INFORMATION TECHNOLOGY ACQUISTIONS

Program Attorneys Acquisition Oversight Course
Defense Acquisition University

August 19, 2010

MaryAnn Engelbert, Associate Director, Cowan & Associates

Objective

To attain basic knowledge of the primary laws and regulations that govern Information Technology Acquisition Program Management Office functions, challenges, and processes involved in fielding IT capabilities in the Department of the Navy.

Agenda

- Important Definitions
- Statutes & Regulations:
- Information Technology (IT) System Statutes
- Major Automated Information Systems (MAIS)
- Clinger Cohen Act (CCA)
- DoDI 5000.02, Enclosure (5)

Important Definitions

(Page 1 of 12)

"Information Technology"

"(A) with respect to an Executive Agency means **any equipment** or interconnected system or subsystem of equipment, **used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display,** switching, interchange, **transmission, or reception** of data or **information by the 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 that requires the use:**

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

"(B) **includes computers, ancillary equipment** (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), **peripheral equipment designed to be controlled by the central processing unit** of a computer, software, firmware and similar procedures, **services (including support services)**, and related resources; but

"(C) does not include any equipment acquired by a federal contractor incidental to a federal contract."

Source: Clinger Cohen Act/40 U.S.C. §11101

Important Definitions

(Page 2 of 12)

Plain English: CCA defines IT to mean any computer hardware, software, equipment, or *services* used to process information by or for the government, including:

- Transmission,
- Receipt,
- Storage,
- Compilation,
- Analyzing, or
- Processing

IT Practice Tip: CCA IT definition includes "support services" required to design, develop, accredit, operate and sustain an agency information system .

Important Definitions

(Page 3 of 12)

"National Security System" (NSS)

A telecommunications or information system operated by the Federal 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) except for systems used for routine administrative and business applications, is critical to the direct fulfillment of military or intelligence missions.

Historical Note: Identical to definition used by Warner Amendment (prior to 1996) for exemption from Federal Information Processing (FIP) requirements.

Source: CCA/40 U.S.C. §11103

Important Definitions

(Page 4 of 12)

NSS Practice Tips:

NSS determinations are made by DOD/DON authorities to identify acquisition programs for which specific IT rules or requirements may be followed to the "extent practicable" or not at all.

NSSs are not addressed consistently in statute, for example:

- NSSs are specifically excluded from the definition of IT in the Paperwork Reduction Act (PRA). See 44 U.S.C. § 3502(9).
- NSSs are specifically defined as IT in the CCA. 40 U.S.C. § 11103 explains how the CCA applies to NSS.

The following CCA requirements apply to NSS "to the extent practicable":

- Capital Planning
- Performance and Results Based management
- Information Technology Standards & Best Practices
- Process Reengineering

NSSs are exempt only from the CCA requirement for designated contracting.

Important Definitions

(Page 5 of 12)

"Information System" ("IS"):

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Source: Paperwork Reduction Act/40 U.S.C. §3502(8)

IS Practice Tips:

- An, IS, as defined, has been interpreted to include hardcopy, hand developed and managed lists, files, tables, notes, or any other compiled set of information used by Federal personnel.
- The term "Automated Information System" (AIS) is not defined by the United States Code.

Important Definitions

"Automated Information System" (AIS):

A system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information.

Source: DODI 5000.02

Excluded are computer resources that are:

a. **an integral part of a weapon or weapon system;**
b. used for highly sensitive classified programs;
c. used for other highly sensitive information technology programs; or
d. **determined by the Under Secretary of Defense for Acquisition Technology & Logistics (USD (AT&L) or designee to be better overseen as a non-AIS program** (e.g., a program with a low ratio of Research, Development, Test and Evaluation (RDT&E) funding to total program acquisition costs development).

Source: DoDI 5000.02, Table 1, note 3

Important Definitions

(Page 7 of 12)

"Information Technology Services":
The performance of any work related to IT and the operation of IT, including NSS including outsourced IT-based business processes, outsourced IT, and outsourced information functions.

