing the [Net-Ready Key Performance Parameter](#) and preparing the Information Support Plan.

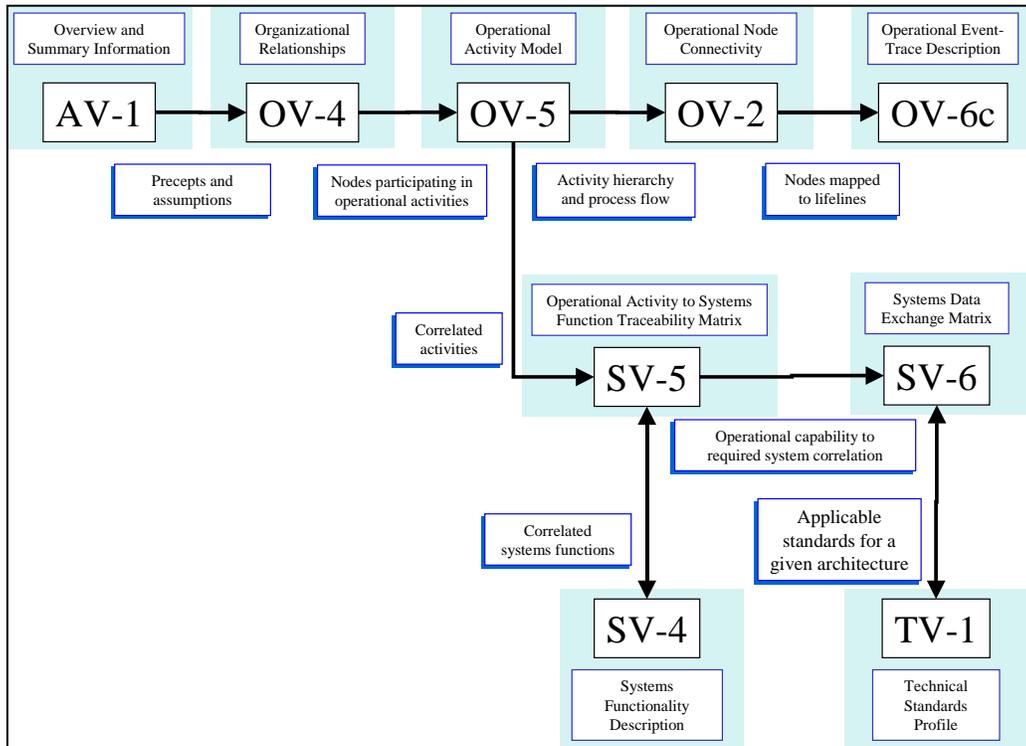


Figure 4. Supporting Integrated Architecture Products

7.3.4.5. Compliance with Integrated Architecture Products

Program manager compliance with required supporting integrated architecture products is demonstrated through inspection and analysis of developed architecture products to determine conformance with [DoD Architecture Framework](#) specifications, and that all required products have been produced. Detailed procedures are contained in [CJCS Instruction 3170.01](#) and [CJCS Instruction 6212.01](#).

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

The following checklist summarizes the requirements for demonstrating compliance with the NR-KPP and should be useful in preparing for milestone approvals:

7.3.5.1. Required Documentation

Does the capability have the following required documentation?

- AV-1, OV-2, OV-4, OV-5, OV-6c, SV-4, SV-5, SV-6
- DISR Standards Compliance with draft TV-1
- LISI Interconnectivity Profile
- NR-KPP Compliance Statement
- [NCOW-RM Compliance](#)
- IA Compliance Statement
- KIP Declaration List

7.3.5.2. Supporting Integrated Architecture Products

- Have all architecture products been developed in accordance with the [DoD Architecture Framework](#)?
- Does the AV-1 describe a net centric environment?
- Has the TV-1 been prepared using applicable information technology standards profiles contained in the DISR?
- Have all the interfaces listed in the OV-2 and SV-6 been appropriately labeled with the GIG core enterprise services needed to meet the requirements of the applicable capability integrated architecture?
- Have all the applicable OV-5 activities identified in the specific capability integrated architecture been appropriately described at each critical or enterprise level interface in terms of policy enforcement controls and data enterprise sharing activities in the NCOW-RM, Node Tree OV-5?
- Have specific capability integrated architecture OV-6c time event parameters been correlated with GIG architecture OV-6c?
- Have verifiable performance measures and associated metrics been developed using the integrated architectures, in particular, the SV-6?

7.3.5.3. Key Interface Profiles

- Have applicable Key Interface Profiles definitions been included as part of the KIP compliance declaration?
- Are the information technology standards for each applicable KIP technical view included in the draft TV-1 for the specific Joint integrated architecture?
- Are the appropriate KIP test procedures addressed as part of the requirement for interoperability system testing and certification?

7.3.5.4. Net-Centric Operations and Warfare Reference Model

- Have the activities listed in the applicable capability integrated architecture OV-5 been mapped to the [NCOW-RM](#) node tree OV-5 activities? Recommend that applicable capability integrated architecture OV-5 activities be characterized by use case diagrams grouped under the applicable [GIG Core Enterprise Services](#) (e.g., Discovery, Messaging, Mediation, Collaboration, etc.) to meet net-centric capabilities requirements for managing net-centric information environment.
- Have NCOW-RM OV-5 activities been used to identify requirements for data correctness, data availability, and data processing necessary for posting data/information elements within a specific joint integrated architecture?
- Has the SV-4 systems functionality been mapped to the applicable GIG Core Enterprise Services?
- Are the information technology standards in the NCOW-RM Target Technical View included in the Draft TV-1 for the applicable capability integrated architecture?

7.3.5.5. Information Assurance

- Have applicable [information assurance](#) requirements of [DoD 8500 Series](#) issuances and DCI Directives been identified for all GIG core enterprise services needed to meet the requirements of the specific joint integrated architecture?

- Has the applicable capability received IA certification and accreditation documentation from the appropriate Designated Approval Authority?

7.3.6. Information Support Plan (ISP)

The ISP (formerly called the Command, Control, Communication, Computers, and Intelligence Support Plan (C4ISP)) is intended to explore the information-related needs of an acquisition program in support of the operational and functional capabilities the program either delivers or contributes to. The ISP provides a mechanism to identify and resolve implementation issues related to an acquisition program's Information Technology (IT), including National Security Systems (NSS), infrastructure support and IT and NSS interface requirements. It identifies IT needs, dependencies, and interfaces for programs in all acquisition categories, focusing attention on interoperability, supportability, synchronization, sufficiency and net-centricity concerns. This provides the program manager a mechanism to identify his/her information-related dependencies, to manage these dependencies and to influence the evolution of supporting systems to meet the demands of the system as it evolves to meet the warfighter's needs. In the case where the supporting system will not be available, the ISP should provide the program manager with awareness of this problem in sufficient time to adjust the program in the most cost effective and operationally efficient manner.

The C4ISP has evolved into the ISP as a result of the revision of the CJCS Instruction 3170.01 requirements documentation. The architecture documentation previously captured in the C4ISP is now required in the Joint Capabilities Integration and Development System documents: Initial Capabilities Document, Capability Development Document, and Capability Production Document. The ISP will use the architecture documentation from the Joint Capabilities Integration and Development System documentation and focus on analysis.

7.3.6.1. Review of Information Support Plan (ISP)-Specific Mandatory Policies

- [DoD Instruction 5000.2, Enclosure 3, Regulatory Information Requirements, Table E3.T2](#) requires that all acquisition programs (except Defense Space Acquisition Board-governed programs as noted below), regardless of acquisition category level, submit an ISP at Milestones B and C, and at Program Initiation for ships.
- [National Security Space Acquisition Policy, Number 03-01](#), requires Defense Space Acquisition Board-governed programs to submit an ISP.
- [DoD Instruction 4630.8, Enclosure 4](#) provides a mandatory ISP format.
- [CJCS Instruction 6212.01](#) also provides detailed implementing guidance regarding the ISP format.

7.3.6.2. ISP Integration into the Acquisition Life cycle

A completed ISP answers the following seven questions for information needed to support the operational/functional capability(ies).

- **What information** is needed?
- **How good** must the information be?
- **How much** information? (needed or provided)
- **How** will the information be **obtained** (or provided)?
- **How quickly** must it be received in order to be useful?

- Is the information implementation **net-centric**?
- **Does it comply** with DoD information policies?

The following paragraphs describe the ISP-related actions that program managers should take in each acquisition phase.

Before Milestone A

- While the ISP is not required until Milestone B, early development of the ISP will assist in development of the program's integrated architecture and Concept for Operations required by the [CJCS Instruction 3170.01](#).

Before Milestone B (or program initiation for ships)

- Define all information related-dependencies according to [DoD Instruction 4630.8](#), [CJCS Instruction 6212.01](#), [CJCS Instruction 3170.01](#), and [CJCS Manual 3170.01](#) to ensure information supportability is addressed in the ISP and Capabilities Development Document
- Submit the ISP for formal, coordinated Stage I and Stage II reviews according to [DoD Instruction 4630.8](#) and [CJCS Instruction 6212.01](#). Submit a final, Stage III, version of the ISP for retention in the OASD(NII) Joint C4I Program Assessment Tool (JCPAT) repository. [Click here for ISP examples/samples web sites](#).

Before Milestone C

- Update all information related-dependencies according to [DoD Instruction 4630.8](#), [CJCS Instruction 6212.01](#), [CJCS Instruction 3170.01](#), and [CJCS Manual 3170.01](#) to ensure information supportability is addressed in the ISP and Capabilities Production Document.
- Submit the updated ISP for formal coordinated Stage I and Stage II reviews according to [DoD Instruction 4630.8](#) and [CJCS Instruction 6212.01](#). Submit a final, Stage III version of the ISP for retention in the OASD(NII) Joint C4I Program Assessment Tool (JCPAT) repository. [Click here for ISP examples/samples web sites](#).

After Milestone C

- Submit an updated ISP for each major upgrade (e.g., block or increment)

7.3.6.3. Estimated Preparation Lead Time

Based on past experience with C4ISPs, for a small program with few interfaces, it takes about 6 months to get an ISP ready for a Stage I review. For most programs, ISP preparation for Stage 1 review takes about a year. For very complex programs, like a major combatant ship, it can take between 18 to 24 months. The process is based on development or existence of an architecture.

7.3.6.4. OSD Review

The Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD (NII)) reviews all ISP documents for ACAT I and IA programs, and for other programs in which OASD(NII) has indicated a special interest.

This review is performed on the C4ISP Assessment Tool in the Joint C4I Program Assessment Tool (JCPAT) suite. The JCPAT suite provides paperless, web-based support for

ISP document submission, assessor review and comment submission, collaborative workspace, and consolidated review comment rollup.

The DISA JCPAT functional analyst is available to assist users with JCPAT functionality and to establish user accounts. A repository of previous C4ISP and current ISP documents is available for viewing in the JCPAT document repository.

7.3.6.5. Example/Sample Web Links

Program managers and other stakeholders will find the links in Table 5 useful in ISP preparation, program analysis, and oversight.

Web Site	NIPRNET	SIPRNET
DSC's C4ISPlan	http://www.dsc.osd.mil	www.dsc.osd.smil.mil/index.html
DISA's JCPAT	http://jcpat.ncr.disa.mil	jcpat.ncr.disa.smil.mil
NII's JMAAT	Not applicable	147.254.161.70/pai/index.htm
Defense Architecture Repository	https://pais.osd.mil/enterprisearchitectures	Not applicable

Table 5. Example/Sample Web Links

7.3.6.6. Points of Contacts

7.3.6.7. Information Support Plan (ISP) Chapter Instructions (13-Step Process for ISP Chapter 2)

The following provides instruction on how to complete each chapter and appendix in the ISP. It contains additional, discretionary guidance beyond that contained in [DoD Instruction 4630.8](#) and [CJCS Instruction 6212.01](#).

ISP Chapter 1. Introduction

- Summarize the program's operational scope.
 - Summarize the program's relationships to relevant Joint Operating Concepts (JOCs) and/or Joint Functional Concepts (JFC).
 - Concepts (JFCs) (e.g., focused logistics), as described in the program's Joint Capabilities Integration and Development System (JCIDS) documents. Provide an OV-1 (High-Level Operational Concept Graphic) for the basic program and descriptive text. For programs not covered by JCIDS, analogous documentation may be used.
- Summarize the program's relationship to other programs.
 - Provide a graphic that shows the major elements/subsystems that make up the system being acquired, and how they fit together (Provide an Internal SV-1 (System Interface Description)/(e.g., a system block diagram)).

- Analyze threat-specific information that will play a role in capability development, design, testing and operation. This information should be obtained from the appropriate Joint Capabilities Integration and Development System (JCIDS) documents. Information Operations (IO) threats should be analyzed using the Information Operations Capstone Threat Capabilities Assessment, DI-1577-12-03, August 2003 [<link>](#). This is the most comprehensive source available for IO-related threat information.
- For a weapon system, briefly describe the purpose, design objectives, warhead characteristics, sensors, guidance and control concept (as appropriate), command and control environment, general performance envelope, and primary Information Technology (IT), including National Security Systems (NSS) interfaces.
- For a command and control system, describe the system's function, dependencies and interfaces with other IT and NSS systems.
- For an Automated Information System (AIS), describe the system's function, its mission criticality/essentiality, dependencies, interfaces with other IT and NSS systems and primary databases supported.
- Program Data.

Provide the following program data in order to help the reviewer understand the level of detail to be expected in the ISP:

- Program contact information (program manager, address, telephone, email address, and ISP point of contact).
- Program acquisition category: ACAT.
- List Milestone Decision Authority: Defense Acquisition Board, Defense Space Acquisition Board, Information Technology Acquisition Board (or component MDA) or other.
- Milestone covered by the specific ISP.
- Projected milestone date.

ISP Chapter 2. Analysis

Analysis of the qualitative and quantitative sufficiency of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) support (e.g., hardware, software, processes, etc.) should be accomplished in terms of the operational/functional capabilities that are being enabled.

This analysis requires the following:

- An understanding of the operational/functional capabilities and the metrics that define whether they are being performed adequately.
- An understanding of what enabling functional capabilities must be performed in order to achieve a higher-level capability (C4ISR functions will almost always be enabling capabilities).
- An understanding of which players (nodes) will direct or perform the missions associated with delivering the capabilities.
- An understanding of DoD Information Policies.
- The information-needs discovery process:

For most systems, the following steps provide an information-needs discovery process that can be used to analyze the system under development. However, other approaches for discovering information needs that apply to the intelligence information needs discovery process are:

- Using the stages of the intelligence cycle (collection, exploitation, dissemination, etc.).
- Life-cycle stages (Concept Refinement, Technology Development, System Development and Demonstration, etc.).

The following steps (and notes) are based on using the Integrated Architecture developed in accordance with the DoD Architectural Framework, during the Joint Capabilities Integration and Development System (JCIDS) process. Click here for Global Information Grid (GIG) details.

Step 1: Identify the warfighting missions and/or business functions within the enterprise business domains that will be accomplished/enabled by the system being procured.

Note: Joint Warfighting missions can be found in [Joint Publication 3.0](#). Click here for [Operation, Series 3-0 publications](#).

Note: AIS programs should consult the DoD Comptroller's [Business Management Modernization Program](#) enterprise integrated architectures for each domain. Click here for BMMP details.

Step 2: Identify information needed to enable operational/functional capabilities for each warfighting mission identified in Step 1 by performing functional capability decomposition.

Note: If a Command and Control capability is the top-level driver of the function breakdown, then the OV-4 (Command Relationships) will be a necessary product to help define the functional capabilities needed. The OV-4 will likely require several OV-5 (Activity Model) functional breakdowns to enable each of the command elements identified.

Note: The architecture product most useful in managing the discovery of enabling/enabled capability relationships for each operational/functional capability is the OV-5 (Operational Activity Model). The OV-5 can be used to show the subordinate capabilities that are necessary to achieve a higher-level operational or functional capability. Notice that the OV-5 focuses on “what” rather than “how.” See Example Capability Breakdown, Figure 5.

This example illustrates specific items to consider for a weapon system that can be used to get the flavor of what is expected in step 2 for a program/system.

Step 2 Example: Clear Mines from Littoral Area

A. Clear mines from littoral area (*Operational Capability*)

Note: *Quality measures must be assigned in order to assess the acceptability of the operational and enabling capabilities/systems*

1. Plan the clearance effort (1st level enabling capability)

a. Obtain necessary intelligence information (*2nd level enabling capability*)

- 1) Navigation Information (charts, tides and currents, etc)
- 2) Enemy maritime mining capability (*3rd level capabilities*)
- 3) Weather information
- 4) Enemy coastal defense capability

b. Collaborate with off board nodes (*2nd level enabling capability*)

Insert 3rdrd and succeeding levels of enabling capability

2. Search for/locate the mines

Insert 2nd and succeeding levels of supporting capability

3. Disable/remove/destroy the mine

Insert 2nd and succeeding levels of supporting capability

4. Share the results of the clearance effort

Insert 2nd and succeeding levels of supporting capability

5. Receive logistic support.

Insert 2nd and succeeding levels of supporting capability

Figure 5. Example Capability Breakdown

Note: The specific form of this information should capture key information from an OV-5 (Operational Activity Model) and/or other information source (e.g., an outline or hierarchical graph). The important point is that the capability relationships are understood and attributes are identified so that assessments can be made.

Note: Specific items to consider:

- For satellite systems include: (e.g. Satellite control)
- For communication systems include: (e.g. Net-management)
- For business process systems include: (e.g. information contained in databases, other information sources)
- For weapons systems include: (e.g. Collection Management Support, Threat or signature support, targeting support, Intelligence Preparation of the Battlefield)
- For sensor systems include: (e.g. Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield, and Remote Operations)

- For platforms consisting of a mix of the above include: (e.g., Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield)

Step 3: Determine the operational users and notional suppliers of the information needed.

Step 3.a: Provide an OV-2 to identify the operational nodes and elements that drive the communications needed to enable the functional capabilities. For large platforms/systems, this effort should identify the major operational nodes (information drivers) within the platform, as well as nodes that are external to the platform/system with which information will be shared.

Step 3a Example: Clear Mines from Littoral Area

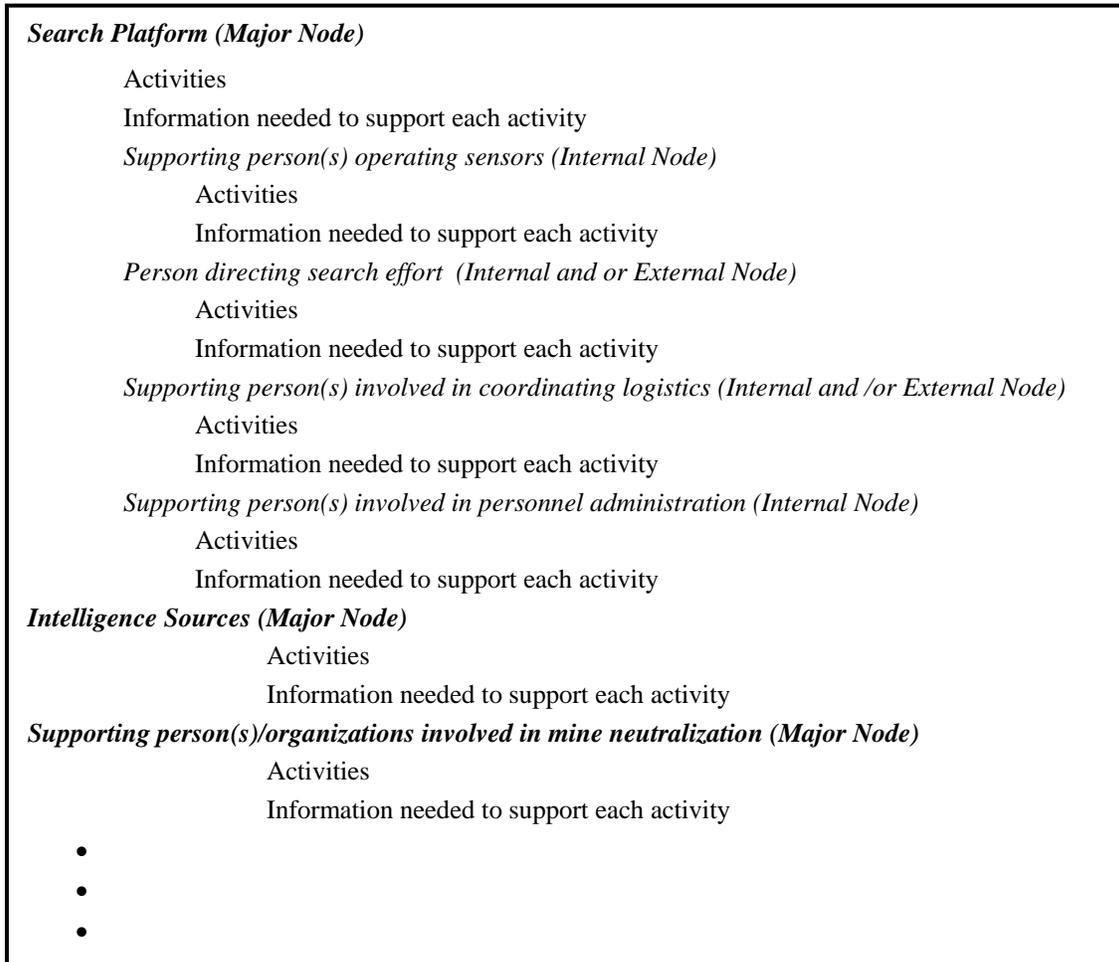


Figure 6. Example OV-2 Nodes For Mine Clearance

Step 3.b: Map these nodes (internal and external systems and people) and their activities to the functions identified in OV-5

Step 4: Establish the quality of the data needed to enable the functions identified in OV-5 and performed by the operational nodes in OV-2 (Operational Node Connectivity)

Note: Establish performance measures and determine the level of satisfaction necessary to make the information useful. (Examples: decimal precision for numerical data, NIIRS for imagery, annotated versus raw data, etc)

Note: When radio and other information transport systems are identified as providing support, establish transmission quality parameters and then assess whether the programs/systems intended to be used can meet these criteria.