Source: DoDI 5000.02, Enclosure 9

"Defense Business Systems":
An information system, other than an National Security System, operated by, for, or on behalf of the DoD, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management."

Source: Title 10 U.S.C. Section 2222

Important Definitions

(Page 8 of 12)

"Major Defense Acquisition Program" (MDAP):

A DOD acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and--

(1) that is **designated by the Secretary of Defense as a MDAP; or**

(2) that is **estimated by the USD(AT&L) to require an eventual total expenditure for RDT&E of more than $365 million in Fiscal Year (FY) 2000 constant dollars or, for Procurement, of more than $2.19 billion in FY '00 constant dollars.**

Historical Note: MDAPs were the originally the acquisition term for large Weapons Systems programs and were managed separately from Federal Information Processing (FIP) programs.

Source: 10 U.S.C. §2430

Important Definitions

(Page 9 of 12)

Practice Tips:

DoDI 5000.01, Table 1 authorizes Milestone Decision Authority (MDA) designation of "**MDAP" based on "Special Interest,"** so that it may be managed as an MDAP for DoD oversight but not for Congressional reporting purposes.

Only "investment dollars" appropriated by Congress (e.g., RDT&E, Ship Conversion Navy (SCN), Aircraft Procurement Navy (APN), Weapon Procurement Navy (WPN), Other Procurement Navy (OPN), and Marine Corps Procurement (MCP)) are included in estimating program costs for determining MDAP dollar thresholds.

Operations & Maintenance Navy (O&MN) dollars and Foreign Military Sales (FMS) dollars are not included in program costs for purposes of determining MDAP dollar thresholds.

Important Definitions

(Page 10 of 12)

"Major Automated Information System" (MAIS):
A DoD program for the acquisition of an AIS (either as a product or a service) if--

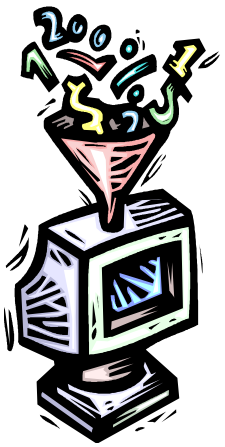
(1) the program is **designated by the Secretary of Defense, or a designee** of the Secretary, **as a MAIS program; or**

(2) the **dollar value of the program is estimated to exceed--**

(A) **$32,000,000** in FY '00 constant dollars **for all program costs in a single fiscal year;**

(B) **$126,000,000** in FY '00 constant dollars for **all program acquisition costs for the entire program**; or

(C) **$378,000,000** in FY '00 constant dollars **for the total life-cycle costs of the program (including O&M costs).**



Source: 10 U.S.C. §2445a

Important Definitions

(Page 11 of 12)

Practice Tips:

- DoDI 5000.01, Table 1 authorizes MDA designation of a program as **a MAIS based on "Special Interest,"** so that it may be managed as a MAIS for DoD oversight but not for Congressional reporting.
- DoDI 5000.02, Table 1 requires **all dollars - regardless of the appropriation or fund source** – to be included in estimating whether a MAIS will reach the MDAP dollar thresholds.
- Currently, USD AT&L staff interprets 10 U.S.C. §2445d to mean that if an acquisition program meets the statutory definitions for both a MDAP and a MAIS, then USD AT&L may elect to manage that program only as an MDAP or only as a MAIS.
- USD AT&L decides whether a program that meets both MDAP and MAIS statutory definitions will be designated a MDAP or MAIS.
- If Program Office estimates indicate an IT Program's dollar thresholds will be in excess of those for a MAIS, coordination with the Assistant Secretary of Defense for Networks and Information Integration (ASD NII) staff occurs to determine program designation as a:
  - MAIS,
  - ACAT II, or
  - ACAT III.
- A NSS determination does not exempt a program from being designated a MAIS. Many NSS communication systems used for command and control purposes are MAIS programs.

Statutes & Regulations

(Page 1 of 5)

Congressional/Office of Management & Budget (OMB):

- Title 40, Subtitle III – Clinger Cohen Act
  - "…quantitatively benchmark agency process performance against those processes in terms of cost, speed, productivity, and quality of outputs and outcomes…"
  - "…ensure that the information security policies, procedures, and practices of the executive agency are adequate…"
- Circular A-130 – Management of Federal Information Resources
  - Agencies shall …"integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology…" and …"protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information…"
  - "Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government…"
  - "Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner…"

Statutes & Regulations

(Page 2 of 5)

Department of Defense (DOD) Directives (DODD) & Instructions (DODI):

- DODD 5000.01 – The Defense Acquisition System
  - Milestone Decision Authorities (MDAs) and Program Managers (PMs) "shall tailor program strategies and oversight, including documentation of program information, acquisition phases, the timing and scope of decision reviews, and decision levels, to fit the particular conditions of that program".
  - "Incremental development is the preferred process for executing" evolutionary acquisition strategies.
  - "Every PM shall establish program goals for the minimum number of cost, schedule, and performance parameters that describe the program over its life".

Statutes & Regulations

(Page 3 of 5)

- DODD 8000.1 – Management of DOD Information Enterprise
  - "Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents…"
  - "All aspects of the Department of Defense Information Enterprise"… shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a netcentric environment".
- DODD 8100.1 – Global Information Grid (GIG) Overarching Policy
  - Requires DOD Component to determine "whether the function that IT will support is central to, or a priority for, the Department's mission".
  - Ensure enterprise and Component level "information sharing, visibility, assurance, and interoperability."
- DODD 8500.01E - Information Assurance (IA)
  - This policy does not apply to weapons systems as defined by DoD Directive 5144.1 (reference (h)) or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.
  - Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems

Statutes & Regulations

(Page 4 of 5)

- DODI 5000.02 - Operation of the Defense Acquisition System
  - Provides mandatory procedures for major programs, all Acquisition Category (ACAT) programs, and acquisition contracts.
  - Provides definitions for ACAT designations and uses Clinger Cohen Act definition of Information Technology.
  - Provides procedures for material solution analysis, technology development, engineering and manufacturing development, production and deployment and operations and support phases of the program life cycle.
  - “Information technology initiatives shall prototype subsets of overall functionality…with the intention of reducing enterprise architecture risks, prioritizing functionality, and facilitating process redesign.”
  - “Program managers shall employ a modular open systems approach to design for affordable change, enable evolutionary acquisition, and rapidly field affordable systems that are interoperable”.
  - “Program Managers for ACAT I and II programs, regardless of planned sustainment approach, shall assess the long-term technical data needs of their systems and reflect that assessment in a Data Management Strategy”.
  - Requires compliance with the Clinger Cohen Act at Milestones A, B and C, Program Initiation for Ships, Full-Rate Production (or Full Deployment) Decision Review (DR) (or equivalent)

Statutes & Regulations

(Page 5 of 5)

Department of the Navy, Secretary of the Navy Instructions (SECNAVINSTs):

- SECNAVINST 5000.2 – Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System
  - Provides mandatory procedures for major programs, all Acquisition Category (ACAT) programs, and acquisition contracts.
  - Requires registration in the "DoD Information Technology Portfolio Repository-DON and Naval Information Technology Exhibits/Standard Reporting".
  - Uses Clinger Cohen Act definition of IT.
  - Requires PM reporting of "their contractor assessment information" per CPARS procedures for those contracts exceeding $1milion.
- SECNAVINST 5000.36 – Department of the Navy Information Technology Applications and Data Management
  - Requires PMs to notify applicable Functional Area Manager prior to initiation of investments in/development of new IT systems, applications, and/or databases.
  - Requires implementation of Department of the Navy IT application and data management policies, standards, and metrics by all acquisition programs.

IT System Statutes

(1 of 3)

Time-Certain Acquisition of an Information Technology (IT) Business System

Section 811 of Public Law 109-364 requires that the "Milestone Decision authority for an information system…may not provide Milestone A approval for the system" unless "that authority determines that the system will achieve initial operational capability within…five years." If such an information system "has not achieved initial operational capability within five years" the system will have been "deemed to have undergone a critical change" requiring evaluation and reporting.