Note: A factor in determining quality is the user (person or sub-system) (i.e. specifically how does the user intend to use the information).

Step 5: Determine if timeliness criteria exist for the information.

Note: To help establish timeliness, use OV-6C (Operational Event Trace Diagram) to establish event sequence. Considerations include:

- Order of arrival of information to enable transaction process(es) (for weapon systems)
Latency of data due to speed of flight issues
- Currency of data in databases to support operations

Step 6: Determine/Estimate the quantity of information of each type that is needed.

Factors influencing quantity include:

- Frequency of request or transmittal.
- Size of the information requested. (packet size, image size, file size etc.)
- Whether data is individual items or a data stream that is provided for a period of time.
- Whether data transmission is “bursty” or continuous over some period of time.
- Whether data transmission is random or occurs at some predictable interval
- The anticipate spectrum of employment (e.g. Military Operations Other than War or Major Theater of War)

Note: Ultimately this analysis should help estimate the bandwidth needs and should provide an assessment as to whether adequate bandwidth is available. If bandwidth is limited, what actions can be taken to reduce demand or use the bandwidth more efficiently?

Step 7: Discuss the way information will be accessed or discovered.

If data links are involved, identify them and also the message sets that will be implemented.

If a web-based ([Global Information Grid \(GIG\) compliant](#)) means of searching for and retrieving posted data is to be used, describe the approach.

- Data stores must exist for your program.
- The type of searching capability needed

Note: In many cases, this discussion will involve multiple levels of enabling systems. For example, maybe the enabling system is a Global Command and Control System (GCCS) application. GCCS rides on the SIPRNET. So both levels of this support should be discussed.

Step 8. Assess the ability of supporting systems to supply the necessary information.

Note: Supporting systems include collection platforms, databases, real time reports, messages, networked data repositories, annotated imagery, etc.

- Assess the ability to collect, store, and tag (to enable discovery and retrieval) the information

- Assess the ability of networks to provide a means to find and retrieve the necessary data.
- Assess the ability of the information transport systems to move the volume of data needed.
- Assess synchronization in time (i.e., years relative to other system milestones) with supporting programs.
- Whether the information will cross security domains.

Note: If systems will in any way tie into the intel Top Secret (TS)/ Sensitive Compartmented Information (SCI) network (JWICS) or utilize TS/SCI info, they will have to comply with Director, Central Intelligence Directives (DCID): DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, June 1999 and [DCID 6/9](#), Physical Security Standards for Sensitive Compartmented Information Facilities, 18 November 2002.

Note: The number of levels of analysis will depend on the detail required to identify the critical characteristics of the information needed to support the program. This should be accomplished for all phases of the acquisition life cycle.

Note: It is anticipated that the other communities such as the intelligence community may have to assist in the determination and analysis of these information needs.

Note: The format in Figure 7 is suggested for capturing the results of the supportability/synchronization assessment:

Step 8 Example: Summary of Synchronization Data

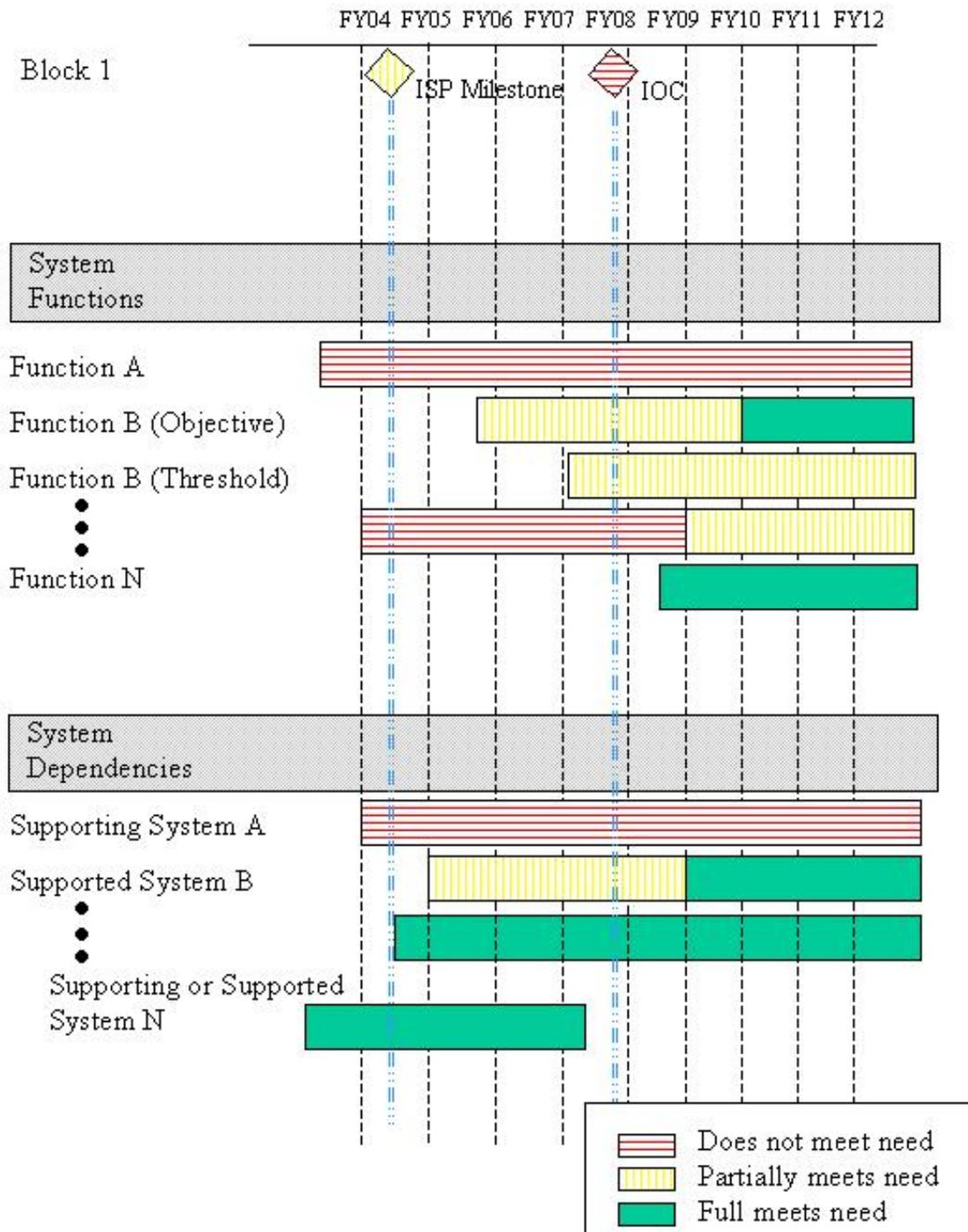


Figure 7. Sample Dependency and Information Needs Analysis Summary

Step 9: Assess Radio Frequency (RF) Spectrum needs. [Click here for Spectrum details.](#)

Note: [DoD Directive 4650.1](#) establishes spectrum management policy within the Department of Defense. ([DoD Instruction 4630.8](#) and [CJCS Instruction 6212.01](#) require Spectrum Supportability (e.g., spectrum certification, reasonable assurance of the availability of operational frequencies, and consideration of E3) to be addressed in the ISP. The Services have additional spectrum management policies and procedures.

To support the [Spectrum Supportability process](#), the ISP should document the following:

- Requirements for use of the electromagnetic spectrum including requirements for wide bandwidths
- Description of the intended operational Electromagnetic Environment (Allows for realistic test and evaluation).
- Impact of the loss of a planned spectrum-dependent command, control, or communication link as a result of an unresolved spectrum supportability issue. (To be identified in the issue section of the ISP)

Note: For platforms that employ Radio Frequency (RF) emitters developed by a separate acquisition program, spectrum documentation for those emitters may be cited here as evidence of compliance with Spectrum Supportability regulations.

Step 10. Assess Net-Centricity.

Note: Consider individual Services net-centric policies and procedures that supplement DoD Net-centric policy.

Note: This is an emerging requirement in the analysis required for ISPs. When [Net-Centric Enterprise Services \(NCES\)/Core Enterprise Services \(CES\)](#) is available, programs will be expected to conduct this as a detailed analysis. Programs should be aware of this developing requirement, as it will become an essential part of determining net-centricity and compliance with the [Global Information Grid \(GIG\)](#).

Step 10a: Using the information provided as a result of Step 7, the PM should evaluate the program against measurement criteria from the most recent version of the NCOW Reference Model, OV-5. The PM should identify differences with the reference model as potential issues.

Step 10b: Provide an analysis of compliance with the emerging Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES).

As the GIG ES develops, its specifications should be cross-walked with the ISP system's planned network service specifications. Identify the issues associated between the CES service specifications and those of the system that is the subject of the ISP. Compliance would mean that the system would connect seamlessly with the defined DoD-level enterprise services.

Step 10c: Assess use of the following:

- Software Compliant Radios (Joint Tactical Radio System). Click here for [Software Compliant Architecture \(SCA\)](#) model and policy.
- [Internet Protocol Version 6.0 \(IPv6\)](#).
- [DoD Net-Centric Data Management Strategy](#)..
- [Global Information Grid \(GIG\) Bandwidth Expansion](#) relationships.

- [Net-centric Enterprise Service \(NCES\)](#) linkages.

The [Net Centric Operations and Warfare Reference Model \(NCOW-RM\)](#) provides a top-level view of the functions.

Step 10c Example: NCOW-RM, OV-5 (See [section 7.2.6](#) for NCOW-RM explanation and details).

Step 11: Discuss the program's inconsistencies with the DoD Global Information Grid (GIG) Architectures and the program's strategy for getting into alignment.

Identify areas where the latest version of the DoD GIG Architectures does not support information needs. [Click here for GIG details.](#)

Step 12: Discuss the program's Information Assurance (IA) strategy.

- Reference the [Program Protection Plan](#) in this section.
- Assess compliance with the [DoD Information Assurance end-to-end strategy](#).

Step 13: Identify information support needs to enable development, testing, and training.

For development phase: Weapon systems include information about potential targets that are necessary to support system development. (Example: target signature data)

For testing: Include information support needs critical to testing (Example: Joint Distributed Engineering Plant (JDEP)). Do not duplicate [Test and Evaluation Master Plan \(TEMP\) information](#) except as needed to clarify the analysis. In addition, for information on software safety testing, please refer to [section 9.3.1](#).

For training: Include trainers and simulators that are not a part of the program being developed. Include:

- Training facilities that are funded separately that your program intends to use for training support.
- Network support that will be needed to meet the training needs of your program.

ISP Chapter 3. Issues.

Present issues as defined in [DoD Instruction 4630.8](#) in a table such as Table 6, or in an outline containing the same data.

Group Operational Issues under the mission impacted, then under the impacted functional capability (for that mission).

When issues involve more than one mission, subsequent missions should be marked with the previous issue number and those fields that remain the same should be marked as such.

Include the following column (or outline) headings:

- Issue Number
- Supporting System
- Issue
- Issue Description
- Source Integrated Architectures (e.g., Command and Control (C2), Focused Logistics, Force Protection, Force Application, Battlespace Awareness, Space, etc.)

- Issue Impact
- Mitigation Strategy or Resolution Path).

Number each issue as "C-#" for critical shortfalls and "S-#" for substantive issue. Click [here](#) for DoD Global Information Grid Architectures details.

Issues shall include resolution paths (according to [DoD Instruction 4630.8, paragraph E4.4.4](#)) with projected dates to be corrected. If resolution details are not known, a discussion on the approach (including anticipated responsible parties) should be provided.

Operational Issues					
Mission					
Functional Capabilities impacted					
Issue number	Supporting system	Source Architecture	Issue Description	Issue Impact	Mitigation Strategy/Resolution Path (and Time-Frame)
Development Issues					
Testing Issues					
Training Issues					

Table 6. Sample Issue Table Format

ISP Appendices

Appendix A. References. Include all references used in developing the ISP. Include Architectures; other relevant program documentation; relevant DoD, Joint Staff and Service Directives, Instructions and Memos; ISPs or ISPs from other programs, any applicable JCIDS documentation and others as deemed necessary.

Appendix B. Systems Data Exchange Matrix (SV-6).

Appendix C. Interface Control Agreements: Identify documentation that indicates agreements made (and those required) between the subject program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency

should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

Appendix D. Acronym List: Provide an Integrated Dictionary (AV-2).

Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant Joint Capabilities Integration and Development System (JCIDS) documents. Additional, or more detailed information, used to satisfy DoD Component-specific requirements, should be included as an appendix, and not incorporated in the body of the subject ISP. Additional architecture views used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP.

7.4 NET-CENTRIC DATA STRATEGY

7.4.1. Implementing the DoD Net-Centric Data Strategy

The [DoD Net-Centric Data Strategy \(May 2003\)](#) outlines the vision for managing data in a net-centric environment. Net-centricity compels a shift to a “many-to-many” exchange of data, enabling many users and applications to leverage the same data—extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the net-centric data objectives are to ensure that all data are visible, available, and usable—when needed and where needed—to accelerate decision cycles. Specifically, the data strategy describes 7 major net-centric data goals as presented in Table 7 below:

Goal	Description
Goals to increase Enterprise and community data over private user and system data	
Visible	Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, nonintelligence, raw, and processed) are advertised or “made visible” by providing metadata, which describes the asset.
Accessible	Users and applications post data to a “shared space.” Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data is stored such that users and applications in the Enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, or security.
Institutionalize	Data approaches are incorporated into Department processes and practices. The benefits of Enterprise and community data are recognized throughout the Department.
Goals to increase use of Enterprise and community data	
Understandable	Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.
Trusted	Users and applications can determine and assess the authority of the source because the pedigree, security level, and access control level of each data asset is known and available.
Interoperable	Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.
Responsive to User Needs	Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

Table 7. Net-Centric Data Strategy Goals

The Strategic Planning Guidance FY2006-FY2011 (March 2004) informs DoD Components that, “all efforts to improve information-sharing capabilities will comply with the Net-Centric Data Strategy, [the GIG Architecture](#), and the [Net-Centric Operations and Warfare Reference Model](#).” Activities required to enable the Net-Centric Data Strategy have been incorporated into the Net-Centric Operations and Warfare Reference Model. These activities serve to guide architects and program managers in implementing the activities and sub-activities that will establish a net-centric data foundation for their program. Detailed implementation

guidance in the form of Implementation Manuals and Handbooks are under development. The activities are summarized below

7.4.2. Data Strategy Activities

Data Strategy activities are separated into four key areas: Data Planning, Manage Data Infrastructure, Provide Enterprise Data Assets and Govern Data Activities. These activities can be conducted across the span of milestones; however, the general groupings of these activities will for the most part dictate the phase in which they are conducted.

7.4.2.1. Activity Area 1, “Data Planning”

This activity area describes activities that result in data plans, standards, specifications, guidance, and policy.

7.4.2.2. Activity Area 2, “Manage Data Infrastructure”

This activity area describes activities that pertain to the establishment and management of components that were planned for in the Data Planning Activity Area. In these activities, software/hardware solutions are identified, established, and operated and maintained. Additionally, the infrastructure activities include the development of metadata products that support data sharing within a program, system, or enterprise.

7.4.2.3. Activity Area 3, “Provide Enterprise Data Assets”

This activity area describes activities that ensure that data assets can be discovered and accessed in the net-centric environment. This includes providing semantic and/or structural metadata and ensuring that data assets are visible by enterprise search capabilities and that the data asset is physically accessible through common methods employed on the GIG (such as through web-based technologies).

7.4.2.4. Activity Area 4, “Govern Data Activities”

This activity area describes activities that track compliance to policy and guidance and participation in oversight processes. Additionally, this activity area includes advocating the data strategy to stakeholders.

7.4.3. Integration into the Acquisition Life-Cycle

7.4.3.1. Before Milestone A—Data Planning Activities

Define Net-Centric Data Sharing Plan:

The activity relates to the development of a comprehensive net-centric plan to share data assets within your program/ organization and to the Enterprise. This includes metadata catalog plans, registry plans, interoperability plans, etc. In essence, this Net-Centric Data Sharing Plan should be the program's/organization's plan to accomplish the goals of the DoD Net-Centric Data Strategy. This is a key product and will drive most data activities and architectures.

Responsibilities: Sponsor/Domain Owners should develop these plans at a broad, strategic level to ensure that architectures for programs and sub-organizations associated with the Domain include net-centric data components. Depending on the scale of the Program or system, Program Managers should develop a more detailed data sharing plan that outlines how their information architecture(s) make their data and processes discoverable, accessible, and understandable to

both known and unanticipated users. These Program data sharing plans should ensure that they align with and make use of enterprise net-centric data sharing capabilities such as those envisioned/planned under the [Net-Centric Enterprise Services](#) and [Business Modernization Management Programs](#).

Define Data Guidance:

Evaluate information from sources such as compliance reports, incentive plan reports, policy, and user needs to create net-centric data guidance documents. Data guidance is the policy, specifications, standards, etc, used to drive data activities within the program/organization. It differs from a net-centric data plan in that the plan is more strategic in nature. Data guidance may be a subset of an overall net-centric data sharing plan.

Responsibilities: Sponsor/Domain Owners should develop appropriate issuance and standards to ensure that incentives, metrics, and direction are in place to drive the transition to net-centricity. Sponsor/Domain Owners should establish policy and governance to ensure that the Domain's Programs and sub-organizations have a voice in the development of standards, specifications, and processes (e.g. empowering a Program to insert its metadata requirements into an overall Domain metadata model).

Define Net-Centric Data Architectures:

Build upon existing and revised architectures and plans to describe the architecture to support data sharing objectives. The architecture should depict components that emphasize the use of discovery, services-based approach to systems engineering, use of metadata to support mediated information exchange, web-based access to data assets, etc.

Responsibilities: Both Sponsor/Domain Owners and Program Managers should include net-centric concepts, activities, and processes into their architectures. Sponsor/Domain Owners should ensure that their Domain-level architectures are developed in a manner that is appropriate for governing under a capabilities-based portfolio management process. Program Managers should ensure that net-centric components are integrated into their program architecture products.

7.4.3.2. Before Milestone B—Data Planning

Identify Data Assets:

Determine what data assets (documents, images, metadata, services, etc) are produced or controlled within a program or organization. This is primarily an inventory of data assets, which should include both structured and unstructured data sources.

Responsibilities: Sponsor/Domain Owners should identify major data assets created or managed within their Domain. This asset listing will assist in the development of visibility, accessibility, and understandability strategic plans (i.e. based on the composition of the major data assets within the Domain, the planning products can reflect the most appropriate approach in supporting net-centric data strategy goals). Likewise, Program Managers should inventory the data assets created or managed by the program and use this asset listing to plan their strategy and implementation approach for making these assets net-centric.

Prioritize Data Assets:

Assess the data asset inventory to identify key data products that are of greatest value to known users and are likely to be of value to unanticipated users. This list should be used to determine data assets a program/organization should make initial efforts at exposing as enterprise data assets.

Responsibilities: Both Sponsor/Domain Owners and Program Managers should analyze and prioritize which data assets are most valuable, initially, to be exposed as enterprise data assets.

Define Communities of Interest (COIs):

Identify appropriate groups of people who should come together to support common mission objectives. COIs are an appropriate construct for defining information exchange formats and metadata definitions as well as vocabularies used to communicate within the COI. This activity does not include the 'establishment' of actual COIs. This is simply the process of identifying COIs that exist or should exist.

Responsibilities: Sponsor/Domain Owners should define major COIs that could benefit missions within the Domain (and across Domains). Program Managers should identify other COIs that serve the goals of the program and its associated functional areas.

7.4.3.3. Before Milestone C—Manage Data Infrastructure [Determine Infrastructure Requirements]

Manage Discovery Metadata Catalog(s):

Identifying/establishing and maintaining searchable catalogs used to locate data assets within the program, organization, or enterprise. Metadata stored within these catalogs facilitates discovery and includes descriptive information about each shared data asset.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata catalogs that allow for the search of data assets across the Domain. Distributed, federated approaches should be used in developing this capability. Program Managers should ensure that their data is tagged and posted to metadata catalogs that are tied into the Domain metadata catalog.

Manage Metadata Registry(s):

Identifying and/or establishing metadata registries that can be used to maintain, manage, and/or search for metadata artifacts such as schema and data definitions. Metadata stored in metadata registries are typically for developers, business analysts, and architects. Metadata registries are a type of metadata catalog specifically designed to support developers/business analysts.

Responsibilities: Sponsor/Domain Owners should ensure that metadata products within their Domain (including associated programs and sub-organizations) are registered into the DoD Metadata Registry. Domain COIs are likely to be structured around the functional areas for which metadata is registered. Program Managers should ensure that program metadata is registered in the DoD Metadata Registry and is maintained.