Definition: For the purposes of this section an information system is any DOD IT business system that is not a national security system.

<u>Note</u>: DoD Appropriations Acts for both FY06 and FY07 contained a similar requirement.

IT System Statutes

(2 of 3)

Congressional Notification of Cancellation or Significant Scope Reduction

Section 806 of Public Law 109-163 requires the "Secretary of Defense notify the congressional defense committee" at least 60 days before cancelling a MAIS "program that has been fielded or approved to be fielded, or making a change that will significantly reduce the scope of such a program".

Each notification submitted to Congress regarding the proposed cancellation or significant reduction in the scope of a MAIS program must include:

(1) "the specific justification for the proposed cancellation or change";
(2) "a description of the impact of the proposed cancellation or change" on the ability of DoD to achieve the objectives of that MAIS program;
(3) a description of steps DoD "plans to take to achieve such objectives"; and
(4) "other information relevant to the change in acquisition strategy".

Definitions: MAIS has the meaning given to that term in DODD 5000.1.
"Approved to be fielded" means received Milestone C approval.

IT System Statutes

(3 of 3)

Defense Business System Modernization

10 U.S.C. §2222 provides that no funds appropriated to DoD may be obligated for a "defense business system modernization that will have a total cost in excess of $1 million", unless—

(1) the approval authority designated for the Defense Business System certifies to the Defense Business Systems Management Committee (DBSMC) the Defense Business System Modernization--

(A) is in compliance with the enterprise architecture developed by the DBSMC;

(B) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or

(C) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect; and

(2) the DBSMC approves the certification submitted by the approval authority.

Definition: "Defense Business System Modernization" is the acquisition or development of a new defense business system; or any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services).

Major Automated Information Systems

(Page 1 of 12)

10 U.S.C. Chapter 144A:

- Establishes Congressional Reporting requirements for MAIS programs.
- Defines *Major Automated Information System* in statute.
- Designates USD AT&L and Service Acquisition Executives as *Senior Officials* responsible for Congressional reporting.
- Requires a MAIS Annual Report (MAR) to be submitted to Congressional defense committees (analogous to Selected Acquisition Report). MAR establishes the Original Estimate (baseline).
- Requires Program Managers to submit MAIS Quarterly Report (MQR) to the Senior Official documenting any variance from the baseline.
- Establishes Significant and Critical Change thresholds.
- Imposes a reporting penalty on programs that fail to achieve an Initial Operational Capability (IOC) within 5 years after Milestone A.
  - FY09 NDAA changed starting time from Milestone A to "funds first obligated" for the program
  - FY10 NDAA changed ending time from IOC to Full Deployment Decision

Major Automated Information Systems

10 U.S.C. Chapter 144A (continued):

- Requires communication to Congress:
  - Significant Change → Notification letter
  - Critical Change → Report with certifications based on program evaluation (analogous to Nunn-McCurdy)

Source: Enacted FY07 NDAA 816; amended FY09 NDAA 812, WSARA 2009 101, and FY10 NDAA 817 and 841.

Major Automated Information Systems

(Page 3 of 12)

Section 812 of FY 2009 NDAA amends 10 U.S.C. Chapter 144A to:

- Add Congressional Reporting requirements for an "Other Major Information Technology Investment Program":
  (1) An investment that is designated by the Secretary of Defense, or a designee of the Secretary, as a 'pre-MAIS' program
  (2) Any other investment in automated information system products or services that is expected to exceed a MAIS threshold, but is not considered to be a MAIS program because a formal acquisition decision has not yet been made
- Change 5-year development 'clock' to start *when funds for program are first obligated* for the program instead of Milestone A. Programs that submitted 2008 MAR will be grandfathered.

Major Automated Information Systems

(Page 4 of 12)

Section 841 of FY 2010 NDAA amends 10 U.S.C. Chapter 144A to:

- Change 5-year development 'clock' to end *at the Full Deployment Decision (FDD) (i.e., the date the FDD Acquisition Decision Memorandum is signed by the Milestone Decision Authority (MDA)).*
  - Programs that achieved Initial Operating Capability prior to FY10 NDAA enactment (October 28, 2009) were grandfathered.
  - The term 'full deployment decision' means the final decision made by the MDA authorizing an increment of the program to deploy software for operational use.
- Add a new mandatory schedule event called full deployment (FD)

  'Full deployment' means the fielding of an increment of the program in accordance with the terms of a full deployment decision.
- FD and FOC will be very similar, but it all depends on:
  - When the user declines to field the operationally effective and suitable system that meets all Key Performance Parameter thresholds, and
  - When the fielding will take several years to accomplish.

Major Automated Information Systems

WSARA 2009 changed Chapter 144A certification requirement #3 –

"(3) the new estimates of the costs, schedule, and performance parameters with respect to the program and system or information technology investment, as applicable, are reasonable and have been determined, with the concurrence of the Director of Cost Assessment and Program Evaluation, to be reasonable;"

Summary of D,CAPE Involvement with Ch 144A Critical Change Reports		
Milestone Decision Authority	Independent Cost Estimate Required?	Cost, Schedule, Performance Concurrence?
USD(AT&L)	Yes	Yes
ASD(NII)	No	Yes
SAE	No	Yes

Major Automated Information Systems

(Page 6 of 12)

MAIS Annual Report (MAR):

- Is due annually to Congress *45 days* after submission of President's Budget .
- Must include the following:
  - Schedule, including estimates of milestone dates, full deployment decision, and full deployment ;
  - Estimates of development and life-cycle *costs ; and*
  - Summary of key *performance* parameters.
- Initially constitutes the baseline for determining Significant and Critical program changes:
  - Baseline can only be changed if a Critical Change Report is sent to Congress. Report of amended baseline may await next MAR.
  - Baseline is not changed by an Acquisition Program Baseline revision. Baseline change is effective after reported in a MAR.

Major Automated Information Systems

(Page 7 of 12)

(a) Quarterly reports by program managers — The Program Manager for a MAIS program must, on a quarterly basis, submit to the Senior Department of Defense Official Responsible for the MAIS program a written report identifying *any variance in the projected development schedule, implementation schedule, life-cycle costs, or key performance parameters*.

(b) Senior Officials responsible for programs — The Senior DOD official responsible for a MAIS program is:

(1) the Senior Acquisition Executive for the military department in the case of an automated information system to be acquired for a military department, or

(2) USD AT&L for any other automated information system to be acquired for DoD or any component of DoD.

Determinations - The Senior DOD Official must review the PM's quarterly report to determine whether a Significant or Critical Change has occurred.

For Significant Changes, notify congressional defense committees of the change within 45 days after receiving the PM's report.

For Critical Changes, within 60 days after the PM's MAIS Quarterly Report was received in the staff office, the Senior Official must :

- Conduct an evaluation of the program, and
- Submit a report and certification to the congressional defense committees through the Secretary of Defense

Major Automated Information Systems

(Page 8 of 12)

Reportable Changes

	Significant	Critical
Cost (program development cost or total life-cycle cost)	**15-25% increase**	**≥ 25% increase**
Schedule	**>6 month – 1 year delay**	**≥ 1 year delay**
		Fail to achieve IOC within 5 years after funds were first obligated for the program
Performance	**"Significant adverse change in expected performance"**	**"Undermine the ability of the system to perform mission as originally intended" (miss a KPP)**
Report to congressional defense committees	**Notification due 45 Days after office of Senior Official receives MQR**	**Program Evaluation and Report due 60 days after office of Senior Official receives MQR**

Major Automated Information Systems

(Page 9 of 12)

For the purpose of MAIS Quarterly Reports, Significant Change is defined as:

- Schedule: a delay of more than six months but less than a year in any program schedule milestone or significant event from the baseline;

- Cost: estimated program development cost or full life-cycle cost for the program has increased by at least 15 percent, but less than 25 percent, over the baseline; or

- Performance: a significant, adverse change in the expected performance of the major automated information system to be acquired.