Manage Service Directory(s):

Identifying and/or establishing service directory(s) that can be used to maintain, manage, and/or search for callable, reusable services from which net-centric capabilities are built. Metadata stored in service directories gives information as to the services available, how to call them, and possibly, expected service levels. Service directories include UDDI Directories used

to maintain Web Services information. This is a key component of establishing a service oriented architecture that supports net-centric data tenets.

Responsibilities: Sponsor/Domain Owners should ensure that services created or managed within their Domain (including associated programs and sub-organizations) are registered into the DoD Services Registry (TBD as first increment of NCES Discovery). Program Managers should ensure that program services are registered in the DoD Services Registry.

Manage Interoperability Components:

Development of metadata artifacts used to enable the interchange of data and information including document vocabularies, taxonomies, common data models, schema, formats, mediation components, and interface specifications.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata models to facilitate the loosely-coupled exchange of information between systems. Program Managers should develop metadata models (e.g. data structures, schema, etc) pertinent to their program. This includes tagging models, service schema, and mapping models to the Domain metadata model.

Develop/Acquire Data Access Mechanism(s):

Post data assets to an information sharing application (e.g., end-user web site, a file system, a document repository) or through the use of web services to provide system-to-system access, etc.

Responsibilities: Sponsor/Domain Owners should establish shared space, as necessary, to support Program's within its scope. Program Managers should ensure that web-enabled services provide access to valuable systems data and processes.

Manage COI(s):

This activity encompasses establishing COI(s), registering COI(s) in the Enterprise COI Directory and COI participation. The outcomes of this activity will ensure that COI(s) can be located and managed throughout the enterprise.

Responsibilities: Both Sponsor/Domain Owners and Program Managers should establish, register, and maintain identified COIs.

7.4.3.4. Before Full Rate Deployment Decision—Provide Enterprise Data Assets

Provide Discovery Metadata:

Associate or generate discovery metadata for data assets. This activity is the 'tagging' of data assets to provide value-added information about data assets that can be used to support discovery, accessibility, IA, and understandability.

Responsibilities: Program Managers should ensure that discovery metadata is provided for all data assets created/managed by the Program.

Post Discovery Metadata:

Providing, or posting, discovery metadata to catalogs, registries, etc, that can be searched. It is through 'posting metadata' that metadata catalogs are populated. This activity allows data assets to be discovered (but does not guarantee access to the data asset).

Responsibilities: Program Managers should ensure that discovery metadata associated with each data asset is posted to searchable metadata catalogs (established by the Domain and by Programs).

7.4.3.5. Cross Milestone Activities--Govern Data Activities

Participate in GIG Governance:

Participate in governance activities that enable net-centric data asset sharing. This includes participation in GIG Enterprise Service efforts, net-centric architectural compliance, IT Portfolio Management for net-centricity, etc.

Responsibilities: Sponsor/Domain Owners should participate in GIG governance activities to ensure the proper processes are followed and executed within their Domain to enable the net-centric Domain environment.

Enforce Data Guidance:

Participate in enforcement/compliance activities that assess net-centric architectures against Net-Centric Data Guidance that was developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and Program Managers should enforce established data guidance (including conformance to standards and adherence to DoD/Domain issuances).

Advocate Data Strategy(s):

This activity involves vetting, publicizing, and institutionalizing the Net-Centric Data Sharing plans and guidance developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and Program Managers should advocate the DoD Net-Centric Data Strategy and Domain-established data guidance.

7.4.4. Supporting Language for IT System Procurements

To ensure support of the goals of DoD Net-Centric Data Strategy, the program manager, through his or her contracting specialists, should include the following sections, as appropriate, in Request for Proposal/Request for Quotation language for the procurement of IT systems.

- The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the [DoD Net-Centric Data Strategy dated May 9, 2003](#).
- Also, the contractor must ensure that any IT systems covered in this procurement or identified in this RFP/RFQ meet the requirements detailed below. Additionally, it is acceptable for vendors and/or integrators to provide functionality (via wrappers, interfaces, extensions) that tailor the COTS system to enable these requirements below (i.e. the COTS system need not be modified internally if the vendor/integrator enables the requirements through external or additional mechanisms. In this case, these mechanisms must be acquired along with the COTS system procurement).
 - *Access to Data:* The contractor shall ensure that all data managed by the IT system can be made accessible to the widest possible audience of Global Information Grid (GIG) users via open, web-based standards. Additionally, the system's data should be accessible to GIG users without 1) the need for proprietary client-side

software/hardware, or 2) the need for licensed user-access (e.g. non-licensed users should be able to access the system's data independent to the licensing model of the COTS system). This includes all data that is used to perform mission-related analysis and processing including structured and unstructured sources of data such as databases, reports, and documents. It is not required that internal, maintenance data structures be accessible.

- Metadata: The contractor shall ensure that all significant business data made accessible by the IT system is tagged with descriptive metadata to support the net-centric goal of data visibility. Accordingly, the system data shall be tagged to comply, at a minimum, with the DoD Discovery Metadata Specification (DDMS). This specification is available at: zzz. The system should provide DDMS-compliant metadata at an appropriate level based on the type of data being tagged. It is not required that individual records within databases be tagged; rather it is expected that the database itself or some segment of it is tagged appropriately. Additionally, the contractor shall ensure that all structural and vocabulary metadata (metamodels, data dictionaries) associated with the exposed system data be made available in order to enable understanding of data formats and definitions. This includes proprietary metadata if it is required to effectively use the system data.
- Enterprise Services/Capabilities: The contractor shall ensure that key business logic processing and other functional capabilities contained within the IT system are exposed using web-based open standards (e.g. APIs provide for Web Services-based access to system processes and data). The level of business logic exposure shall be sufficient to enable reuse/extension within other applications and/or to build new capabilities. The contractor shall provide an assessment of how any licensing restrictions affect or does not affect meeting the goals of re-use and exposure as GIG-wide enterprise services.
- Optional Components/Modules: The contractor shall ensure that all standard and/or optional components of the IT system are identified and procured in a manner that ensures the requirements outlined in this document are met.

7.5 INFORMATION ASSURANCE (IA)

7.5.1. Information Assurance (IA) Overview

Most programs delivering capability to the warfighter or business domains will use information technology to enable or deliver that capability. For those programs, developing a comprehensive and effective approach to IA is a fundamental requirement and will be key in successfully achieving program objectives. DoD defines IA as “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.” DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Program Managers and functional proponents for programs should be familiar with statutory and regulatory requirements governing information assurance, and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the program’s architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program. The information in the following sections will explain these tasks, the policy from which they are derived, their relationship to the acquisition framework, and the details one should consider in working towards effective IA defenses-in-depth in a net-centric environment.

7.5.2. Mandatory Policies

- [DoD Directive 5000.1, Enclosure 1, Paragraph E1.9, Information Assurance](#), states:

Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in [DoD Directive 8500.1](#), reference (j).

- [DoD Instruction 5000.2, Enclosure 4, Paragraph E.4.2, IT System Procedures](#) states: “The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.”

The DoD CIO must certify (for MAIS programs) and confirm (for MDAPs) that the program is being developed in accordance with the CCA before Milestone approval. One of the key elements of this certification or confirmation is the DoD CIO’s determination that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards. (See [Table E4.T1](#). See section [7.8](#) of this Guidebook for a discussion of CCA compliance.)

- [DoD Directive 8500.1](#), "Information Assurance (IA)": This directive establishes policy and assigns responsibilities under [10 U.S.C. 2224](#) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates

the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

- [DoD Instruction 8500.2](#), "Information Assurance (IA) Implementation": This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under [DoD Directive 8500.1](#).
- [DoD Instruction 5200.40](#), "DoD Information Technology Security Certification And Accreditation Process (DITSCAP)": This instruction implements policy, assigns responsibilities and prescribes procedures under [DoD Directive 8500.1](#) for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the DoD.
 - According to [DoD Directive 8500.1](#), all acquisitions of Automated Information Systems (AISs) (to include Automated Information System applications, outsourced IT-based processes, and platforms or weapon systems with connections to the [Global Information Grid \(GIG\)](#) must be certified and accredited according to [DoD Instruction 5200.40](#), DITSCAP.
 -
 - See other applicable Certification & Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information Systems" for systems processing Sensitive Compartmented Information).

7.5.3. Information Assurance (IA) Integration into the Acquisition Life Cycle

7.5.3.1. Before Milestone A

- 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 (Click here to find guidelines on making this determination: IA compliance requirements.)
- Establish an IA organization. Appoint a trained IA professional in writing as the IA Manager. This and other IA support may be organic to the program office, matrixed from other supporting organizations (e.g. Program Executive Office), or acquired through a support contractor.
- Begin to identify system IA requirements. Click here for [Baseline IA Controls](#) and [IA Requirements Beyond Baseline Controls](#).
- Develop an acquisition IA strategy, if required. Click here for IA Compliance Decision Tree or click here for an [Acquisition IA Strategy Template](#). Acquisition IA strategies developed in preparation for Milestone A will be more general, and contain a lesser level of detail than acquisition IA strategies submitted to support subsequent Milestone decisions. Click here to see the detailed [Acquisition IA Strategy guidelines](#).

7.5.3.2. Before Milestone B

- If program is initiated post-Milestone A, complete all actions for Milestone A.
- Ensure IA considerations are incorporated in the program's Acquisition Strategy. Click here for example language for [Acquisition Strategy IA Considerations](#).

- Update and submit the acquisition IA strategy. Click here for an [Acquisition IA Strategy Template](#).
- 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).
- Initiate DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Click here for [DoD Instruction 5200.40](#) or other applicable Certification & Accreditation process (such as Director of Central Intelligence Directive (DCID) 6/3 “Protecting Sensitive Compartmented Information Within Information Systems” for systems processing Sensitive Compartmented Information).

7.5.3.3. Before Milestone C

- Incorporate IA solutions through:
 - Systems Security Engineering efforts
 - Procurement of IA/IA enabled products. [DoD Instruction 5000.2, Section E4.2.7](#), states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made." The [Enterprise Software Initiative \(ESI\)](#) includes commercial IA tools and should be utilized as the preferred source for the procurement of IA tools. The [ESI Home Page](#) lists covered products and procedures, and also shows [DFARS \(SUBPART 208.74\)](#) and Defense Acquisition System ([DoD Instruction 5000.2, E4.2.7](#)) requirements for compliance with the DoD ESI.
 - Implementation of security policies, plans, and procedures
 - Conducting IA Training
- Test and evaluate IA solutions. Click here for [IA Testing details](#).
 - Developmental Test
 - Security Test & Evaluation, Certification and Accreditation activities
 - Operational Test
- Accredite the system under the [DITSCAP](#) or other applicable Certification and Accreditation process. For systems using the DITSCAP, DITSCAP Phase III should be completed, and an Approval to Operate should be issued by the Designated Approval Authority. Click here for [DoD Instruction 5200.40](#) discussion of the Approval to Operate and Designated Approval Authority or other applicable Certification & Accreditation process elements (such as (DCID) 6/3 “Protecting Sensitive Compartmented Information Within Information Systems” for systems processing Sensitive Compartmented Information).

7.5.3.4. After Milestone C (or the Full Rate Production Decision Review for MAIS Systems)

- Maintain the system’s security posture throughout its life cycle. This includes periodic re-accreditation.

7.5.4. Estimated Information Assurance (IA) Activity Durations and Preparation Lead Times

The following chart shows the relationship between the acquisition framework and typical timeframes for accomplishing key IA activities.

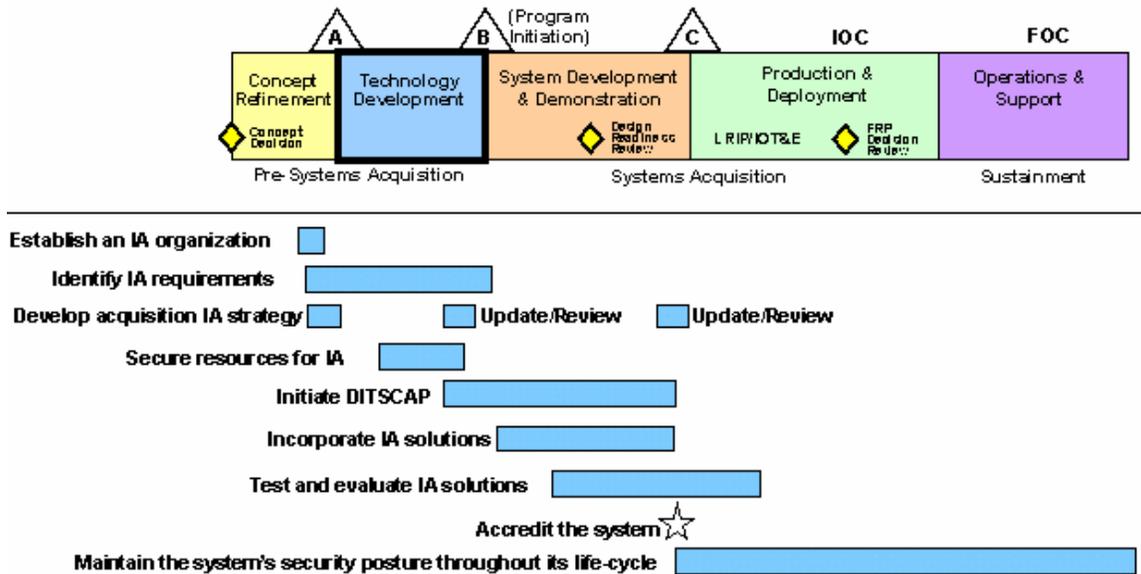


Figure 8. Typical Timeframes for Accomplishing Key IA Activities

Based on experience with a number of acquisition programs (both Major Automated Information Systems and Major Defense Acquisition Programs), an IA strategy for a pre-Milestone B program can be developed, staffed and coordinated, approved by the DoD Component Chief Information Officer and reviewed by the DoD Chief Information Officer in a period of 4-6 months. Typically 3-4 months of this effort is dedicated to defining the system IA architecture, which is a function of the overall system architecture.

For a pre-Milestone C program, a typical IA strategy can be completed, approved, and reviewed in 6 weeks to 3 months, because the system architecture will be more mature. However, there is an increased possibility that development of the strategy at this late date may uncover IA shortfalls because the strategy is being developed after IA-impacting decisions have been made. Click here for acquisition IA Strategy details.

7.5.5. Integrating Information Assurance (IA) into the Acquisition Process

The IA Compliance Decision Tree, Figure 9, is designed to help program managers determine the degree to which the 8500 series applies to any acquisition and whether an Acquisition IA Strategy is required. A tabular depiction of the same information appears in Table 8. IA Compliance by Acquisition Program Type.

Because requirements for IA vary greatly across acquisition programs, program managers should examine acquisition programs carefully to identify applicable IA requirements. The following guidelines derived from [DoD Directive 8500.1](#) apply:

1) Programs that do not involve the use of Information Technology (IT) in any form have no IA requirements. However, program managers should examine programs carefully, since many programs have IT, such as automatic test equipment, embedded in the product or its supporting equipment.

2) Programs that include IT always have IA requirements, but these IA requirements may be satisfied through the normal system design and test regimen, and may not be required to comply with [DoD Directive 8500.1](#). Acquisitions that include Platform IT with no network interconnection to the Global Information Grid fit into this category. However, such programs require an IA Strategy if they are designated Mission Critical or Mission Essential.

3) Acquisitions of Platforms with network interconnections to the Global Information Grid must comply with the IA requirements of [DoD Directive 8500.1](#) and DoD Instruction 8500.2.

4) Acquisitions of Automated Information System applications or outsourced IT processes also must comply with [DoD Directive 8500.1](#) and DoD Instruction 8500.2.

5) Programs that include IT, and that are designated Mission Critical or Mission Essential, require an IA Strategy without regard to the applicability of [DoD Directive 8500.1](#). The DoD Component Chief Information Officer is responsible for approving the IA Strategy. Subsequent to the DoD Component Chief Information Officer approval, in accordance with [DoD Instruction 5000.2](#), the DoD Chief Information Officer must review the IA Strategy.

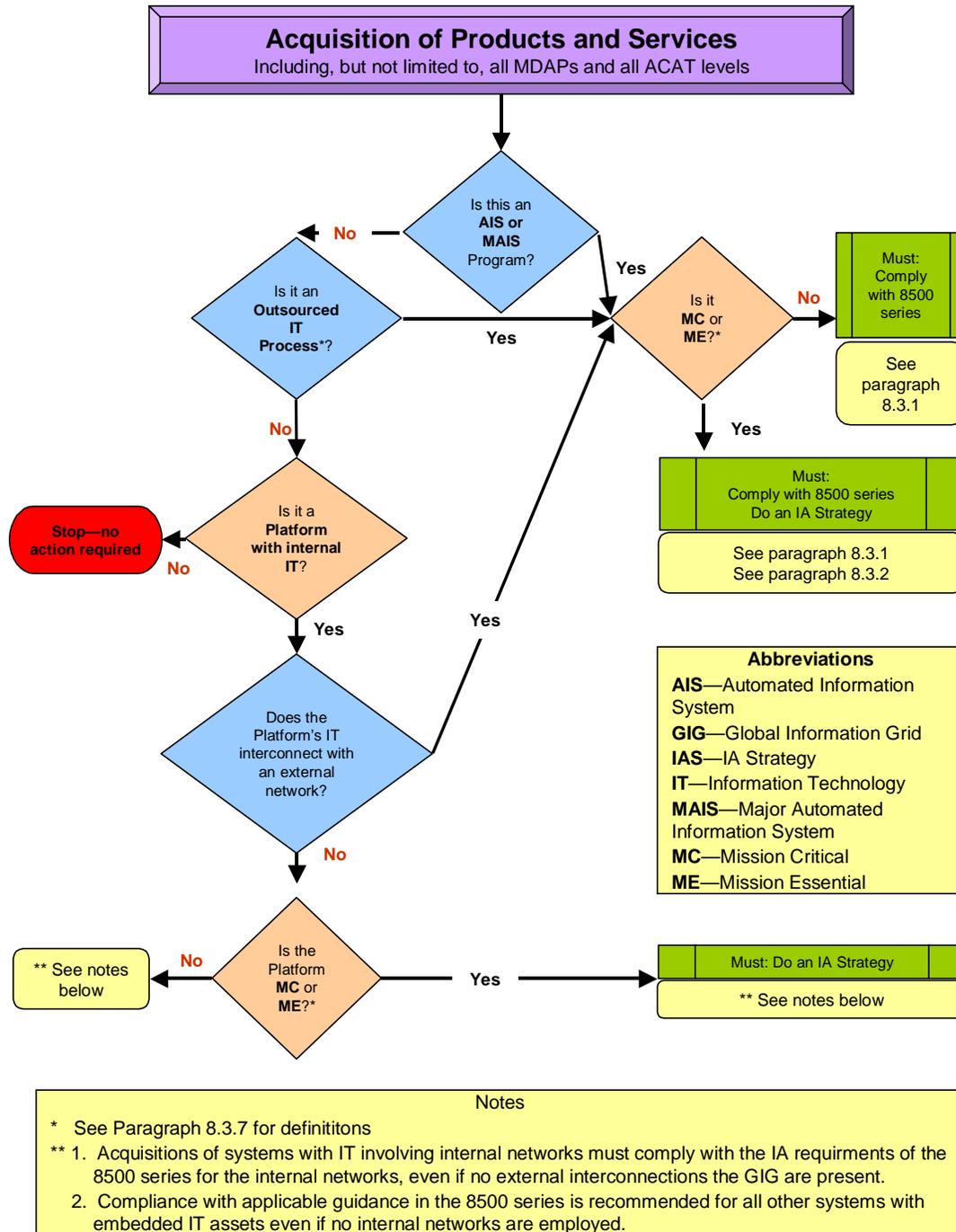


Figure 9. IA Compliance Decision Tree

Acquisition Programs for:		Acquisition IA Strategy	Compliance with 8500 series
No IT		Not Required	Not Required
Non-MC/ME AIS		Not Required*	Required
Non-MC/ME MAIS		Not Required*	Required
MC/ME AIS		Required	Required
MC/ME MAIS		Required	Required
Outsourced IT-based Processes		Not Required*	Required
Outsourced IT-based Processes that are MC/ME		Required	Required
Platform IT products/weapons systems that are, or have:			
MC/ME	Network Interconnections to the GIG		
No	No	Not Required*	Recommended**
No	Yes	Not Required*	Required
Yes	No	Required	Recommended**
Yes	Yes	Required	Required
Legend: AIS = Automated Information System GIG = Global Information Grid IT = Information Technology MAIS = Major Automated Information System MC/ME = Mission Critical/Mission Essential PM = Program/Project Manager			
* Although not required by DoD, the Component may require an Acquisition IA Strategy. ** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system			

Table 8. IA Compliance by Acquisition Program Type

7.5.6. Program Manager (PM) Responsibilities

7.5.6.1. Platform Information Technology (IT) Systems

Program managers for acquisitions of platforms with internal IT, including platforms such as weapons systems, sensors, medical technologies, or utility distribution systems, remain ultimately responsible for the platform's overall Information Assurance (IA) protection. If the Platform IT has an interconnection to the Global Information Grid (GIG), in accordance with [DoD Instruction 8500.2](#), the program manager must identify all assurance measures needed to ensure both the protection of the interconnecting GIG enclave, and the protection of the platform from connection risks, such as unauthorized access, that may be introduced from the enclave. However, connecting enclaves have the primary responsibility for extending needed IA services (such as Identification and Authentication) to ensure an assured interconnection for both the enclave and the interconnecting platform. These IA requirements should be addressed as early in the acquisition process as possible. Program managers for acquisitions of Platforms with IT that does not interconnect with the GIG retain the responsibility to incorporate all IA protective

measures necessary to support the platform's combat or support mission functions. The definition of the GIG recognizes "non-GIG IT that is stand-alone, self-contained or embedded IT that is not or will not be connected to the enterprise network." Non-GIG IT may include "closed loop" networks that are dedicated to activities like weapons guidance and control, exercise, configuration control or remote administration of a specific platform or collection of platforms. The primary test between whether a network is part of the GIG or is non-GIG IT is whether it provides enterprise or common network services to any legitimate GIG entity. In any case, PMs for systems that are not connected to GIG networks would demonstrate prudent judgment by considering the IA program provisions in [DoD Direction 8500.1](#) and [DoD Instruction 8500.2](#), and employing those IA controls appropriate to their system.