Major Automated Information Systems

(Page 10 of 12)

For the purposes of MAIS quarterly reporting, Critical Change is defined as:

- Five-year to full deployment decision threshold: *failure to achieve a full deployment decision within five years* of when funds for program were first obligated (criteria changed by FY09 NDAA and FY10 NDAA) . The 5-Year Clock begins when Funds First Obligated. The "funds first obligated" date for each Increment is the earliest of the following:
  - An ADM that approves a Milestone A;
  - An ADM that approves the preferred alternative for an Increment of a program; or
  - The date explicitly established in an ADM as a funds first obligated" date.
- Schedule: *a delay of one year or more* in any program schedule milestone or significant event from the baseline .
- Cost: the estimated program development cost or total life-cycle cost for the program has *increased by 25 percent or more* over the baseline.
- Performance: a change in expected performance that will *undermine the ability of the system to perform the functions anticipated* in the original baseline.
- DoD has defined a failure to achieve a Threshold Key Performance Parameter as a Critical Change.

Major Automated Information Systems

(Page 11 of 12)

Program Evaluation Requirements for Critical Changes include an assessment of:

(1) the projected cost and schedule for completing the program if current requirements are not modified;

(2) the projected cost and schedule for completing the program based on reasonable modification of such requirements; and

(3) the rough order of magnitude of the cost and schedule for any reasonable alternative system or capability.

Reports on Critical Changes must include Senior Official's written certification (with supporting explanation) that:

(1) the automated information system to be acquired is essential to the national security or to the efficient management of the Department of Defense;

(2) there is no alternative to the system which will provide equal or greater capability at less cost;

(3) the new estimates of the costs, schedule, and performance parameters with respect to the program and system are reasonable; and

(4) the management structure for the program is adequate to manage and control program costs.

Major Automated Information Systems

(Page 12 of 12)

Prohibition on Obligation of Funds - If the Senior Official does not submit the required report on Critical Changes within 60 days of receiving the PM's report, appropriated funds may not be obligated for any major contract under the program.

For Chapter 144A purposes, the term "major contract" means any contract under the program that:

(1) Is not a firm-fixed price contract,

(2) Has target cost exceeding $17M (FY00 constant dollars); or

(3) Is the largest contract under the program.

Programs should not obligate funds during Critical Change Report preparation. This prohibition ceases to apply on the date on which Congress receives a report in compliance with the law.

Clinger Cohen Act

(Page 1 of 4)

Information Technology Management Reform Act (ITMRA) of February 10, 1996 combined with the Federal Acquisition Reform Act (FARA) and became the Clinger-Cohen Act (CCA) attempted to resolve the following issues perceived by Congressional members:

- Little business process improvement before investing in IT;
- Little or no improvement in mission performance;
- Implementation of ineffective information systems resulting in waste, fraud, and abuse; and
- Outdated approaches to buying IT that did not adequately take into account the competitive and fast pace nature of the IT industry.

Clinger Cohen Act
(Page 2 of 4)

Clinger Cohen Act (CCA)/Title 40, Subtitle III:

- Defines Information Technology (IT) and Information Technology Architecture.
- Repealed central authority of the General Services Administration.
- Assigns Key responsibilities to Director of Office of Management and Budget (OMB), including:
  - Capital Planning and Investment Control: key assessment role;
  - IT Standards oversight through National Institute of Standards and Technology;
  - Agency IT Return on Investment and management practices evaluation; and
  - Authority to adjust apportionments for IT.
- Requires Agencies to establish Chief Information Officers (CIOs).
- Requires CIOs establish processes to provide for financial accountability and performance measurement for IT systems.