7.5.6.2. Automated Information Systems (AIS)

Program managers for acquisitions of AIS applications are responsible for coordinating with enclaves that will host (run) the applications early in the acquisition process to address operational security risks the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement. The baseline IA Controls serve as a common framework to facilitate this process. The Designated Approving Authority for the enclave receiving an AIS application is responsible for incorporating the IA considerations for the AIS application into the enclave's IA plan. The burden for ensuring an AIS application has adequate assurance is a shared responsibility of both the AIS application Program Manager and the Designated Approving Authority for the hosting enclave; however, the responsibility for initiation of this negotiation process lies clearly with the Program Manager. Program managers should, to the extent possible, draw upon the common IA capabilities that can be provided by the hosting enclave.

7.5.6.3. Outsourced IT-based Processes

Program managers for acquisitions of Outsourced IT-based Processes must comply with the IA requirements in the 8500 policy series. They are responsible for delivering outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services that present specific and unique challenges for the protection of the Global Information Grid. The program manager for an Outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied to protect DoD information in the service provider's operating environment and interconnected DoD information systems. Acquisition Contracting Officers should be familiar with IA requirements in general.

7.5.7. Information Assurance (IA) Controls

7.5.7.1. Baseline Information Assurance (IA) Controls

[DoD Instruction 8500.2, Enclosure 3](#), establishes fundamental IA requirements for DoD information systems in the form of two sets of graded baseline IA Controls. Program managers are responsible for employing the sets of baseline controls appropriate to their programs. The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the User Representative on behalf of the information owner. IA Controls addressing availability and integrity requirements are keyed to the system's MAC based on the importance of the information to the mission, particularly the warfighters' combat mission. IA

Controls addressing confidentiality requirements are based on the sensitivity or classification of the information. There are three MAC levels and three confidentiality levels with each level representing increasingly stringent information assurance requirements. The three MAC levels are identified in Table 9.

MISSION ASSURANCE CATEGORY			
	DEFINITION	Integrity	Availability
1	These systems handle 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.	HIGH	HIGH
2	These systems handle information that is important to the support of deployed and contingency forces.	HIGH	MEDIUM
3	These systems handle 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.	BASIC	BASIC

Table 9. Mission Assurance Category (MAC) Levels for IA Controls

The other major component in forming the baseline set of IA controls for every information system is determined by selecting the appropriate confidentiality level based on the sensitivity of the information associated with the information system. DoD has defined three levels of confidentiality, which are identified below.

Confidentiality Level	Definition
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoDD 8500.1 , to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release)

Table 10. Confidentiality Levels for IA Controls

7.5.7.2. Determining Baseline Information Assurance (IA) Controls

The specific set of baseline IA controls that the program manager should address is formed by combining the appropriate lists of Mission Assurance Category (MAC) and Confidentiality Level controls specified in the [DoD Instruction 8500.2, Enclosure 2](#). Table 11 illustrates the possible combinations.

Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	MAC 1	Classified	1 and 4
2	MAC 1	Sensitive	1 and 5
3	MAC 1	Public	1 and 6
4	MAC 2	Classified	2 and 4
5	MAC 2	Sensitive	2 and 5
6	MAC 2	Public	2 and 6
7	MAC 3	Classified	3 and 4
8	MAC 3	Sensitive	3 and 5
9	MAC 3	Public	3 and 6

Table 11. Possible Combinations of Mission Assurance Category and Confidentiality Level

There are a total of 157 individual IA Controls from which the baseline sets are formed. Each IA Control describes an objective IA condition achieved through the application of specific safeguards, or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the objective condition for every IA Control are assignable, and thus accountable. The IA Controls specifically address availability, integrity, and confidentiality requirements, but also take into consideration the requirements for non-repudiation and authentication.

It is important to exercise due diligence in establishing the MAC level of an information system. The baseline set of IA controls for availability and integrity are purposefully graded to become increasingly stringent for the higher MAC levels. The required resource costs to achieve compliance with the baseline IA controls at the higher MAC levels can be very significant as befits information and information systems on which a warfighter's mission readiness or operational success depends. The IA controls also become increasingly stringent or robust at the higher Confidentiality levels.

7.5.7.3. Information Assurance (IA) Requirements Beyond Baseline IA Controls

There are several additional sources of IA requirements beyond the Baseline IA Controls.

A system being acquired may have specific IA requirements levied upon it through its controlling capabilities document (i.e., Capstone Requirements Document, Initial Capabilities Document, Capabilities Development Document or Capabilities Production Document). These IA requirements may be specified as performance parameters with both objective and threshold values.

All IA requirements, regardless of source, are compiled in a single system Requirements Traceability Matrix. [DoD Instruction 5200.40](#) discusses the Requirements Traceability Matrix and other applicable Certification & Accreditation processes (such as Director of Central

Intelligence Directive (DCID) 6/3 “Protecting Sensitive Compartmented Information Within Information Systems” for systems processing Sensitive Compartmented Information).

7.5.8. Information Assurance (IA) Testing

See [section 9.9.2.](#) for a discussion of IA testing considerations.

7.5.9. Acquisition Information Assurance (IA) Strategy

The primary purpose of the Acquisition IA Strategy is to ensure compliance with the statutory requirements of the [Clinger Cohen Act](#), as implemented by [DoD Instruction 5000.2](#). As stated in [Table E4.T1](#) of that Instruction, the Acquisition IA Strategy provides documentation that “The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.” The PM develops the Acquisition IA Strategy to help the program office organize and coordinate its approach to identifying and satisfying IA requirements consistent with DoD policies, standards, and architectures.

The Acquisition IA Strategy serves a purpose separate from the System Security Authorization Agreement (SSAA). Developed earlier in the acquisition life cycle and written at a higher level, the Acquisition IA Strategy documents the program’s overall IA requirements and approach, including the certification and accreditation approach (which will subsequently result in an SSAA). The Acquisition IA Strategy must be available for review at all Acquisition Milestone Decisions, including early milestones when an SSAA would not yet be available.

The Acquisition IA Strategy lays the groundwork for a successful SSAA by facilitating consensus among the Program Manager, Component Chief Information Officer and DoD Chief Information Officer on pivotal issues such as Mission Assurance Category, Confidentiality Level, and applicable Baseline IA Controls; selection of the appropriate certification and accreditation process; identification of the Designated Approving Authority and Certification Authority; and documenting a rough timeline for the certification and accreditation process.

7.5.9.1. Development

Ideally, a Working-level Integrated Product Team (WIPT) should support the development of the Acquisition IA Strategy. The WIPT should consist of subject matter experts familiar with the system being acquired, the intended use of the system, and the operational and system architectures within which the system will function. As the operational and system architectures mature, the WIPT should plan for and coordinate interface details with managers of systems and subsystems with which the system being acquired will interface.

The Acquisition IA Strategy should be a stand-alone document. Although other key documents can be referenced within the Acquisition IA Strategy to identify supplemental or supporting information, the Acquisition IA Strategy should contain sufficient internal content to clearly communicate the strategy to the reader. If a single document is employed by the program to consolidate acquisition documentation, the Acquisition IA Strategy should be included as a separate section of the document.

Configuration control of the Acquisition IA Strategy should be maintained with respect to the program’s governing requirements document (Initial Capabilities Document, etc.) and the Information Support Plan (formerly known as the C4ISP). If a governing capabilities document

or the Information Support Plan is updated, the Acquisition IA Strategy should be validated or updated accordingly.

The [IA Strategy Format Template](#), while not mandatory, will help you construct an Acquisition IA Strategy document that will satisfy statutory review requirements. Write the document at the unclassified level, and include classified annexes, if required. Factors determining the specific content and level of detail needed can include the following:

- Acquisition life cycle stage. Strategies for programs that are early in the acquisition life cycle will be necessarily at a higher level and less definitive than more mature programs. The level of detail in an Acquisition IA Strategy will increase as a program transitions from one acquisition phase to the next. At program initiation, an IA Strategy is not expected to contain all of the information about initial operating capabilities or future system interfaces that will be available at Milestone B or at the full-rate production decision point. Requirements, employment concepts, and architectures for both the system being acquired, and the systems with which it interfaces, will evolve and mature throughout the acquisition life cycle. As the program matures, the IA Strategy should also evolve. The strategy should be maintained with revisions as required until system retirement and disposal. [Click here for acquisition IA Strategy details](#).
- Extent of system/network interaction. Systems with a high degree of system-to-system information exchange, or systems connected to the Global Information Grid will require more comprehensive discussions of IA considerations related to their environment.
- Mission Assurance Category and Confidentiality Level. Systems with higher mission assurance categories and higher confidentiality levels will necessarily require more comprehensive strategies than those with lower levels.
- Developmental systems versus Commercial-off-the-Shelf (COTS)/Non-Developmental-Item (NDI). Programs acquiring new systems through development will require more robust treatment of the identification, design, systems engineering and testing of IA requirements than non-developmental programs. However, IA Strategies for the acquisition of COTS/NDI systems should also address the approach employed to ensure that the COTS/NDI products meet IA requirements and comply with the requirements of [DoD Instruction 8500.2, Enclosure 3](#). [<link>](#)
- Evolutionary Acquisitions. Programs employing evolutionary acquisition should differentiate the identification and satisfaction of IA requirements, certification and accreditation activities, and milestone reviews for each increment planned.
- Special Circumstances. In the following specific cases, Acquisition IA Strategy content is limited as noted, in consideration of the unique characteristics of these acquisition programs:
 - Family of Systems or System of Systems Acquisition Programs. The Acquisition IA Strategy for these programs should be written at a capstone level, focusing on the integration of IA requirements and controls, coordination of System Security Authorization Agreement boundaries, and ensuring IA resourcing for own and subordinate systems. [Click here for acquisition IA Strategy details](#).
 - Platform IT with interconnection to an external system or network. In accordance with [DoD Instruction 8500.2](#), the Acquisition IA Strategy must specifically address

IA protection for the interconnection points. Click here for [acquisition IA Strategy](#) details.

- Platform IT with no interconnection to an external system or network. The requirement for an Acquisition IA Strategy can be satisfied by inserting the following statement in the program’s [Clinger Cohen Act compliance table](#) submission: “Platform IT does not have an interconnection to an external network.” [DoD Instruction 8500.2, Enclosure 4](#) provides further guidance on the submission of a [Clinger Cohen Act compliance table](#). Although not required, program managers responsible for this type of acquisition would be prudent to consider and implement the IA guidance in [DoD Directive 8500.1](#) and [DoD Instruction 8500.2](#). Click here for more on the [Clinger Cohen Act](#).

DoD Components may require additional questions/areas of concerns (e.g. Critical Infrastructure Protection; Privacy Impact, etc.) in separate DoD Component-specific implementing guidance for Acquisition IA Strategy content and submission.

7.5.9.2. Review Requirements

Acquisition IA Strategies must be submitted for approval and review in accordance with Table 12, which is based on submission requirements detailed in [DoD Instruction 5000.2, Enclosure 4](#). Sufficient time should be allowed for Acquisition IA Strategy preparation or update, Component CIO review and approval, and DoD CIO review prior to applicable milestone decisions, program review decisions, or contract awards.

Acquisition Category *	Events requiring prior DoD CIO Review	Acquisition IA Strategy Approval	Acquisition IA Strategy Review
ACAT IAM, IAC, and ID	Milestone A, B, C (or full rate production decision), and acquisition contract award	Component CIO	DoD CIO
All other acquisitions	Acquisition contract award	Component CIO or Designee	Delegated to Component CIO

*Acquisition Category (ACAT) descriptions are provided in [DoD Instruction 5000.2, Table E2.T1](#).

Table 12. IA Strategy Approval and Review Requirements

7.5.9.3. Additional Information

Questions or recommendations concerning the Acquisition IA Strategy or its preparation or the IA strategy template should be directed to the Defense-wide Information Assurance Program Office (OASD(NII)-DIAP).

7.5.9.4. Information Assurance Strategy Template

(PROGRAM NAME)

1. **Program Category and Life Cycle Status:** Identify the Acquisition Category (ACAT) of the program. Identify current acquisition life cycle phase and next milestone decision.

Identify whether the system has been designated “Mission Critical” or “Mission Essential” in accordance with DoD Instruction 5000.2. Include a graphic representation of the program’s schedule.

2. **Mission Assurance Category (MAC) and Confidentiality Level:** Identify the system’s MAC and Confidentiality Level as specified in the applicable requirements document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2.
3. **System Description:** Provide a high-level overview of the specific system being acquired. Provide a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe the system’s function, and summarize significant information exchange requirements (IER) and interfaces with other IT or systems, as well as primary databases supported. Describe, at a high level, the IA technical approach that will secure the system, including any protection to be provided by external systems or infrastructure. PMs should engage National Security Agency (NSA) early in the acquisition process for assistance in developing an IA approach, and obtaining information systems security engineering (ISSE) services, to include describing information protection needs, defining and designing system security to meet those needs, and assessing the effectiveness of system security.
4. **Threat Assessment:** (Include as classified annex if appropriate) Describe the methodology used to determine threats to the system (such as a System Threat Assessment Report (STAR)), and whether the IT was included in the overall weapon system assessment. In the case of an AIS application, describe whether there were specific threats unique to this system’s IT resources due to mission or area of proposed operation. For MAIS programs, utilization of the “Information Operations Capstone Threat Capabilities Assessment” (DIA Doc # DI-1577-12-03) [1st Edition Aug 03] is required by DoD Instruction 5000.2.
5. **Risk Assessment:** (Include as classified annex if appropriate) Describe the program’s planned regimen of risk assessments, including a summary of how any completed risk assessments were conducted. For systems where software development abroad is a possible sourcing option, describe how risk was assessed.
6. **Information Assurance Requirements:** Describe the program’s methodology used for addressing IA requirements early in the acquisition lifecycle. Specify whether any specific IA requirements are identified in the approved governing requirements documents (e.g. Capstone Requirements Document, Initial Capabilities Document, Capabilities Design Document, or Capabilities Production Document). Describe how IA requirements implementation costs (including costs associated with certification and accreditation activities) are included and visible in the overall program budget.
7. **Acquisition Strategy:** Provide a summary of how information assurance is addressed in the program’s overall acquisition strategy document. Describe how the Request for Proposal (RFP) for the System Development and Demonstration Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and

testing. In addition, describe how the RFP communicates the requirement for personnel that are trained in IA. Address whether the program will be purchasing commercial off-the-shelf IA or IA-Enabled products, and the program's means for verifying that the mandates of National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products" will be followed.

- 8. DoD Information Technology Security Certification and Accreditation Process (DITSCAP):** Provide the name, title, and organization of the Designated Approving Authority (DAA), Certification Authority (CA), and User Representative. If the program is pursuing an evolutionary acquisition approach (spiral or incremental development), describe how each increment will be subjected to the certification and accreditation process. Provide a timeline describing the target completion dates for each phase of certification and accreditation in accordance with DoD Instruction 5200.40. Normally, it is expected that DITSCAP Phase 1 will be completed prior to or soon after Milestone B; Phase 2 and 3 completing prior to Milestone C; and Authority to Operate (ATO) issued prior to operational test and evaluation. If the DITSCAP process has started, identify the latest phase completed, and whether an Authority to Operate (ATO) or Interim Authority to Operate (IATO) was issued. If the system being acquired will process, store or distribute Sensitive Compartmented Information (SCI), compliance with Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information Systems" is required, and approach to compliance should be addressed.
- 9. IA Testing:** Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test & Evaluation Master Plan.
- 10. IA Shortfalls:** (Include as classified annex if appropriate) Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall. If applicable, identify any Acquisition Decision Memoranda that cite IA issues.
- 11. Policy/Directives:** List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable. This list is available at <http://iase.disa.mil/policy.html>.
- 12. Relevant Associated Program Documents:** Provide statement that this version of the Acquisition IA Strategy is reflective of the Program CRD/ICD/CDD/CPD dated _____, and the Information Support Plan (ISP) dated _____. [Note: subsequent revisions to the requirements documents or ISP will require a subsequent revision or revalidation of the Acquisition IA Strategy.]

13. **Point of Contact:** Provide the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document. It is recommended that the program office's formally appointed Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.

7.5.9.5. Information Assurance (IA) Strategy Considerations

The following text is recommended for tailoring as the Acquisition IA section of an Acquisition Strategy. The presented "considerations" are examples, but experience has shown that they are common to most programs. The program manager should tailor and include this text as appropriate.

Information Assurance

The _____ PMO has reviewed all appropriate Information Assurance (IA) policy and guidance, and has addressed the implementation of these IA considerations in the _____ Program Information Assurance Strategy. IA requirements shall be addressed throughout the system life cycle in accordance with DoD Directive 8500.1, DoD Instruction 8500.2, DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," [*include: "and Director of Central Intelligence Directive 6/3" but only if system handles SCI*]. The IA Strategy is an integral part of the program's overall acquisition strategy, identifying the technical, schedule, cost, and funding issues associated with executing requirements for information assurance. The following summarizes significant IA considerations impacting the program's acquisition strategy.

IA Technical Considerations. _____ will employ Commercial-Off-The-Shelf (COTS) IA and IA-enabled products as part of the security architecture. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). Similarly, GOTS IA or IA-enabled products employed by the system must be evaluated by the NSA or in accordance with NSA-approved processes. [*and/or other significant technical issues as required*]

IA Schedule Considerations. The IA certification and accreditation timeline includes significant events that impact the overall testing, operational assessment and deployment schedules. Key milestones such as the approval of the Phase I SSAA, Interim Authority to Test, Interim Authority to Operate, and Authority to Connect, as well as the overall certification and accreditation schedule, are integrated into the program's Test & Evaluation Master Plan (TEMP). [*other significant schedule issues as required*]

IA Cost Considerations. IA specific costs include the development/procurement, test & evaluation, and certification & accreditation of the IA architecture. It also includes operations and maintenance costs related to maintaining the system security posture following deployment. [*identify any high-impact issues*]

IA Funding Considerations. All IA lifecycle costs are adequately funded. [*if not, what and why*]

IA Staffing and Support Issues. The PMO is adequately staffed to support IA requirements, with (X) Government staff assigned full time IA duties. One member of the PMO staff has been appointed Information Assurance Manager for the system, in accordance with DoD Directive 8500.1. Support contractors provide X full-time-equivalents

of IA support to the PMO. In addition, [activity X] will provide C&A support to the program.
[other significant staffing and support issues as required]

7.5.10. DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

In accordance with [DoD Directive 8500.1](#), all acquisitions of AISs (to include MAIS), outsourced IT-based processes, and platforms or weapon systems with connections to the GIG must be certified and accredited in accordance with [DoD Instruction 5200.40](#), *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*.

7.5.11. Software Security Considerations

For the acquisition of software-intensive Information Technology, especially that used in National Security Systems, program managers should consider the significant operational threat posed by the intentional or inadvertent insertion of malicious code.

The Defense Intelligence Agency can perform an analysis to determine foreign ownership, control, and/or influence of vendors bidding for selection to provide information technology, if warranted. If there is sufficient cause for security concerns based on the analysis, the acquiring organization should conduct an independent evaluation of the software.

The Program Manager should identify the software-intensive Information Technology candidates for Defense Intelligence Agency analysis before the Milestone B decision.

7.5.12. Information Assurance (IA) Definitions

The following IA related definitions are provided to assist the reader in understanding IA terminology. For a more comprehensive set of IA definitions, see [DoD Directive 8500.1](#) and [DoD Instruction 8500.2](#), and [DoD Instruction 5200.40](#).

Accreditation. Formal declaration by the Designated Approving Authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Acquisition Program. A directed, funded effort that provides new, improved, or continuing materiel, weapon, or information system or service capability, in response to an approved need.

Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Automated Information System (AIS). See DoD Information System.

Availability. Timely, reliable access to data and information services for authorized users.

Certification. Comprehensive evaluation of the technical and non-technical security features of an information technology system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Authority (CA). Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying, and assessing the risks associated

with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation package.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Confidentiality Level. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has defined three confidentiality levels: classified, sensitive, and public.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

DoD Information System. The entire infrastructure, organization, personnel, and components for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology-based processes, and platform information technology interconnections.

Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program such as those described in DoD Directive 5000.1. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or fire control); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave.