Clinger Cohen Act

(Page 3 of 4)

Agencies must:

- Do capital planning and investment control;
- Establish process to select, manage, and evaluate IT investments;
- Integrate IT with budget and management processes;
- Link IT Performance Measures to agency programs;
- Develop processes to verify progress in IT investments;
- Establish performance and result-based management goals;
- Tie IT performance measures into agency goals;
- Do BPR before making significant IT investments;
- Ensure INFOSEC policies are adequate; and
- Use “modular contracting” principles with contract award within 180 days and 18 month delivery of discrete increments that are “not dependent on any subsequent increment, in order to perform its principal functions”.

Clinger Cohen Act
(Page 4 of 4)

On October 25, 1996, OMB Director Franklin Raines issued a memorandum setting forth guidance commonly known as "Raines' Rules". The first three of these subsequently became known as the Three Pesky Questions:

1. Does the investment support core/priority mission functions that need to be performed by the Federal government. (i.e. Should the Agency be doing the function at all?)
2. Should the investment be undertaken because no alternative private sector or governmental source can efficiently support the function. (i.e. Can someone else do it better? If the private sector should do it, should it be done under contract or should the government component be privatized? Who performs the work?)
3. Does the investment support work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf (COTS) technology. (i.e. Is it organized and being done in the best way possible? A competitive advantage with efficient financial systems will hedge financial management from A-76 threats/privatization. Have the business processes been re-engineered?)

DODI 5000.02, Enclosure 5

CCA Compliance requirements apply to all IT investments, including NSS.

For all programs that acquire IT, including an NSS, at any ACAT level, the Milestone decision Authority shall not initiate a program or an increment of a program, or approve entry into any phase of the acquisition process; and the DoD Component shall not award a contract until:

(1) The sponsoring DoD Component or Program Manager has satisfied the requirements of Title 40/CCA;

(2) The DoD Component Chief Information Officer (CIO), or designee, confirms Title 40/CCA compliance; and

(3) For Major Defense Acquisition Programs and Major Automated Information Systems programs only, the DoD CIO also confirms Title 40/CCA compliance.

DODI 5000.02, Enclosure 5

(2 of 5)

Table 8, CCA Compliance Matrix

Actions Required to Comply With CCA	Applicable Program Documentation
1. Make a determination that the acquisition supports core, priority functions of DON. [1]	ICD Approval
2. Establish outcome-based performance measures linked to strategic goals. [1, 2]	ICD, CDD, CPD and APB approval
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [1, 2]	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD

1. These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command & Control Systems that are not themselves IT systems.
2. These actions are also required to comply with section 811 of NDAA FY 2001.

DODI 5000.02, Enclosure 5

(3 of 5)

Table 8, CCA Compliance Matrix

Actions Required to Comply With CCA	Applicable Program Documentation
4. Determine that no Private Sector or Government source can better support the function. [3]	Acquisition Strategy page XX, para XX AoA page XX
5. Conduct an analysis of alternatives. [2,3]	AOA
6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a Life-Cycle Cost Estimate. [2,3]	Program LCCE Program Economic Analysis for MAIS

2. These actions are also required to comply with Section 811 of NDAA FY 2001.
3. For NSS, these requirements apply to the extent practicable.

DODI 5000.02, Enclosure 5

(4 of 5)

Table 8, CCA Compliance Matrix

Actions Required to Comply With CCA	Applicable Program Documentation
7. Develop clearly established measures and accountability for program progress.	Acquisition Strategy page XX APB
8. Ensure that the acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards.	APB (Net-Ready KPP) ISP (Information Exchange Requirements)
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards. [2]	Information Assurance Strategy

2. These actions are also required to comply with Section 811 of NDAA FY 2001.

DODI 5000.02, Enclosure 5

(5 of 5)

Table 8, CCA Compliance Matrix

Actions Required to Comply With CCA	Applicable Program Documentation
10. Ensure, 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
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO.	DoD IT Portfolio Repository

Back Up

- Acronyms
- Additional Statutes and Regulations
- Additional References
- DoDI 5000.02 Select Provisions
- JCIDS Select Provisions
- Financial Management Systems
- Defense Science Board's Recommendation
- FAR Guidance
- DFARS Guidance
- DON Guidance
- Open Source Software