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced information technology-based processes they support, and derive their security needs from those systems. They provide standard Information Assurance capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, tactical networks, and data processing centers.

Outsourced Information Technology (IT)-based Process. For DoD Information Assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform Information Technology (IT) Interconnection. For DoD Information Assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT 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 such as weapons, 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. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration and remote upgrade or reconfiguration.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities. [Click here](#) to for DoD Instruction 5200.40 or other applicable Certification & Accreditation process (such as Director of Central Intelligence Directive (DCID) 6/3 “Protecting Sensitive Compartmented Information Within Information Systems” for systems processing Sensitive Compartmented Information).

Family of Systems (FoS). A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities, dependent on the situation. An example of an FoS would be an anti-submarine warfare FoS consisting of submarines, surface ships, aircraft, static and mobile sensor systems and additional systems. Although these systems can independently provide militarily useful capabilities, in collaboration they can more fully satisfy a more complex and challenging capability: to detect, localize, track, and engage submarines.

Global Information Grid (GIG). Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG Information Technology (IT) is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

[Click here for GIG details.](#)

Information Assurance (IA) Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality.

Information Assurance (IA) Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

Information Assurance (IA)-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Major Automated Information System (MAIS). An acquisition program where: (1) the dollar value estimated by the DoD Component Head is to require program costs (all appropriations) in any single year in excess of \$32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of \$126 million in FY 2000 constant dollars, or total life-cycle costs in excess of \$378 million in FY 2000 constant dollars, or (2) MDA designation as special interest.

Milestone Decision Authority (MDA). The designated individual with overall responsibility for a program. The MDA shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.

Mission Assurance Category. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

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.

Mission Critical (MC) Information System. A system that meets the definitions of "information system" and "national security system," the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a DoD Component Head, a Combatant

Commander, or their designee. A financial management Information Technology (IT) system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense(Comptroller.) A “Mission-Critical Information Technology System” has the same meaning as a “Mission-Critical Information System.” For additional information, see DoD Instruction 5000.2, Enclosure 4.

Mission Essential (ME) Information System. A system that meets the definition of “information system” that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the Under Secretary of Defense(Comptroller) A “Mission-Essential Information Technology System” has the same meaning as a “Mission-Essential Information System.” For additional information, see DoD Instruction 5000.2, Enclosure 4.

National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

- Involves intelligence activities;
- Involves cryptologic activities related to national security;
- Involves command and control of military forces;
- Involves equipment that is an integral part of a weapon or weapons system; or
- Subject to the following limitation, is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Outsourced Information Technology-based Process. See DoD Information System.

Platform Information Technology Interconnection. See DoD Information System.

Program Manager (PM). The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority throughout the life cycle.

System of Systems (SoS). A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SoS could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or agency), the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.

System Security Authorization Agreement (SSAA). A formal agreement among the Designated Approving Authority(ies), the Certification Authority, the Information Technology (IT) system user representative, and the program manager. It is used throughout the entire DoD

Information Technology Security Certification and Accreditation Process (see DoD Instruction 5200.40) to guide actions, document decisions, specify IT security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Weapon(s) System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

7.6 ELECTROMAGNETIC SPECTRUM

7.6.1. Electromagnetic Spectrum Considerations

The program manager must consider the electromagnetic spectrum when delivering capability to the warfighters or business domains. The fundamental questions are if and how the system or equipment being developed will depend on and interact with the electromagnetic spectrum (hereafter referred to as “spectrum”). Other key questions include the following:

- Will the system/equipment require spectrum to operate as it is intended (e.g., to communicate with other systems; to collect and/or transmit data, to broadcast signals, etc.)?
- Will the spectrum the system/equipment needs to operate be available for use in the intended operational environment?
- Will the system/equipment, including commercial-off-the-shelf systems delivered by the program, radiate electromagnetic energy that could be detrimental to other systems or equipment?
- Will the intended operational electromagnetic environment produce harmful effects to the intended system, even if the proposed system does not radiate electromagnetic energy (such as ordnance)?

National, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum direct program managers developing spectrum-dependent systems/equipment to consider spectrum supportability requirements and Electromagnetic Environmental Effects (E3) control early in the development process. Given the complex environment (both physical and political) in which DoD forces operate, and the potential for worldwide use of capabilities procured for DoD, early and thorough consideration is vitally important. The spectrum supportability process ensures the following:

- The spectrum-dependent system/equipment being acquired is designed to operate within the proper portion of the electromagnetic spectrum;
- Permission has been (or can be) obtained from designated authorities of sovereign (“host”) nations (including the United States) to use that equipment within their respective borders; and
- The newly acquired equipment can operate compatibly with other spectrum dependent equipment already in the intended operational environment (electromagnetic compatibility).

Because this process requires coordination at the national and international levels, starting the process early helps a program manager address the full range of considerations and caveats, obtain the necessary approvals to proceed through the acquisition process, and successfully deliver capabilities that will work.

E3 control is concerned with the proper design and engineering to minimize the impact of the electromagnetic environment on equipment, systems, and platforms. E3 control applies to the electromagnetic interactions of both spectrum-dependent and non-spectrum-dependent objects within the operational environment. Examples of non-spectrum-dependent objects that

could be affected by the electromagnetic environment are ordnance, personnel, and fuels. The increased dependency on and competition for portions of the electromagnetic spectrum have amplified the likelihood of adverse interactions among sensors, networks, communications, and weapons systems.

Ensuring the compatible operation of DoD systems in peace and in times of conflict is growing in complexity and difficulty. DoD has established procedures, described below, to successfully obtain spectrum supportability for, and control the electromagnetic environmental effects impacts upon the equipment, systems, and platforms used by our military forces. While the requirements to obtain spectrum supportability should be addressed early in the acquisition programs, the proper design and engineering techniques to control E3 should be considered throughout the acquisition process to ensure the successful delivery of the operational capability to the warfighter.

7.6.2. Mandatory Policies

- [DoD Instruction 5000.2, Enclosure 3, Table E3.T1](#) (Statutory Information Requirements) requires all systems/equipment that require utilization of the electromagnetic spectrum to obtain spectrum certification compliance through the submission of a [DD Form 1494](#), "Application for Equipment Frequency Allocation." Compliance (obtained by receiving host nation approval of the submitted DD1494) is required at Milestone B (or at Milestone C, if there is no Milestone B).
- [Title 47, CFR, Chapter III, Part 300.1](#) requires compliance with the [National Telecommunications and Information Administration "Manual of Regulations and Procedures for Federal Radio Frequency Management,"](#) and applies to all Federal Agencies that use the electromagnetic spectrum within the United States and U.S. possessions.
- [OMB Circular A-11, Part 2](#), contains the requirement to obtain certification by the National Telecommunications and Information Administration that the radio frequency can be made available before estimates are submitted for the development or procurement of major radio spectrum-dependent communications-electronics systems (including all systems employing satellite techniques) within the United States and U.S. possessions.
- [DoD Directive 4650.1](#), "Policy for the Management and Use of the Electromagnetic Spectrum," contains policy applicable to all DoD Components that prohibits spectrum-dependent systems under development from

(1) Proceeding into the System Development and Demonstration Phase without a spectrum supportability determination unless the MDA grants specific authorization to proceed; or

(2) Proceeding into the Production and Deployment Phase without a spectrum supportability determination unless the Under Secretary of Defense (Acquisition, Technology, and Logistics) or the Assistant Secretary of Defense for Networks and Information Integration grants specific authorization to proceed.

The Directive also requires that spectrum-dependent "off-the-shelf" or other non-developmental system have a spectrum supportability determination before being purchased or procured.

- [DoD Directive 3222.3](#), “DoD Electromagnetic Environmental Effects (E3) Program,” establishes policy and responsibilities for the management and implementation of the DoD E3 Program. This program ensures mutual electromagnetic compatibility and effective electromagnetic environmental effects control among ground, air, sea, and space-based electronic and electrical systems, subsystems, and equipment, and the existing natural and man-made electromagnetic environment.

7.6.3. Spectrum Management Integration into the Acquisition Life Cycle

Assigned managers should take the following actions to obtain spectrum supportability for spectrum-dependent equipment, and minimize the electromagnetic environmental effects on all military forces, equipment, systems, and platforms (both spectrum-dependent and non spectrum-dependent). Consideration of these critical elements throughout the acquisition process will help to ensure successful delivery of capability to the warfighter.

The assigned manager should include the funding to cover spectrum supportability and control of electromagnetic environmental effects as part of the overall program budget. [Section 7.6.4.1](#) addresses spectrum supportability; [Section 7.6.4.2](#) addresses electromagnetic environmental effects.

7.6.3.1. Before Milestone A

As early as possible:

- Develop spectrum supportability and electromagnetic environmental effects (E3) control requirements and perform initial spectrum supportability and E3 risk assessments to ensure Spectrum issues are addressed early in the program acquisition. (Click here for definition of [spectrum supportability and E3](#), and information relating to [spectrum supportability processes](#) and [E3 control requirements](#)).
- Complete and submit an initial Stage 1 (Conceptual) [DD Form 1494](#) for coordination. Click here for [DD Form 1494 processing for Spectrum Certification](#) herein.

7.6.3.2. Before Milestone B (or before the first Milestone that authorizes contract award)

- If the system is spectrum-dependent and has not yet obtained Certification of Spectrum Support from National Telecommunications and Information Administration or the Military Communications-Electronics Board to proceed into the System Development and Demonstration Phase, the PM must develop a justification and a proposed plan to obtain spectrum supportability. ([DoD Directive 4650.1](#) requires Milestone Decision Authorities and/or DoD Component Acquisition Executives to provide such a justification and proposed plan to the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Director, Operational Test and Evaluation (DOT&E), and the Chair, Military Communications-Electronics Board.)
- Address spectrum supportability and electromagnetic environmental effects (E3) control requirements in the [Statement of Work \(SOW\)](#), [Contract Data Requirements List \(CDRL\)](#), and [Performance Specifications](#).

- Update the spectrum supportability and E3 control requirements according to [CJCSM 3170.01](#) to ensure spectrum issues are addressed in the [Capability Development Document](#).
- Ensure completion/update and submission of the [DD Form 1494](#). If previously submitted, ensure information is current. Click here for [DD Form 1494 processing for Spectrum Certification](#).
- Define spectrum supportability and E3 control requirements in the [Information Support Plan](#).
- Define in the [Test Evaluation Master Plan](#) (1) spectrum supportability and E3 control requirements to be tested during Developmental Test and Evaluation, and (2) the spectrum supportability and E3 assessments to be performed during Operational Test and Evaluation.

7.6.3.3. Before Milestone C

- Review and update spectrum supportability and electromagnetic environmental effects control requirements in the [Capability Production Document](#), the [Information Support Plan](#), and [Test Evaluation Master Plan](#). (Click here for information relating to Spectrum Certification Actions). Clarify relationship of hyperlink.
- If the system is spectrum-dependent and has not yet obtained the spectrum supportability required to allow the system to proceed into the Production and Deployment Phase, the PM must develop a justification and a proposed plan to obtain spectrum supportability. ([DoD Directive 4650.1](#) requires MDAs and/or CAEs to provide such a justification and proposed plan to the USD(AT&L)/ASD(NII)/DoD(CIO), the DOT&E, and the Chair, MCEB.)

7.6.3.4. After Milestone C

- Monitor system changes to determine their impact on requirements for spectrum supportability and electromagnetic environmental effects (E3) control. Changes to operational parameters (e.g., tuning range, bandwidth, emission characteristics, antenna gain and/or height, or output power) or proposed operational locations may require additional spectrum certification actions through an updated [DD Form 1494](#) or require additional E3 analysis or tests. Program managers should work with their spectrum managers to determine and satisfy additional requirements, as appropriate.

7.6.3.5. Estimated Preparation Lead Time

Spectrum certification must be addressed at milestone reviews as required by [DoD Instruction 5000.2](#). Nominal time to complete the spectrum certification process (time from DD Form 1494 submittal to approval) is normally three to nine months, but often takes longer. Therefore, at a minimum, the program manager should plan to submit the [DD Form 1494](#) three to nine months prior to a Milestone decision. Processing time depends upon quality of data, the number of host nations whose coordination is required, and the size of the staffs at the host nations' spectrum offices. The host nation approval process can be a critical factor in obtaining spectrum certification. It is sometimes a lengthy process, so start early to obtain approval. To avoid unnecessary processing delays, list on the DD Form 1494 **only those nations in which permanent deployment is planned, (i.e., do not list "worldwide deployment" as the intended operational environment)**.

7.6.3.6. Key Review Actions by Assigned Managers

- Define, and update as necessary, applicable electromagnetic environments where systems/equipment are intended to operate;
- Establish electromagnetic environmental effects (E3) control requirements, with special emphasis on mutual compatibility and Hazards of Electromagnetic Radiation to Ordnance guidance;
- Define E3 programmatic requirements to include analyses, modeling and simulation, and test and evaluation;
- Ensure that E3 developmental test and evaluation / operational test and evaluation requirements and spectrum management planning and analyses are addressed in the Test and Evaluation Master Plan, and that resources are identified to support these activities.

7.6.3.7. Electromagnetic Environmental Effects (E3) Control and Spectrum Certification Requirements in the Joint Capabilities Integration and Development System

Both [CJCSM 3170.01](#) and [CJCSI 6212.01](#) require the Capstone Requirements Document, the Capability Development Document, and the Capability Production Document to address spectrum certification and E3 control.

The Joint Staff will employ the following assessment criteria when reviewing the Capstone Requirements Document:

- Does the Capstone Requirements Document address spectrum certification and supportability?
- Does the Capstone Requirements Document address the control of electromagnetic environmental effects (E3)?

According to the Capability Development Document and Capability Production Document template in CJCSM 3170.01 and CJCSI 6212.01, both spectrum supportability and E3 control requirements must be addressed. The Joint Staff will employ the following assessment criteria when reviewing the Capability Development Document and/or the Capability Production Document:

- Does the Capability Development Document and/or the Capability Production Document address spectrum certification, supportability, and host nation approval?
- Does the Capability Development Document and/or the Capability Production Document address the control of E3?
- Does the Capability Development Document and/or the Capability Production Document address the safety issues regarding hazards of electromagnetic radiation to ordnance?

Sample Language. The three sample statements shown below should be included, as applicable, as THRESHOLD requirements. The first applies to communications-electronics equipment and is used to denote compliance with applicable DoD, national, and international spectrum policies and regulations. The second is used to require compatible operation. Finally, the third would be used if ordnance safety were of concern.

Spectrum Certification. *The XXX System will comply with the applicable DoD, National, and International spectrum management policies and regulations*

and will obtain spectrum certification prior to operational deployment. DD Form 1494 will be submitted to the Military Communications Electronics Board Joint Frequency Panel. (Threshold)

Electromagnetic Environmental Effects. The XXX System shall be mutually compatible and operate compatibly in the electromagnetic environment. It shall not be operationally degraded or fail due to exposure to electromagnetic environmental effects, including high intensity radio frequency (HIRF) transmissions or high-altitude electromagnetic pulse (HEMP). Ordnance systems will be integrated into the platform to preclude unintentional detonation. (Threshold)

Hazards of Electromagnetic Radiation to Ordnance. All ordnance items shall be integrated into the system in such a manner as to preclude all safety problems and performance degradation when exposed to its operational electromagnetic environment. (Threshold)

7.6.3.8. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Information Support Plan (ISP)

According to [DoD Instruction 4630.8](#) and [CJCSI 6212.01](#), the ISP must address Spectrum Supportability (e.g., Spectrum Certification, reasonable assurance of the availability of operational frequencies, and consideration of E3 control). Specific items to be addressed are listed in DoD Instruction 4630.8 paragraph 8.2.7.3.3.2, Step 9.

7.6.3.9. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Test and Evaluation Master Plan (TEMP)

Within the TEMP, the critical operational issues for suitability or survivability are usually appropriate to address spectrum supportability and E3 control requirements. The overall goals of the test program with respect to spectrum supportability and E3 control requirements are to ensure that appropriate evaluations are conducted during developmental test and evaluation, and that appropriate assessments are performed during operational test and evaluation. These evaluations and assessments should define the performance and operational limitations and vulnerabilities of spectrum supportability and E3 control requirements. See sections [9.9.3](#). and [9.9.5](#) for details.

Sample Language. The following are four examples of critical operational issues statements in the TEMP:

- Will the platform/system (or subsystem/equipment) detect the threat in a combat environment at adequate range to allow a successful mission? (Note: In this example, the “combat environment” includes the operational electromagnetic environment.)
- Will the system be safe to operate in a combat environment? (Note: In this example, electromagnetic radiation hazards issues such as hazards of electromagnetic radiation to personnel, ordnance, and volatile materials and fuels can be addressed, as applicable.)
- Can the platform/system (or subsystem/equipment) accomplish its critical missions? (Note: This example determines if the item can function properly without degradation to or from other items in the electromagnetic environment.)

- Is the platform/system (or subsystem/equipment) ready for Joint and, if applicable, Combined operations? (Note: In this example, the item must be evaluated in the projected Joint and, if applicable, Combined operational electromagnetic environment.)

7.6.3.10. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in Performance Specifications

Although the use of E3 Control Requirements extracted from Military Standards (MIL-STD) 461 and 464A and [Military Handbook \(MIL-HDBK\) 237C](#) is not mandatory, these three documents provide crucial guidance that, if followed, should preclude E3 problems with the critical systems provided to the warfighter.

Performance specifications should invoke spectrum supportability and E3 control requirements. [MIL-STD-461](#), which defines E3 control (emission and susceptibility) requirements for equipment and subsystems, and [MIL-STD-464A](#), which defines E3 control requirements for airborne, sea, space, and ground platforms/systems, including associated ordnance, can be used as references. Ordnance includes weapons, rockets, explosives, electrically initiated devices, electro-explosive devices, squibs, flares, igniters, explosive bolts, electric primed cartridges, destructive devices, and jet-assisted take-off bottles.

Sample Language. The following examples address E3 control in subsystem/equipment performance specifications:

Electromagnetic Interference (EMI) Control. *The equipment shall comply with the applicable requirements of MIL-STD-461”*

Electromagnetic Interference (EMI) Test. *The equipment shall be tested in accordance with the applicable test procedures of MIL-STD-461”*

As an alternative, the program manager can tailor system-level E3 control requirements from MIL-STD-461 or MIL-STD-464. Both MIL-STD-461 and MIL-STD-464 are interface specifications. See [section 9.9.3](#). for testing standards and guidance from Director, Operational Test & Evaluation and Development Test and Evaluation. See [section 9.9.5](#). for mandatory and non-mandatory use of DoD Single Stock Point for Specifications and Standards/MILSPEC reform homepage.

7.6.3.11. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Statement of Work (SOW)

The following is an example SOW statement to address spectrum supportability and E3 control requirements:

The contractor shall design, develop, integrate, and qualify the system such that it meets spectrum supportability and E3 control requirements of the system specification. The contractor shall perform analyses, studies, and testing to establish spectrum supportability and E3 control requirements and features to be implemented in the design of the item. The contractor shall perform inspections, analyses, and tests, as necessary, to verify that the system meets its spectrum supportability and E3 control requirements. The contractor shall prepare and update the DD Form 1494 throughout the development of the system for spectrum dependent equipment and shall perform analysis and testing to characterize the equipment, where necessary. The contractor shall establish and support a

spectrum supportability and E3 control requirements Working-level Integrated Product Team (WIPT) to accomplish these tasks. MIL-HDBK-237 may be used for guidance.

7.6.3.12. Data Item Requirements for Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Contract Data Requirements List (CDRL)

The following are examples of data item requirements typically called out for spectrum supportability and E3 control requirements in the CDRL:

- DI-EMCS-80199B EMI [Electromagnetic Interference] Control Procedures
- DI-EMCS-80201B EMI Test Procedures
- DI-EMCS-80200B EMI Test Report
- DI-EMCS-81540 E3 Integration and Analysis Report
- DI-EMCS-81541 E3 Verification Procedures
- DI-EMCS-81542 E3 Verification Report
- DI-MISC-81174 Frequency Allocation Data

7.6.4. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Summary

7.6.4.1. Spectrum Supportability

Spectrum certification effects **spectrum supportability**. The program manager should initiate the spectrum certification process, to ensure spectrum supportability, early in the acquisition cycle.

The purpose of spectrum certification is to:

- Obtain authorization from the National Telecommunications and Information Administration to develop or procure items that use a defined frequency band(s) or specified frequencies to accommodate a specific electronic function(s);
- Ensure compliance with national policies and allocation tables which provide order in the use of the radio frequency spectrum; and
- Ensure spectrum availability to support the item in its intended operational environment.

7.6.4.1.1. Process

A diagram depicting the Spectrum Certification Process is presented below in **Figure 10**.

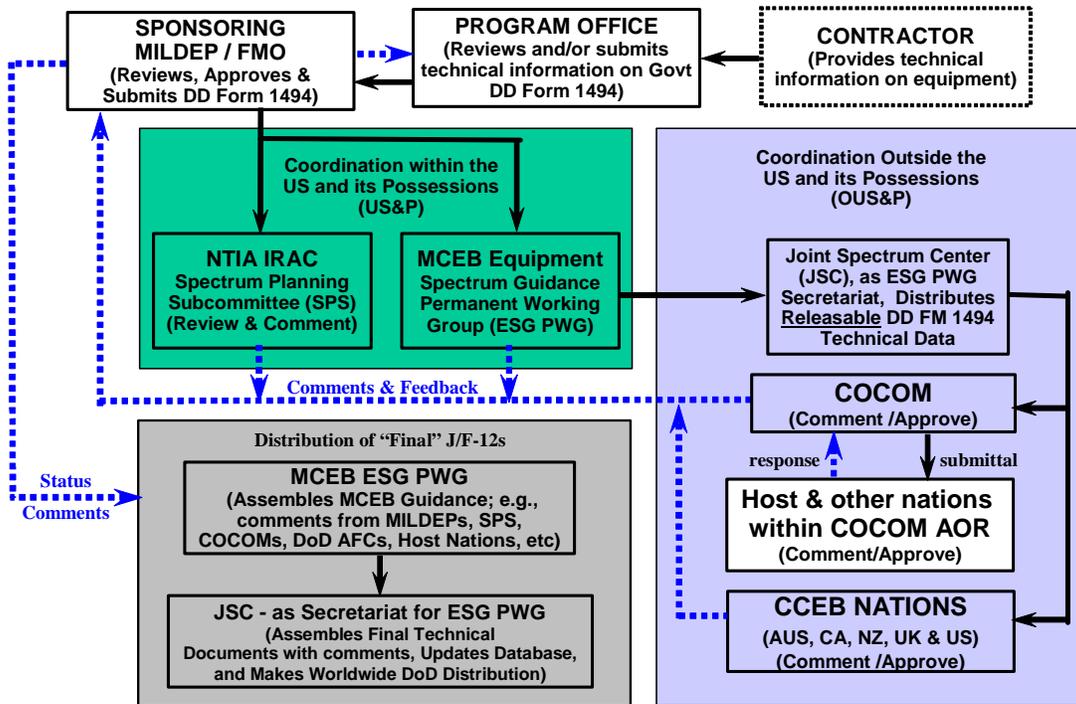


Figure 10. DoD Equipment Spectrum Certification Process

The Spectrum Certification Process is also called “Frequency Allocation” or the “JF-12 Process.” The Program Manager submits [DD Form 1494](#), “Application for Equipment Frequency Allocation,” to obtain spectrum certification.

- The DD Form 1494 documents the spectrum-related technical and performance characteristics of an acquisition item to ensure compliance with the applicable DoD, individual national, both U.S. and foreign, and international spectrum management policies and regulations.
- The DD Form 1494 is routed through command channels to the sponsoring Military Department Frequency Management Office: the U.S. Army Spectrum Management Office, the Navy-Marine Corps Spectrum Center, or the Air Force Frequency Management Agency. The Military Department Frequency Management Office then submits the form simultaneously or as required to:
 - The Spectrum Planning Subcommittee of the Interdepartment Radio Advisory Committee under the National Telecommunications and Information Administration and

- The Equipment Spectrum Guidance Permanent Working Group under the Frequency Panel of the Joint Staff Military Communications-Electronics Board.

Spectrum Certification within the United States and Its Possessions. The National Telecommunications and Information Administration Spectrum Planning Subcommittee provides a national level review and approval for the DD Form 1494.

Department of Defense Internal Review. Within the Department of Defense, the Equipment Spectrum Guidance Permanent Working Group is responsible for the overall review, coordination and processing of all DoD frequency allocation applications. Within the Equipment Spectrum Guidance Permanent Working Group (formerly called the J-12 Permanent Working Group) the DD Form 1494 receives a tracking number (e.g., J/F-12/XXXX) and is reviewed by the other Military Department Frequency Management Office representatives. The Equipment Spectrum Guidance Permanent Working Group then sends the DD Form 1494 to other entities throughout the Department of Defense for review and comment. The Equipment Spectrum Guidance Permanent Working Group prepares the final J/F-12/XXXX for Military Communications-Electronics Board approval after all internal and external (e.g., National Telecommunications and Information Administration and/or Host Nation(s)) review and coordination has occurred.

Spectrum Certification outside the United States and Its Possessions. Any information intended to be released to a foreign nation must be approved for release by the appropriate DoD Component authority. Once a J/F-12 is approved for release to foreign nations and forums, it is then coordinated through the appropriate Combatant Command or other appropriate military offices, such as a Defense Attaché Office or Military Assistance Group office, with the foreign countries (also called “Host Nations”) that have been identified as projected operating locations for the particular equipment. Since Host Nation coordination can be a lengthy and difficult process, the Program Manager should only list those nations on the DD Form 1494 in which permanent deployment is planned.

Per [Office of Management and Budget Circular A-11, Part 2](#), program managers must heed the advice provided by National Telecommunications and Information Administration. In addition, program managers should follow guidance provided by foreign governments (i.e., host nation comments provided in response to the request to coordinate on a J/F-12) and implement suggested changes even if testing and/or operation is intended to occur within the United States but eventual deployment and operation is intended or desired for that host nation.

7.6.4.1.2. Note-to-Holders Mechanism

A “Note-to-Holders” is a mechanism provided within the spectrum certification process to permit minor changes to existing spectrum certification documentation in lieu of generating a completely new, separate application. The types of modifications permitted include:

- Adding the nomenclatures(s) of equipment which have essentially identical technical and operating characteristics as a currently allocated item,
- Adding comments that have been provided by the National Telecommunications Information Administration or host nations,
- Documenting minor modifications, or improvements to equipment that do not essentially alter the operating characteristics (transmission, reception, frequency response), or

- Announcing the cancellation or reinstatement of a frequency allocation.

A Note-to-Holders can be initiated by contacting the appropriate Military Department Frequency Management Office.

7.6.4.1.3. Frequency Assignment

Frequency assignments are issued by designated authorities of sovereign nations, such as telecommunications agencies within foreign countries, and the National Telecommunications and Information Administration for the United States and Its Possessions. Under certain conditions, other designated authorities, such as DoD Area Frequency Coordinators or Unified and Specified Commanders may grant frequency assignments. Equipment that has not been previously granted some level of spectrum certification will normally not receive a frequency assignment. Procedures for obtaining frequency assignments, once the equipment, sub-system, or equipment has become operational, are delineated in regulations issued by the Unified and Specified Commands and/or Military Services.

In most cases, the operational frequency assignments are requested and received after a program has been fielded. However, if the Program Manager has implemented guidance received in response to the submission of a DD Form 1494 during program development (e.g., incorporation of spectrum supportability comments) and designed the system as described in the [DD Form 1494](#), system operators have not historically encountered problems in obtaining operational frequency assignments. Note: Spectrum congestion, competing systems, and interoperability, all may contribute to the operator encountering some operational limitations such as geographical restrictions or limitations to transmitted power, antenna height and gain, bandwidth or total number of frequencies made available, etc. Certification to operate in a particular frequency band does not guarantee that the requested frequency(ies) will be available to satisfy the system's operational spectrum requirements over its life cycle.

7.6.4.2. Electromagnetic Environmental Effects (E3)

7.6.4.2.1. Objective for E3 Control

The objective of establishing E3 control requirements in the acquisition process is to ensure that DoD equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational electromagnetic environment. To be effective, the program manager should establish E3 control requirements early in the acquisition process to ensure compatibility with co-located equipment, subsystems, and equipment, and with the applicable external electromagnetic environment.

7.6.4.2.2. Impacts When E3 Control Is Not Considered

It is critical that all electrical and electronic equipment be designed to be fully compatible in the intended operational electromagnetic environment. The Department of Defense has experience with items developed without adequately addressing E3. Results include poor performance, disrupted communications, reduced radar range, and loss of control of guided weapons. Failure to consider E3 can result in mission failure, damage to high-value assets, and loss of human life. Compounding the problem, there is increased competition for the use of the spectrum by DoD, non-DoD Government, and civilian sector users; and many portions of the electromagnetic spectrum are already congested with electromagnetic-dependent items. In addition, new platforms/systems and subsystems/equipment are more complex, more sensitive,

and often use higher power levels. All of these factors underscore the importance of addressing E3 control requirements early in the acquisition process.

7.6.4.3. Additional Resources

Spectrum management related information is available on the [Joint Spectrum Center website](#). Spectrum compliance is a special interest area on the [Acquisition Community Connection website](#).

7.6.5. Definitions

Key terms pertaining to spectrum supportability and electromagnetic compatibility processes are defined below.

Electromagnetic (EM) Spectrum. The range of frequencies of EM radiation from zero to infinity. For the purposes of this guide, "electromagnetic spectrum" shall be defined to be the range of frequencies of EM radiation that has been allocated for specified services under the U.S. and international tables of frequency allocation, together with the EM spectrum outside the allocated frequency range where use of unallocated frequencies could cause harmful interference with the operation of any services within the allocated frequency range. The terms "electromagnetic spectrum," "radio frequency spectrum," and "spectrum" shall be synonymous.

Electromagnetic Compatibility (EMC). The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic Environment (EME). The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. EME is the sum of electromagnetic interference, electromagnetic pulse, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials, and natural phenomena effects of lightning and precipitation static.

Electromagnetic Environmental Effects (E3). The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility (EMC) and electromagnetic interference (EMI); electromagnetic vulnerability (EMV); electromagnetic pulse (EMP); electrostatic discharge, hazards of electromagnetic radiation to personnel (HEMP), ordnance (HERO), and volatile materials (HERF); and natural phenomena effects of lightning and precipitation static (P-Static).

Equipment Spectrum Certification. The statement(s) of adequacy received from authorities of sovereign nations after their review of the technical characteristics of a spectrum-dependent equipment or system regarding compliance with their national spectrum management policy, allocations, regulations, and technical standards. Equipment Spectrum Certification is alternately called "spectrum certification. Note: Within the United States and Its Possessions the requirement for certification of DoD spectrum-dependent equipment is prescribed by OMB

Circular A-11, Part 2, and Title 47, CFR, Chapter III, Part 300 (the National Telecommunications and Information Administration "Manual of Regulations and Procedures for Federal Radio Frequency Management) and also applies to all equipment or systems employing satellite techniques.

Host Nations (HNs). Those sovereign nations, including the United States, in which the Department of Defense plans or is likely to conduct military operations with the permission of that nation.

Spectrum Management. The planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference

Spectrum Supportability. The assessment as to whether the electromagnetic spectrum necessary to support the operation of a spectrum-dependent equipment or system during its expected life cycle is, or will be, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" requires, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation from HNs, and a consideration of EMC. (Note: While an actual determination of spectrum supportability for a spectrum-dependent system within a particular country (i.e., Host Nation) may be possible based upon "spectrum supportability" (e.g., equipment spectrum certification) comments provided by that host nation, the overall determination of whether a spectrum-dependent system has spectrum supportability is the responsibility of the MDA based upon the totality of spectrum supportability comments returned from those host nations whose comments were solicited.)

Spectrum-Dependent Systems. Those electronic systems, subsystems, devices and/or equipment that depend on the use of the electromagnetic spectrum for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition, and transfer of information.

7.7 BUSINESS MODERNIZATION MANAGEMENT PROGRAM

7.7.1. The Business Modernization Management Program (BMMP)

In addition to the [Global Information Grid](#) (GIG)-related programs, the [Business Modernization Management Program \(BMMP\)](#) and its associated [Business Enterprise Architecture \(BEA\)](#) are important to the DoD business domains, their functional proponents, and program managers who are acquiring capabilities for those domains. The Secretary of Defense established the BMMP to provide policy, strategic planning, oversight, and guidance for the Department's BMMP transformation efforts. The [Business Management and System Integration \(BMSI\) Office](#), within the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)), and the Business Domains comprise the organizational elements within BMMP.

The BEA and Transition Plan were approved by the USD(C) in April 2003. The BEA is an extension of the [GIG Architecture](#) and is in conformance with the overall GIG Architecture. The BEA extension is a "to-be" architecture: it describes the DoD Business Enterprise of the future and represents a framework of requirements for transforming DoD and business processes. Due to the GIG conformance with the [Federal Enterprise Architecture \(FEA\)](#), programs compliant with the BEA are deemed compliant with the FEA.

See the [BMMP Home Page](#) for detailed information regarding the BMMP and the BEA. Program managers should become familiar with the website, including the following information:

- (1) Secretary of Defense memorandum, July 19, 2001, establishing the BMMP program (initially called the Financial Management Modernization Program);
- (2) Key information about each of the [Business Domains](#); and
- (3) USD(C) memoranda establishing guidelines on when and how to obtain USD(C) certification or approval for proposed acquisitions of, or improvements in, Financial Management systems.
- (4) USD(C) memorandum, July 16, 2004, expanding the Comptroller certification requirements to include non-financial business systems.

(Note: DoD Instruction 5000.2 captures the requirements that flow from statute and from implementing Comptroller memoranda. These requirements are summarized below under "Mandatory Policies.")

7.7.2. Mandatory Policies

[DoD Instruction 5000.2, Operation of the Defense Acquisition System](#)

- [Section E4.2.8](#) requires the USD(C) to certify that financial management MAIS acquisition programs comply with the requirements of the BMMP and BEA before the MDA grants any milestone or full-rate production approval.
- [Section E4.2.9](#) states that before a DoD Component can obligate more than \$1,000,000 for a defense financial system improvement (i.e., a new, or modification of, a budgetary, accounting, finance, enterprise resource planning, or mixed (financial and non-financial) information system), the USD(C) must determine and certify that the

system is being developed or modified, and acquired and managed in a manner that is consistent with both the BEA and the BMMP Transition Plan. Furthermore, the USD(C) will certify the program to the MDA before the MDA gives any milestone or full-rate production approval (or their equivalent).

7.7.3. Integration within the Acquisition Process

The following categories of systems and system initiatives require USD(C) approval before obligation of funds or, when required, milestone approval:

- a) All [financial management, mixed and non-financial business](#) system initiatives with projected pre-Milestone A (or equivalent) costs greater than \$1,000,000.
- b) All financial management, mixed and non-financial business systems currently in development, with program costs greater than \$1,000,000 and requiring a Milestone A, Milestone B, Milestone C, Full Rate Production, or fielding decision, or requesting a change to approved functional or technical baselines.
- c) All financial management, mixed and non-financial systems in sustainment with costs of greater than \$1,000,000 for upgrades or enhancements.

For the approvals defined above, the following generic process describes steps that PMs, Domains, BMSI and the USD(Comptroller) will follow to review and approve requests. For acquisition programs, these steps should be accomplished using the Joint Capabilities Integration and Development System and the acquisition process, including appropriate Functional Capabilities Boards (FCBs), WIPTs, IIPs, OIPs and Information Technology Acquisition Board (ITAB) meetings. BMMP-related issues identified in the process will be resolved through the IPT process. For MAIS and MDAPs, when an OIPT recommends that a program is ready to proceed for MDA approval as a result of meeting all requirements, including those encompassed by the BMMP, the USD(C) will provide BMMP certification of the program as soon as possible, but not later than the ITAB meeting. For programs below the scope of MAIS or MDAP, follow Domain and Comptroller procedures.

1. Contact the lead Business Domain for the system improvement.
2. If the Lead and Partner Business Domains support initiation of the project based on an initial portfolio management review, they will provide the PM a package containing the related Business Domains' and OUSD(C) compliance assessment requirements, including the unique requirements based on the program's business capabilities. The requestor completes the program assessment of (1) architecture and programmatic information required by the [BMMP Comptroller Compliance Certification Criteria](#) and the applicable Domain(s) unique compliance assessment requirements, and (2) an evaluation of the program's proposed implementation plan against Component, and BMMP transition plans to ensure compatibility.
3. The Lead Business Domain, in coordination with applicable Partner Domains, reviews and validates the documentation for consistency with the Department's/Domain's business processes and management objectives. Based on this review, the Lead Business Domain will determine one of the following:
 - The program/initiative is compliant and there are no compliance issues;
 - The program/initiative is compliant but not required since duplicate of other initiatives;

- The program/initiative is non-compliant but acceptable because the Domain(s) determine that mitigations exist to resolve identified issues; or
- The program/initiative is non-compliant, and the Domain(s) will not certify based on non-compliance with BEA/Domain architectures, transition plans, incomplete documentation, or unacceptable issue resolution/mitigation.

4. After coordination and content concurrence between the Business Domains, the Lead Domain forwards the certification package to the BMSI Program Office for evaluation.

5. BMSI, working in consultation with the Domains, reviews the certification package to ensure that it is complete, addresses cross-domain impacts, and supports the Department's enterprise business objectives.

6. BMSI provides a recommendation memorandum, through the Deputy Chief Financial Officer, to the USD (Comptroller) to approve or deny the Program/Initiative. (If BMSI does not recommend certification, BMSI will work with the applicable Domain Owner to resolve issues.)

7.7.4. Comptroller Compliance Certification Criteria

The Comptroller Compliance Certification Criteria are 26 questions that were approved by the BMMP Steering Committee. Certification Decision Packages submitted to obtain USD(C) approval must include the answers to these questions. The answers are generally originated by the program office or the functional proponent within the DoD Component, are validated by the Lead and Partner Business Domain(s), and results of their evaluation are submitted to the BMSI as part of the Certification Decision Package. Examples of the 26 questions include 14 general questions on the program (e.g., Component owner, Program Manager, User Base, Acquisition Type), compliance status with various DoD and Congressional Mandates (e.g., [Clinger-Cohen Act](#) and [DoD Information Technology Security Certification and Accreditation Process \(DITSCAP\)](#)), transition planning (interfacing and sunsetting systems and dates), and the Business Domain(s) evaluation of soundness of the program (the economic analysis results and compliance with the BEA and Domain architectures). The 26 questions are available through a link to the [BMMP Portal](#) on the [System Compliance tab of the BMMP Home Page](#). A user ID and password are required to access the portal and can be obtained by registering online.

7.7.5. Definitions

The following definitions are taken from the [Office of Management and Budget Circular A-127 Revised](#):

The term "financial system" means an information system, comprised of one or more applications, that is used for any of the following:

- collecting, processing, maintaining, transmitting, and reporting data about financial events;
- supporting financial planning or budgeting activities;
- accumulating and reporting cost information; or
- supporting the preparation of financial statements.

A financial system supports the financial functions required to track financial events, provide financial information significant to the financial management of the agency, and/or required for the preparation of financial statements. A financial system encompasses automated

and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. A financial system may include multiple applications that are integrated through a common database or are electronically interfaced, as necessary, to meet defined data and processing requirements.

The term "non-financial system" means an information system that supports non-financial functions of the Federal government or components thereof and any financial data included in the system are insignificant to agency financial management and/or not required for the preparation of financial statements.

The term "mixed system" means an information system that supports both financial and non-financial functions of the Federal government or components thereof.

The term "financial management systems" means the financial systems and the financial portions of mixed systems necessary to support financial management.

7.8 CLINGER-COHEN ACT

7.8.1. The Clinger Cohen Act

7.8.1.1. Purpose

This section assists program managers, domain managers and members of the joint staff to understand and comply with the Clinger Cohen Act (CCA). This section is organized into the key requirements of CCA that must be met in order to receive milestone approval. For a more detailed background and comprehensive guidance, please access the CCA Community of Practice.

7.8.1.2. CCA Background

[The Information Technology Management Reform Act](#), now known as the Clinger-Cohen Act of 1996, is designed to improve the way the Federal Government acquires and manages information technology. It requires the Department and individual programs to use performance based management principles for acquiring information technology (IT), including National Security Systems (NSS).

The CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing acquisition of IT, including NSS; it elevated oversight responsibility to the Director, OMB, and established and gave oversight responsibilities to the departmental CIO offices. In DoD, the ASD(NII) has been designated as the DoD CIO and provides management and oversight of all DoD information technology, including national security systems.

7.8.1.3. Definitions

The term “information technology,” with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. “Information technology” does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract

The term “National Security System” (NSS) means any telecommunications or information system operated by the United States Government, the function, operation, or use of which, (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command and control of military forces; (d) involves equipment that is an integral part of a weapon or weapons system; or (e) is critical to the direct fulfillment of military or intelligence missions.

7.8.2. Mandatory Policies

Table 13 details CCA Compliance regulatory requirements, mandatory DoD policy and the applicable program documentation that can be used to fulfill the requirement. This table instantiates information from the [DoD Instruction 5000.2 CCA Compliance Table \(Table E4.T1\)](#), reorders the content to provide for a more logical flow, and adds columns relating applicable milestones and regulatory guidance with each of the requirements.

To navigate via hyperlinks, go to the CCA Requirements table and select the appropriate hyperlink to get to guidance information. Some CCA requirements are discussed only briefly, and then are hyperlinked to a more complete discussion. Additionally, some of the more detailed requirements will have links to the [CCA Community of Practice website](#) which provides more comprehensive understanding of the CCA requirements, their rationale, the associated policy documents, best practices, and lessons learned.

Paragraphs following the table will describe each requirement. Some paragraphs will identify who is responsible for fulfilling and reviewing the requirement, and suggest how the requirement is to be fulfilled. Others will briefly describe the requirement and provide a link to a detailed discussion contained elsewhere.