Acronyms

(Page 1 of 3)

- Acquisition Decision Memorandum (ADM)
- Aircraft Procurement Navy (APN)
- Assistant Secretary of Defense for Networks and Information Integration (ASD NII)
- Automated Information System (AIS)
- Clinger Cohen Act (CCA)
- Department of Defense (DoD)
- Department of Defense Instruction (DoDI)
- Department of the Navy (DON)
- Fiscal Year (FY)
- Foreign Military Sale (FMS)
- Full Deployment Decision (FDD)
- Full Operational Capability (FOC)
- Initial Operational Capability (IOC)
- Major Automated Information System (MAIS)
- Major Defense Acquisition Program(MDAP)
- MAIS Annual Report (MAR)
- MAIS Quarterly Report (MQR)
- Milestone Decision Authority (MDA)

Acronyms

(Page 2 of 3)

- Marine Corps Procurement (MCP)
- National Defense Authorization Act (NDAA)
- National Security System (NSS)
- Office of Management and Business (OMB)
- Operations and Maintenance, Navy (O&M,N)
- Operations and Maintenance, Marine Corps (O&M,MC)
- Other Procurement Navy (OPN)
- Paperwork Reduction Act (PRA)
- Research, Development, Test & Evaluation (RDT&E)
- Ship Conversion Navy (SCN)
- Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L)
- Weapon Procurement Navy (WPN)

Additional Statutes &Regulations

- E-Government Act of 2002 Public Law 107-347
  - Improves the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.
  - Shares effective practices for access to, dissemination of, and retention of Federal information.
- Title 5 Section 552a - Privacy Act of 1974
  - "No agency shall disclose any record which is contained in a system of records by any means of communication to any person,…"
  - Each agency must keep an accurate accounting of the date, nature, and purpose of each disclosure.
- Title 10, Subtitle A, Part IV - Defense Information Assurance Program
  - "…protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces …"
  - Objectives to provide continuously for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems

Additional Statutes &Regulations

- Title 44, Chapter 35 Subchapter I – Paperwork Reduction Act
  - "…minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons…"
  - "…improve the quality and use of Federal information to strengthen decision making, accountability, and openness in Government…"
- Circular A-11 – Preparing, Executing, and Submitting the Budget
  - Discusses planning, budgeting, and acquisition of capital assets.
  - Is fully revised annually.
- M-05-04 - Policies for Federal Agency Public Web sites
  - Manage Federal agency public websites as part of their information resource management program following guidance in OMB Circular A-130.
  - OMB will monitor agency compliance with these policies as part of its oversight of agency information resource management programs.
- DODD 3020.40 – DOD Policy and Responsibilities for Critical Infrastructure
  - Requires "that, prior to system fielding or deployment, either commercial system developers remediate or the appropriate senior-level DoD program manager documents a risk management decision for all vulnerabilities identified."
  - Incorporate "requirements for the risk management" of Defense Critical Infrastructure in "acquisition, maintenance, and sustainment contracts."

Additional References

- Section 811 of Public Law 109-364, "John Warner National Defense Authorization Act for Fiscal Year 2007," "Time-Certain Development for Department of Defense Information Technology Business Systems"
- *Section 806 of Public Law 109-163, National Defense Authorization Act for 2006*
- *Section 8068 of Public Law 110-116, Defense Appropriations Act of 2008*
- DOD Directive 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), of 5 May 04
- DOD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), of 30 Jun 04
- DOD Directive 8115.01, Information Technology Portfolio Management, of 10 Oct 05
- DOD Directive 8320.2, Data Sharing in a Net-Centric DOD,of2Dec04
- DOD Instruction 8500.2, Information Assurance (IA) Implementation, of 6 Feb 03
- DOD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 07
- DOD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key Enabling, of 1 Apr 04
- DOD Instruction 8580.1, Information Assurance in the Defense Acquisition System, 9 Jul 04
- CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, of 8 Mar 06