Requirements From the DoDI 5000.2 Clinger-Cohen Act (CCA) of 1996 Table (DoDI Table E4.T1.)			
Information Requirements	Applicable Program Documentation **	Applicable Milestone ****	Regulatory Requirement
***Make a determination that the acquisition supports core, priority functions of the Department	ICD Approval	Milestone A	CJCSI 3170.01
*No Private Sector or Government source can better support the function	AoA(FSA) page XX Acquisition Strategy page XX, para XX	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
*** Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology	Approval of the ICD, Concept of Operations, AoA (FSA), CDD, and CPD	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
*An analysis of alternatives has been conducted	AoA (FSA)	Milestone A	CJCSI 3170.01 DoDI 5000.2
*An economic analysis has been conducted that includes a calculation of the return on investment; or for non-AIS programs, a Life-Cycle Cost Estimate (LCCE) has been conducted	Program LCCE Program Economic Analysis for MAIS	For MAIS: Milestone A & B, & FRPDR (or their equivalent) For non-MAIS: Milestone B or the first Milestone that authorizes contract award	DoDI 5000.2
***Establish outcome-based performance measures linked to strategic goals.	ICD, CDD, CPD and APB approval	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
There are clearly established measures and accountability for program progress	Acquisition Strategy page XX APB	Milestone B	DoDI 5000.2
The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards	ICD, CDD, & APB (NR-KPP) ISP (Information Exchange Requirements)	Milestone A, B & C	CJCSI 6212.01 DoDI 5000.2
The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Information Assurance Strategy	Milestone A (MAIS), B, FRPDR or equivalent	DoDI 5000.2 DoDI 8500.1
To the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments	Acquisition Strategy page XX	Milestone B or the first Milestone that authorizes contract award	DoDI 5000.2
The system being acquired is registered	Registration Database	Milestone B, Update as required	DoDI 5000.2

* For weapons systems and command and control systems, these requirements apply to the extent practicable ([40 U.S.C. 1451](#))

** The system documents/information cited are examples of the most likely but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited.

***These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command and Control Systems that are not themselves IT systems

**** The purpose of the “Applicable Milestone” column in the table above is to indicate at which Milestone(s) the initial determination should be made regarding each element of Clinger-Cohen Act implementation. For MAIS programs, the DoD CIO must certify CCA compliance before granting approval for Milestone A or B or the Full-Rate Deployment decision (or their equivalent).

Table 13. Requirements from DoD Instruction 5000.2, Table E4.T1., CCA Compliance Table

Two other CCA-related topics not addressed in the CCA table in DoDI 5000.2 are Post-Implementation Review (PIR)/Post Deployment Performance Review (PDPR) and CCA certifications and notifications to Congress required by [Section 8084\(c\) of the Appropriations Act for FY 2004 \(Public Law 108-87\)](#).

See [section 7.9](#) of this Guidebook for a discussion of PIR/PDPR.

See [section 7.8.3.12](#) of this Guidebook for a discussion of certifications and notification required by Section 8084(c) of the Appropriations Act for FY 2004 (Public Law 108-87).

7.8.3. Guidance for Complying with the CCA

This section details guidance associated with the CCA Information Requirements listed above. Each section provides an overview of the requirement. Some sections will provide additional guidance about the requirement, while other sections will have links to additional guidance contained in other parts of this Guidebook or to other resources located elsewhere on the web.

7.8.3.1. Determining that the Acquisition Supports the Core, Priority Functions of the Department

Overview: This element of the CCA asks if the function supported by a proposed acquisition is something the Federal government actually needs to perform; i.e., for DoD, is the function one that we (the DoD and/or its Components) must perform to accomplish the military missions or business processes of the Department?

For DoD, this question is answered in the [Joint Capabilities Integration and Development System \(JCIDS\)](#) process. Before a functional requirement or new capability enters the acquisition process, the JCIDS process (See [CJCSM 3170.01, Enclosure A](#)) requires the sponsor to conduct a series of analyses (i.e., the Functional Area Analysis, Function Needs Analysis and Functional Solution Analysis). These analyses are normally completed before preparing an Initial Capabilities Document (ICD). Ideally, these analyses will show that the acquisition supports core/priority functions that should be performed by the Federal Government. Moreover, the analysis should validate and document the rationale supporting the relationship between the Department's mission (i.e., core/priority functions) and the function supported by the acquisition.

Who is Responsible? The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the JCIDS process.

Implementation Guidance: Ensure that the JCIDS analytical work addresses the CCA question by establishing the linkage between the mission, the function supported, the capability gap and potential solutions. The following questions should be helpful in determining whether a program supports DoD core functions:

- Does the program support DoD core/primary functions as documented in national strategies and DoD mission and strategy documents like the Quadrennial Defense Review (QDR), Strategic Planning Guidance (SPG), Joint Operating Concepts (JOC), Joint Functional Concepts (JFC), Integrated Architectures (as available), the Universal Joint Task List (UJTL), domain mission statements, or Service mission statements?
- Does JCIDS (i.e., FAA/FNA/FSA) validate that the function needs to be performed by the Government?

- Is the program consistent with the goals, objectives, and measures of performance in the lead Sponsor/Domain owner's Functional Strategic Plan?

7.8.3.2. Determining That No Private Sector or Other Government Source Can Better Support the Function

Overview: This element of the CCA asks if any private sector or other government source can better support the function. This is commonly referred to as the "outsourcing determination." The Sponsor/Domain Owner determines that the acquisition MUST be undertaken by DoD because there is no alternative source that can support the function more effectively or at less cost. Note that for weapon systems and for command and control systems, the need to make a determination that no private sector or Government source can better support the function only applies to the maximum extent practicable. This requirement should be presumed to be satisfied if the acquisition has a Milestone Decision Authority-approved acquisition strategy.

Who is Responsible:

- The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the AoA(FSA) process.
- The PM updates and documents the supporting analysis in the AoA and a summary of the outsourcing decision in the Acquisition Strategy.

7.8.3.3. Redesigning the Processes that the Acquisition Supports

Overview: This element of the CCA asks if the business process or mission function supported by the proposed acquisition has been designed for optimum effectiveness and efficiency. This is known as Business Process Reengineering (BPR) and is used to redesign the way work is done to improve performance in meeting the organization's mission while reducing costs. The CCA requires the DoD Component to analyze its mission, and based on the analysis, revise its mission-related processes and administrative processes as appropriate before making significant investments in IT. To satisfy this requirement, BPR is conducted before entering the acquisition process. However, when the results of the JCIDS analysis, including the Analysis of Alternatives, results in a [Commercial-Off-The-Shelf \(COTS\)](#) enterprise solution, additional BPR is conducted after program initiation, to reengineer an organization's retained processes to match available COTS processes. As stated in [DoD Instruction 5000.2](#), for a weapon system with embedded information technology and for command and control systems that are not themselves IT systems, it shall be presumed that the processes that the system supports have been sufficiently redesigned if one of the following conditions exist: (1) the acquisition has a [Joint Capabilities Integration and Development System \(JCIDS\)](#) document (ICD, CDD or CPD) that has been approved by the Joint Requirements Oversight Council (JROC) or JROC designee, or (2) the Milestone Decision Authority determines that the Analysis of Alternatives (AoA) (Functional Solution Analysis (FSA)) is sufficient to support the initial Milestone decision."

Who is Responsible:

- The Sponsor/Domain Owner with cognizance over the function with input from the corresponding DoD Component functional is responsible for BPR.
- The PM should be aware of the results of the BPR process and should use the goals of the reengineered process to shape the acquisition.

- The OSD PA&E assesses an ACAT IAM program's AoA/FSA to determine the extent to which BPR has been conducted.
- The DoD CIO assesses an ACAT IAM program's AoA/FSA to determine whether sufficient BPR has been conducted.

Business Process Reengineering: Benchmarking

Benchmarking is necessary for outcome selection and business process reengineering (BPR). The Sponsor/Domain Owner should quantitatively benchmark agency outcome performance against comparable outcomes in the public or private sectors in terms of cost, speed, productivity, and quality of outputs and outcomes.

Benchmarking should occur in conjunction with a BPR implementation well before program initiation. Benchmarking can be broken into four primary phases:

- Planning Phase: Identify the product or process to be benchmarked and select the organizations to be used for comparison. Identify the type of benchmark measurements and data to be gathered (both qualitative and quantitative data types). One method to gather data is through a questionnaire to the benchmarking organization that specifically addresses the area being benchmarked.
- Data Collection and Analysis Phase: Initiate the planned data collection, and analyze all aspects of the identified best practice or IT innovation to determine variations between the current and proposed products or processes. Compare the information for similarities and differences to identify improvement areas. Use root cause analysis to break the possible performance issues down until the primary cause of the gap is determined. This is where the current performance gap between the two benchmarking partners is determined.
- Integration Phase: Communicate the findings; establish goals and targets; and define a plan of action for change. This plan of action is often the key to successful BPR implementation. Qualitative data from a benchmarking analysis is especially valuable for this phase. It aids in working change management issues to bring about positive change.
- Implementation Phase: Initiate the plan of action and monitor the results. Continue to monitor the product or process that was benchmarked for improvement. Benchmark the process periodically to ensure the improvement is continuous.

EXAMPLE

The Military Health System PEO Joint Medical Information Systems Office was faced with increasing cost and decreasing performance in their 20+ call centers that service 8.3 million military healthcare beneficiaries. To understand the industry standards for call center performance, the PEO staff approached the Gartner Group and the benchmarking services offered by Brady and Associates, a hospital management consultancy. A comparison of the as-is cost and performance with the industry benchmarks suggested that a business case could be made to reengineer the Military Health System call center process and realize both improved service and a significant ROI.

Following completion of the business case, a competitive solicitation was made for consolidated call and help desk services. This would be a performance based services contract

using performance measures developed from the benchmarking exercise. The award was made to IBM with incentivized performance metrics as shown in Table 14.

The contracting tool selected was a variation of a firm fixed price contract with established target and ceiling prices. Underruns below the target price and overruns between the target and ceiling price are shared in a ratio bid between the vendor and government. Of note is that this was the first such incentivized-shard risk contract based upon a GSA Schedule and now serves as a template for use by all government agencies.

The results of this reengineering have been dramatic. The consolidated call center is in San Antonio, Texas. Pre-consolidation cost for 20+ centers was \$25M. The current cost is \$10M per year and customer satisfaction for FY 03 was 98%.

Criteria	Positive Incentive range	Acceptable range	Negative Incentive range
Customer Satisfaction Survey Response Rate1	Above 18%	15 - 18 %	Below 15%
Customer Satisfaction1	Above 90%	85 - 90%	Below 85%
Call Abandonment Rate	Below 3%	3 - 5%	Above 5%
Average Speed of Answer (sec)	Below 20 sec.	20 – 30 sec.	Above 30 sec.
Problem Resolution Rate for High Priority problems/requests2	90 % within 60 minutes	89% within 90 min. <i>with hardware exception of 24 hour best effort repair/replace</i>	Greater than 90 min. for any problem
Problem Resolution Rate for Moderate Priority problems/requests2	75% within 4 hours	89% within in 6 hours <i>with hardware exception of 24 hour best effort repair/replace</i>	Greater than 6 hours for any problem
Problem Resolution Rate for Low Priority problems/requests2	50% with in 2 business days	89% with in 3 business days or less <i>with hardware exception of 24 hour best effort repair/replace</i>	Greater than 3 business days for any problem.
First Contact Resolution	Greater than 80%	64 to 80%	Less than 64%

Table 14. Consolidated Military Health System Calldesk Incentivized Performance Metrics

Additional BPR Resources:

- National Partnership for Reinventing Government Benchmarking site: <http://govinfo.library.unt.edu/npr/initiati/benchmk/>
- Best Manufacturing Practices site: <http://www.bmpcoe.org/>
- The Brady Group Call Center Benchmarking: <http://bradyinc.com>
- The Gartner Group: <http://www4.gartner.com/Init>
- BusinessRanks.com: <http://www.businessranks.com/call-centers.htm>

Implementation Guidance: BPR implementation guidance exists in both the private and public sector. In addition to the steps required to conduct a BPR, it is critical that the Sponsor/Domain Owners and Program Managers recognize change management as a key aspect of any successful BPR implementation. Two government sources recommended for BPR implementation guidance are the following:

1. The [BPR Internet Resources Kiosk](#): The BPR Internet Resources Kiosk site provides a set of links to BPR education, tools, and implementation guidance for BPR implementations. It includes a link to the [The DoD Process Innovation Site](#), which includes links to the [Turbo BPR tool](#) and the [BPR Fundamentals course](#).

2. The [General Accounting Office \(GAO\) BPR Guide](#): The GAO has developed a comprehensive framework for assessing BPR implementations that the Department of Defense can adopt to aid programs in conducting their BPR analysis. This framework involves three key parts <link>:

Part A: Assessing the Agency's Decision to Pursue Reengineering:

Part B: Assessing New Process Development

Part C: Assessing Project Implementation and Results

7.8.3.4. Analysis of Alternatives (Functional Solutions Analysis)

Overview: The Office of the Director, Program Analysis and Evaluation (OD/PA&E), provides basic policies and guidance associated with the AoA process. For [ACAT ID and IAM programs](#), OD/PA&E prepares the initial AoA guidance, reviews the AoA analysis plan, and reviews the final analysis products (briefing and report). After the review of the final products, OD/PA&E provides an independent assessment to the milestone decision authority ([see DoD Instruction 5000.2, Enclosure 6, E.6.5](#)). See [section 3.3](#) of this guide for a general description of the AoA and the AoA Study Plan..

7.8.3.5. Economic Analysis and Life-Cycle Cost Estimates

Overview: An Economic Analysis consists of a life-cycle cost and benefits analysis and is a systematic approach to selecting the most efficient and cost effective strategy for satisfying an agency's need. See [sections 3.6](#) and [3.7](#) of this guide for detailed EA and LCCE guidance. <link>.

7.8.3.6. Establish Outcome-based Performance Measures

Overview: The CCA requires the use of performance and results-based management in planning and acquiring investments in information technology, including national security systems (IT, including NSS). This section defines measurement terminology, relates it to DoD policy and provides guidance on formulating effective outcome-based performance measures for IT, including NSS investments. As stated in DoDI 5000.2, for a weapon system with embedded information technology and for command control systems that are not themselves IT systems, it shall be presumed that the acquisition has outcome-based performance measures linked to strategic goals if the acquisition has a JCIDS document (ICD, CDD or CPD) that has been approved by the JROC or JROC designee.

IT, including NSS outcome-based performance measures are also referred to as measures of effectiveness (MOEs). For clarification, the various uses and DoD definitions of MOEs are provided on the [CCA Community of Practice](#). Regardless of the term used, the Clinger Cohen Act states that the respective Service Secretaries shall:

- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology.

- Ensure that performance measurements are prescribed for information technology programs used by or to be acquired for the executive agency and that the performance measurements measure how well the information technology supports programs of the executive agency.
- Conduct post-implementation reviews of information systems to validate estimated benefits and document effective management practices for broader use.

In summary, we are obligated to state the desired outcome, develop and deploy the solution, and then measure the extent to which we have achieved the desired outcome. For further discussion, see the CCA language in page 24 of [Circular No.A-11, Part 7](#), Section 300, Exhibit 300, Part I, Section I.C. Additionally discussions on the statutory basis [<link>](#) and regulatory basis for MOEs and their verification [<link>](#) are available.

Who is Responsible:

- The Sponsor/Domain Owner with cognizance over the function develops the MOEs as part of the JCIDS process. This individual should ensure the MOEs are outcome-based and relate to the outcomes identified as benefits in the benefits analysis.
- The PM should be aware of the MOEs and how they relate to overall program effectiveness and document these MOEs in the Exhibit 300 that is part of DoD's budget submission to OMB.
- The DoD CIO assesses the outcome-based measures in deciding whether to certify CCA compliance for ACAT IA programs.

Implementation Guidance: This section is written to help the functional proponent prepare the MOEs and to help the PMO understand his/her role in the MOE refinement process. The key to understanding and writing MOEs for IT, including NSS investments is to recognize their characteristics and source. Therefore, MOEs should be:

- Written in terms of desired outcomes
- Quantifiable
- A measure of the degree to which the desired outcome is achieved
- Inclusive of both DoD Component and enterprise performance benefits
- Independent of any solution and should not specify system performance or criteria

To satisfy the requirement that an MOE be independent of any solution and not specify system performance or criteria, the MOE should be established before the Concept Decision that starts the acquisition process. The MOEs guide the analysis and selection of alternative solutions that are discussed in the AoA/FSA during pre-Milestone A. Although the MOE may be refined as a result of the analysis undertaken during this phase, the source of the initial mission/capability MOE is the functional community. The MOE is the common link between the ICD, the AoA and the benefits analysis.

A primer for this section is found in the [Performance Institute's Government Performance Logic Model](#). The Performance Institute is a private think tank that has developed a logical chain of events that they view as a blueprint for mission achievement. For further guidance on MOEs, see the Information Technology Community of Practice [Measures of Effectiveness Area](#) which contains the following additional guidance:

- JCIDS MOE Development Process

- BEA Domain MOE Development Process

7.8.3.7. Acquisition Performance Measures

Overview: Acquisition performance measures are clearly established measures and accountability for program progress. The essential acquisition measures are those found in the acquisition program baseline (APB): cost, schedule and performance. See [section 2.1.1](#), of this guide for detailed APB guidance.

7.8.3.8. The acquisition is consistent with the Global Information Grid policies and architecture

Overview: The GIG is the organizing and transforming construct for managing information technology (IT) for the Department. See [section 7.2](#), Global Information Grid (GIG), for a detailed guidance on GIG policies and architecture.

7.8.3.9. The program has an information assurance strategy that is consistent with DoD policies, standards and architectures

Overview: Information Assurance (IA) concerns information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities. See [section 7.5](#) of this guide for detailed guidance on IA.

7.8.3.10. Modular Contracting

Overview: Under modular contracting, a system is acquired in successive acquisitions of interoperable increments. The CCA is concerned with modular contracting to ensure that each increment complies with common or commercially acceptable standards applicable to Information Technology (IT) so that the increments are compatible with the other increments of IT comprising the system.

Who is Responsible:

- The program manager is responsible for ensuring that modular contracting principles are adhered to.
- The contracting strategy is addressed in the Acquisition Strategy, which is approved by the MDA and reviewed by all IIPT members.

Implementation Guidance: See [section 4.5.4](#), of this guide for a discussion of Modular, Open Systems Approach as a systems engineering technique that will support modularity, , and [section 39.103 of the Federal Acquisition Regulations](#) for a detailed discussion of Modular Contracting.

7.8.3.11. DoD Information Technology (IT) Registry

Overview: The [DoD Information Technology Registry](#) supports the CCA inventory requirements and the capital planning and investment processes of selection, control, and evaluation. The Registry contains a comprehensive inventory of the Department's mission critical and mission essential national security systems and their interfaces. It is web-enabled to .mil users, and has classified and unclassified portions accessible through NIPRNET and SIPRNET. [Department of Defense Information Technology \(IT\) Registry Policy Guidance for](#)

[2004](#), dated December 1, 2003 establishes Registry responsibilities to include update and maintenance of information in the Registry.

Who is Responsible: The Program Manager is responsible for ensuring the system is registered and should follow applicable Component CIO procedures and guidance.

IT Registry Update Procedure: The DoD Information Technology Registry uses a standard, documented procedure for updating its contents. Updates to the Registry are required on a quarterly basis. The rules, procedures, and protocols for the addition, deletion, and updating of system information are available to users once they are registered. Service and Agency CIOs confirm the accuracy of its contents on an annual basis.

Use of the IT Registry for Decision Making: The Registry has recently expanded its support to decision makers managing IT assets. In support of the Federal Information Systems Management Act and the Privacy Act additional fields have been added to the Registry. The Registry also supports the Comptroller's Business Management Modernization Program by providing baseline data on mission critical and mission essential financial systems. Service and Agency CIOs determine the addition or deletion of mission critical and essential systems based on mission needs and ongoing investment decisions.

7.8.3.12. CCA Certification for MAIS Systems

Overview: [Section 8084\(c\) of the Appropriations Act for FY 2004 \(Public Law 108-87\)](#) requires the Department of Defense (DoD) Chief Information Officer (CIO) to provide a notification of certification report at each acquisition milestone that Major Automated Information Systems (MAIS) are being developed in accordance with Subtitle III of Title 40 of the United States Code (Formally the CCA of 1996).

Who is Responsible:

- The Program Manager is responsible for developing the initial notification of certification report and then delivering it to their component CIO.
- The Component CIO is responsible for submitting the Section 8084(c) CCA certification report to the DoD CIO.
- The DoD CIO certifies MAIS program CCA compliance to the congressional defense committees at each acquisition milestone

Implementation Guidance: Each DoD Component CIO certification must be accompanied by a notification report that shall include:

- A statement that the MAIS is being developed in accordance with Clinger-Cohen Act of 1996
- The funding baseline (prior year and FY 2004 – 2007 including Operational and Maintenance; Procurement, and Research, Development, Test and Evaluation)
- The milestone schedule (denoting milestones and the dates for the milestones already attained, and for future milestones) for each MAIS
- A succinct and clear description of efforts to accomplish each of the following:
 - Business Process Reengineering.
 - An analysis of alternatives.
 - An economic analysis that includes a calculation of the return on investment.

- Performance measures.
- An information assurance strategy consistent with the Department's Global Information Grid.

The [Section 8084\(c\)](#) certification report is due from the DoD Component CIO to the DoD CIO at the time of milestone decision request. If a certification and notification report has been previously submitted for the program and if there has been no change regarding a particular issue, then the response for that issue should simply state that there has been no change from the previous submission.

7.9 POST IMPLEMENTATION REVIEWS

7.9.1. Background

The [Government Performance and Results Act \(GPRA\)](#) requires that Federal Agencies compare actual program results with established performance objectives. In addition, the [Clinger-Cohen Act](#) requires that Federal Agencies ensure that performance measurements are prescribed for the information technology (IT) to be acquired, that these performance measurements measure how well the IT supports the programs of the Agency. ([5 U.S.C. 306](#); 40 U.S.C. 11313)

[DoD Instruction 5000.2, Table E3.T1.](#), refers to this information requirement as a Post-Deployment Performance Review (PDPR) and requires a PDPR for MAIS and MDAP acquisition programs at the Full-Rate Production Decision Review. DoDI 5000.2 cites both GPRA and the Clinger-Cohen Act as the basis for the requirement.

In addition, the Office of Management and Budget (OMB) has prescribed specific procedures for measuring how well acquired IT supports Federal Agency programs. [OMB Circular A-130](#) refers to this performance-measurement requirement for IT as a Post Implementation Review (PIR). The Office of the DoD General Counsel has made the determination that the PIR fully satisfies both GPRA and Clinger Cohen Act requirements.

As a result, within the Department of Defense, the PDPR and the PIR are essentially the same thing—they both assess actual system performance against program expectations.

To avoid confusion, the next change to DoDI 5000.2 will rename the PDPR. Since OMB Circular A-130 specifically calls the described performance assessment a PIR, the Instruction will use that term. DoDI 5000.2 will require the PIR for **MAIS and MDAP** programs. This section of Chapter 7 of the Defense Acquisition Guidebook will provide details of the expected information (to comply with statute) for any PIR.

In practice, a PDPR/PIR *Plan* will be required at the Full-Rate Production Decision Review, and the actual PIR will be conducted after IOC (if possible, before FOC).

Until the official DoDI 5000.2 change takes effect, the two terms, PDPR and PIR, may be used interchangeably. Both terms refer to the same process: the evaluation of how well actual program results have met established performance objectives for any acquisition program.

7.9.2. Overview

This section provides guidance on how to conduct a PIR for a system that has been fielded, and is operational in its intended environment. A PIR verifies the Measures of Effectiveness (MOEs) of the Initial Capabilities Document and answers the question, “*Did the Service/Agency get what it needed, per the ICD, and if not, what should be done?*”

Who is Responsible:

- The Sponsor/Domain Owner is responsible for articulating outcome-based performance measures in the form of measures of effectiveness.
- The Sponsor/Domain Owner is responsible for planning the PIR, gathering data, analyzing the data, and assessing the results.

- The PM is responsible for maintaining an integrated program schedule that facilitates the PIR on behalf of the Sponsor/Domain Owner.
- The PM is responsible for translating Sponsor/Domain Owner planning into specific PIR implementation events.

What is a PIR:

The PIR is not a single event or test. It is a sequence of activities that when combined, provide the necessary information to successfully compare actual system performance to program expectations. In some cases, these activities can take place over a long period of time. The list in Table 19 indicates that some PIR activities may be accomplished in the context of typical program acquisition activities or system operational processes.

•FOT&E Results	•Annual CFO Report
•Platform Readiness	•Mission Readiness
•CC Exercise	•ROI
•User Satisfaction	•War Games
•IA Assessments	•Lessons Learned

Table 15. Potential PIR Activities

7.9.3. PIR Within the Acquisition Life Cycle

The Sponsor/Domain Owner initially articulates high-level, outcome-based performance measures in the form of measures of effectiveness in the ICD. Development of the CDD, CPD, contract, and build specifications follows, each providing increasingly detailed performance outcomes. During integration and test, procedures called out in the [Systems Engineering Plan \(SEP\)](#) should verify compliance with the build specification. The [Test and Evaluation Master Plan \(TEMP\)](#) and associated test products describe verification of compliance with the contract specification during [developmental test and evaluation \(DT&E\)](#) and verification of compliance with the CPD during [operational test and evaluation \(OT&E\)](#). Finally, the PIR benefits analysis evaluates system compliance with the original MOEs documented in the ICD.

7.9.4. PIR Implications for Evolutionary Acquisition

PIRs provide important user feedback and consequently are a fundamental element of evolutionary acquisition. Optimally, we need to understand how well a recently completed increment meets the needs of users before finalizing the requirements for a subsequent increment. The opportunity for such feedback depends on the level of concurrency in the schedule.

Additionally, changes in the environment may drive new requirements. The PIR gives both the Sponsor and the program manager empirical feedback to better understand any issues with the completed increment. This feedback enables the acquisition principals to adjust or correct the CDD/CPD for subsequent increments.

7.9.5. PIR Implementation Steps

1. Schedule the PIR. The PIR should take place post-IOC, after a relatively stable operating environment has been established. A typical time frame is 6 to 12 months after IOC.

2. Assemble a PIR Team. The PIR team should include:

- Functional experts with detailed knowledge of the capability or business area and its processes.
- User representatives, CIO representatives, functional sponsors, and Domain Owners.

3. Assemble and Review Available Information Sources. Data can be gleaned from operations conducted in wartime and during exercises. The lead-time for most major exercises is typically one year and requires familiarity with the exercise design and funding process.

Additional sources to consider are:

- Economic calculations to establish the payback period and ROI of business systems (if applicable).
- Qualitative assessments related to expected benefits
- Combatant Commander operational, logistics, and exercise data
- Information Assurance assessments
- Annual CFO Reporting of IT investment measured performance
- Stakeholder satisfaction surveys

4. Conduct the PIR. The PIR should be carried out according to the PIR planning that was reviewed and approved at Full Rate Production Decision Review. Care should be given to ensuring that accurate raw data is captured, and it can be later used for analysis. Based on the PIR plan, the PIR should, at a minimum, address:

- Customer Satisfaction: Is the warfighter satisfied that the IT investment meets their needs?
- Mission/Program Impact: Did the implemented system achieve its intended impact?
- Return on investment calculations, if applicable. Compare actual project costs, benefits, risks, and return information against earlier projections. Determine the causes of any differences between planned and actual results.

5. Conduct the Analysis. The analysis portion of the PIR should answer the question, “Did we get what we needed?” This provides a contrast to the test and evaluation measurements of KPPs that answer the question, “Did we get what we asked for?” This would imply, if possible, that the PIR should assess the extent to which the DoD’s investment decision-making processes were able to capture the warfighter’s initial intent. The PIR should also address, if possible, whether the warfighter’s needs changed during the time the system was being acquired.

The outputs of the analysis become the PIR findings. The findings should clearly identify the extent to which the warfighter got what they needed.

6. Prepare a Report and Provide Recommendations. Based on the PIR findings, the PIR team should prepare a report and make recommendations that can be fed back into the capabilities and business needs processes. The primary recipient of the PIR report should be the Sponsor/Domain Owner who articulated the original objectives and outcome-based performance measures on which the program or investment was based. The results of the PIR can aid in

refining requirements for subsequent increments. Recommendations may be made to correct errors, improve user satisfaction, or improve system performance to better match warfighter/business needs. The PIR team should also determine whether different or more appropriate outcome-based performance measures can be developed to enhance the assessment of future spirals or similar IT investment projects.

For further guidance on PIRs, see the Information Technology Community of Practice [Post Implementation Review Area](#). This contains the following additional guidance:

- [PIR Measurement Framework](#).
- [Common Problems with PIR Implementations](#).

7.9.6. PIR Further Reading

Both government and the commercial sector address the practice of conducting PIRs for materiel, including software and IT, investments. The GAO and several not-for-profit organizations have written on the subject of measuring performance and demonstrating results. The [CCA Community of Practice PIR area](#) lists a number of key public and private sector resources that can be used in planning and conducting a PIR.

7.10 COMMERCIAL, OFF-THE-SHELF, SOFTWARE SOLUTIONS

7.10.1. The Impetus for Commercial, Off-the-Shelf (COTS) Solutions

- The goal of the [President's Management Agenda](#) and the Department's [Quadrennial Defense Review \(QDR\)](#) is rapid transformation by significantly increasing, where appropriate, the use of commercially available and proven business solutions in the conduct of DoD business.
- One of the Department's goals is to migrate to COTS solutions to fill Information Technology capability gaps.
- The [Clinger-Cohen Act of 1996](#), DoD Instruction 5000.2, Sections [3.5.3.](#) and [3.6.4.](#), and Management Initiative Decision (MID) 905, "Net-Centric Business Transformation and E-Government," all require the use of COTS Information Technology solutions to the maximum practical extent.

7.10.2. Definition

Commercial Off-the-Shelf (COTS) is defined as "commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency."

[From the [Eleventh Edition of GLOSSARY: Defense Acquisition Acronyms and Terms.](#)]

7.10.3. Mandatory Policies

The following bullets quote or paraphrase sections in the DoD 5000 series that specifically address Commercial Off-the-Shelf (COTS):

- [DoD Directive 5000.1, Section E1.18.](#), states the following:
*"... The DoD Components shall work with users to define capability needs that facilitate the following, listed in descending order of preference:
E1.18.1. The procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies;"*
Hence, commercially available products, services, and technologies are a first priority for acquisition solutions.
- [DoD Instruction 5000.2, Section 3.5.3.](#), states that "existing commercial off-the-shelf (COTS) functionality and solutions drawn from a diversified range of large and small businesses shall be considered," when conducting the Analysis of Alternatives.
- [DoD Instruction 5000.2, Enclosure 4, "IT Considerations," Table E4.T1., "CCA Compliance Table."](#) requires that, to be considered CCA compliant, the Department must redesign the processes being supported by the system being acquired, to reduce costs, improve effectiveness and maximize the use of COTS technology.
- [DoD Instruction 5000.2, Enclosure 4, "IT Considerations," Section E4.2.7.](#), states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made."

7.10.4. Modifying Commercial Off-the-Shelf (COTS) Software—Reuse Custom Components

It is important to note that modifying the core code of a COTS product should be avoided. It is possible to add code to the existing product, to make the product operate in a way it was not intended to do ‘out-of-the-box.’ This, however, significantly increases program and total life cycle costs, and turns a commercial product into a DoD-unique product. The business processes inherent in the COTS product should be adopted, not adapted, by the organization implementing the product. Adopting a COTS product is done through business process re-engineering. This means the organization changes its processes to accommodate the software, not vice versa. In many cases there will be a few instances where business process re-engineering is not possible. For example, due to policy or law, it may be necessary to build or acquire needed reports, interfaces, conversions, and extensions. In these cases, adding to the product must be done under strong configuration control. In cases where a particular COTS product does not provide the entire set of required functionality, a ‘bolt-on’ could be used. A bolt-on is not part of the COTS software product, but is typically part of a suite of software that has been certified to work with the product to provide the necessary additional functionality. These suites of software are integrated together to provide the full set of needed functionality. Using a ‘bolt-on,’ however, increases program and total life cycle costs.

Once an individual program or project develops a report, interface, conversion, or extension object, or acquires a ‘bolt-on’ capability, it should be possible for other efforts to share and reuse the solution. An initial operating capability for a repository of these custom software components is now available. It can be accessed via the Reports, Interfaces, Conversions, Extensions Repository in the [Enterprise Integration Toolkit](#) . This repository can help adapt COTS products for DoD use and reuse.

See [section 7.10.6.3](#). for a more detailed discussion of reports, interfaces, conversions, and extensions.

7.10.5. Commercial Off-the-Shelf (COTS) Integration into the Acquisition Life Cycle

The actions below are unique to acquiring COTS Information Technology solutions. These activities should occur within a tailored, responsive, and innovative program structure authorized by [DoD Instruction 5000.2](#). The stakeholder primarily responsible for each action is shown at the end of each bullet.

7.10.5.1. Before Milestone A

- Define strategy and plan for conducting [business process re-engineering](#) during Commercial Off-the-Shelf (COTS) software implementation phase of the program. (Domain Owner/Principal Staff Assistant)
- Consider COTS and business process re-engineering when developing the Analysis of Alternatives/Functional Solution Analysis. (See sections [3.3](#). and [7.8.3.4](#). of this guidebook). (Domain Owner/Principal Staff Assistant)
- Consider commercially available products, services, and technologies when defining initial user needs in the [Initial Capabilities Document](#). (Domain Owner/Principal Staff Assistant)

- When developing the [Technology Development Strategy](#) and/or the [Acquisition Strategy](#), consider commercial best practice approaches and address the rationale for acquiring COTS. (Program Manager)
- Consider the Initiation and Acquisition best practices available in the [Enterprise Integration Toolkit](#) when contracting for the COTS product and the system integrator (if required). (Domain Owner/Principal Staff Assistant and Program Manager)

7.10.5.2. Before Milestone B

- To the maximum extent possible, [redesign business processes](#) to conform to the best practice business rules inherent in the Commercial Off-the-Shelf product. Define a process for managing and/or approving the development of reports, interfaces, conversions, and extensions. (See the [Enterprise Integration Toolkit](#) for best practices in the methodologies and techniques to be successful in this phase.) (Domain Owner/Principal Staff Assistant and Program Manager)
- Consider the Implementation, Preparation, and Blueprinting best practices available in the Enterprise Integration Toolkit. (Domain Owner/Principal Staff Assistant and Program Manager)

7.10.5.3. Before Milestone C or Full Rate Production Decision Review

- Ensure scope and requirements are strictly managed and additional reports, interfaces, conversions, and extensions objects are not developed without prior authorization. (Program Manager)
- Consider best practices in the [Enterprise Integration Toolkit](#) regarding the implementation phase of the Commercial Off-the-Shelf effort. (Program Manager)
- Ensure adequate planning for life-cycle support of the program. See section 3.4, Engineering for life-cycle support, of [“Commercial Item Acquisition: Considerations and Lessons Learned”](#).

7.10.5.4. After Milestone C or Full Rate Production Decision Review

- Conduct ongoing engineering and integration for sustainment activities throughout the lifecycle of the program.

7.10.6. Best Practices, Tools, and Methods

Various methodologies, toolsets, and information repositories have been developed to assist the Program Manager in the implementation of COTS software-based programs. The remainder of this section provides the Program Manager descriptions of best practices, available tools and methods, and critical success factors for use in the acquisition of commercially-based solutions. Additionally, [Chapter 4](#) of this Guidebook, *Systems Engineering*, presents a complete discussion of applicable systems engineering practices, to include a discussion of the [Modular, Open Systems Approach](#).

7.10.6.1. DoD Enterprise Software Initiative

The [DoD Enterprise Software Initiative](#) is a joint project designed to implement a software enterprise management process within the Department of Defense. By pooling commercial software requirements and presenting a single negotiating position to leading software vendors, the Enterprise Software Initiative provides pricing advantages not otherwise available to

individual Services and Agencies. The Enterprise Software Initiative can use the Defense Working Capital Fund to provide “up-front money” for initial wholesale software buys. This funding process assures maximum leverage of the combined buying power of the Department of Defense, producing large software discounts. Agreement negotiations and retail contracting actions are performed by information technology acquisition and contracting professionals within participating DoD Services and Agencies, as Enterprise Software Initiative “Software Product Managers.” The [DoD Enterprise Software Initiative](#) Home Page lists covered products and procedures, and also shows [Defense Federal Acquisition Regulation Supplement Subpart 208.74](#) and [DoD Instruction 5000.2, E4.2.7](#), requirements for compliance with the DoD Enterprise Software Initiative.

The [DoD Business Initiative Council](#) endorsed the Enterprise Software Initiative and provided DoD Service funding to develop a DoD-wide Software Asset Management Framework. The Council authorized Business Initiative Council Initiative IT11 to extend Software Asset Management to the DoD Component level. The Business Initiative Council also approved extension of the project to establish a [Virtual Information Technology Marketplace](#) for online purchasing of Information Technology.

7.10.6.2. SmartBUY

[SmartBUY](#) is a federal government-wide commercial software asset management and enterprise-licensing project developed by the General Services Administration in coordination with the Office of Management and Budget.

Its purposes are (a) to create a new, federal agency business process to manage commercial software as an asset, and (b) to obtain optimal pricing and preferred terms and conditions for widely used commercial software products. This effort was formally announced on June 2, 2003 in an [Office of Management and Budget memorandum](#) to the federal agencies.

The General Services Administration is the SmartBUY Executive Agent and leads the interagency team in negotiating government-wide licenses for software. The DoD Enterprise Software Initiative Team has been working closely with the SmartBUY project for several months, and has coordinated the initial SmartBUY commercial software survey response.

7.10.6.2.1. SmartBUY Implementation

The [DoD Enterprise Software Initiative](#) Team is developing policy to implement SmartBUY within the DoD. This policy will provide the framework for migrating existing Enterprise Software Initiative Enterprise Agreements to SmartBUY Enterprise Agreements. In the meantime, the [Office of Management and Budget memo](#) establishes requirements to be followed by federal departments and agencies. Specifically, federal agencies are to:

- Develop a migration strategy and take contractual actions as needed to move to the government-wide license agreements as quickly as practicable; and
- Integrate agency common desktop and server software licenses under the leadership of the SmartBUY team. This includes, to the maximum extent feasible, refraining from renewing or entering into new license agreements without prior consultation with, and consideration of the views of, the SmartBUY team.

7.10.6.2.2. SmartBUY Resource

Click here for the latest and most complete information about [SmartBUY](#).

7.10.6.3. Enterprise Integration Toolkit

The [Enterprise Integration Toolkit](#) provides program managers with a repeatable Commercial Off-the-Shelf (COTS) implementation process, a knowledge repository that incorporates both government and commercial industry best practices and lessons learned, and a Reports, Interfaces, Conversions, and Extensions (RICE) Repository. The objectives of the Enterprise Integration Toolkit are to assure cost savings within the program, to achieve program speed and efficiency, and to reduce program risk. A user ID and password is required and may be obtained by registering at the website..

The Toolkit is the single point of reference for COTS program product examples and templates, and contains a repository of Education & Training courses and lessons learned. Program managers should use the Enterprise Integration Toolkit to leverage proven approaches and lessons learned in the areas of program initiation, software and system integration services sourcing, contracting, implementation, education and training, information assurance/security, performance metrics and change management. The Toolkit enables program managers to leverage work already done, and to reduce the redundancy, effort, and costs associated with a COTS implementation. (Education & Training represents a significant portion of COTS implementation costs.)

The Enterprise Integration Toolkit also contains a repository of RICE development objects to be used by program managers to leverage work already done, and to reduce redundancy, effort, and costs of Commercial Off-the-Shelf (COTS) implementations. RICE objects represent a significant portion of COTS cost, not only in the initial development, but in on-going maintenance and updating.

During a COTS implementation, there are additional configuration, design, and/or programming requirements necessary to satisfy functional requirements and achieve the desired functionality. These requirements are not supported within the commercial, core functionality of the COTS product being implemented, and therefore require additional technical development. RICE objects represent the solution to these additional requirements.. This development (or reuse) of RICE objects enables the creation of unique Reports not standard in the product; the creation of Interfaces to external systems; the creation of Conversion programs to transfer data from an obsolete system to the new system; and the creation of Enhancements (or Extensions) to allow additional functionality to be added to the system without disturbing the core software code.

To ensure consistency across programs and within the RICE Repository, RICE is further defined as follows:

- Report - A formatted and organized presentation of data.
- Interface - A boundary across which two independent systems meet and act on or communicate with each other.
- Conversion - A process that transfers or copies data from an existing system to load production systems.
- Extension - A program that is in addition to an exiting standard program but that does not change core code or objects.

The Enterprise Integration Toolkit also includes a Concept of Operations that provides program managers with a process for leveraging the value of the RICE Repository. This process

describes how to take data from and how to provide data to the repository. It describes the timing for its use, and at what point and level approvals are to be obtained throughout the life cycle of a program.

Program managers should ensure vendors include these repositories in their implementation methodologies. The Enterprise Integration Toolkit's software and systems integration acquisition and contracting processes contain boilerplate language for program managers to use in acquisition documents.

For more detail or additional definitions, to review the CONOPS, or to download the Enterprise Integration Toolkit, go to <http://www.eitoolkit.com>.

7.10.6.4. Commercial Off-the-Shelf (COTS) Testing

On June 16, 2003, the Director, Operational Test and Evaluation, signed a memorandum issuing the "[Guidelines for Conducting Operational Test and Evaluation \(OT&E\) for Software-Intensive System Increments](#)." The guidelines help streamline and simplify COTS software testing procedures. They assist in tailoring pre-deployment test events to the operational risk of a specific system increment acquired under OSD oversight. For increments that are of insignificant to moderate risk, these guidelines streamline the operational test and evaluation process by potentially reducing the degree of testing. Simple questions characterize the risk and environment upon which to base test decisions, for example, "If the increment is primarily COTS, non-developmental items, or government off-the-shelf items, what is the past performance and reliability?"

7.10.6.5. Commercial Off-the-Shelf (COTS) Lessons Learned

As the Department migrates to COTS, the workforce should be educated and trained in COTS software best practices. The objective is to raise the awareness of what is going on in the Government and in the commercial sector relative to the use of COTS software. Best practices and lessons learned should be swiftly imported into DoD and used to improve program outcomes. The **attached briefing** provides a set of Air Force lessons learned that can be applied generally across the Department. Another good source of lessons learned is the [Carnegie Mellon University COTS-based systems lessons learned web site](#). As indicated earlier, the [Enterprise Integration Toolkit](#) also contains a section on lessons learned.