OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301

MAR 8 2002

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES

SUBJECT: Clinger-Cohen Act Compliance Policy

The Clinger-Cohen Act (CCA) of 1996 required the Department to appoint a DoD Chief Information Officer (CIO) and a CIO for each Military Department. The CIO's primary responsibility is to oversee investments in information technology (IT) (including National Security Systems (NSSs)) to ensure that the Department's IT systems are interoperable, secure, properly justified and contribute to mission goals. Additional legislative requirements for certification of Major Automated Information System (MAIS) compliance with the CCA and for registration of mission critical and mission essential IT systems have been imposed by recent DOD Authorization and Appropriations Acts.

Compliance with the CCA is required for all IT systems, including those in weapons and weapons systems programs. The requirement for certification of compliance with the CCA, as required by DOD Appropriations Acts, is limited to MAIS programs as explained in DODI 5000.2. Registration requirements in the DOD Appropriations Acts are for mission critical and mission essential IT systems (including NSS).

The basic requirements of the CCA that relate to the Department's acquisition process have been institutionalized in DoD Instruction 5000.2. The purpose of this policy memorandum is to clarify and simplify the requirements for judging compliance with the law.

The requirements of DoD Instruction (DoDI) 5000.2 (Paragraphs. 4.7.3.1.5 and 4.7.3.2.3.2) regarding CCA compliance are modified as follows:

a. Acquisition documents required by DoDI 5000.2 to support acquisition milestone decisions shall be used to address CCA requirements.
b. The attached table illustrates the program-level documents that may typically be used to address individual CCA requirements. If those documents include specific CCA compliance information, Program Managers shall indicate CCA compliance by providing a table that (1) lists the requirements of paragraph. 4.7.3.2.3.2 (subject to applicable exceptions in paragraph c below), and (2) specifically cites the page and paragraph (e.g.

Acquisition Strategy, page 32, paragraph 4.1) in the program documentation where the requirement is satisfied.

c. The following CCA requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command and Control Systems that are not themselves IT systems:

CCA Requirement	Compliance Source
(1) Make a determination that the acquisition supports core, priority functions of the Department	MNS Approval
(2) Establish outcome-based performance measures linked to strategic goals	MNS, ORD and APB approval
(3) Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology	Approval of the MNS, Concept of Operations, AoA and ORD

d. The requirement for submission of written confirmation required by DoDI 5000.2 paragraph 4.7.3.2.3.2 shall be satisfied by the component CIO's concurrence with the Program Manager's CCA Compliance Table.

e. The requirement to register mission critical and mission essential IT systems in DoD 5000.2-R, Appendix 7 is amended as follows. For mission critical and mission essential IT that is an integral part of a weapons system or platform (e.g. ship, aircraft or tank) registration will be done at the program level.

f. Issues relative to CCA compliance shall be resolved through the IPT process described in section 7, DoD 5000.2-R.

The above changes are effective immediately and will be included in the next update to the DoD 5000 series regulations.

E.C. Aldridge, Jr.
Under Secretary of Defense for
Acquisition, Technology and Logistics

John P. Stenbit
Assistant Secretary of Defense for
Command, Control,
Communications & Intelligence

Clinger-Cohen Act (CCA) Compliance Table

Requirements Related to the Clinger-Cohen Act (CCA) of 1996 (paragraph 4.7.3.2.3.2 DoDI 5000.2)	Applicable Program Documentation **
***Make a determination that the acquisition supports core, priority functions of the Department	MNS Approval
***Establish outcome-based performance measures linked to strategic goals	MNS, ORD and APB approval
***Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology	Approval of the MNS, Concept of Operations, AoA and ORD
* No Private Sector or government source can better support the function	Acquisition Strategy page XX, para XX AOA page XX
* An analysis of alternatives has been conducted	AOA
* An economic analysis has been conducted that includes a calculation of the return on investment; or for non-AIS programs, an LCCE has been conducted	Program LCCE
There are clearly established measures and accountability for program progress	Acquisition Strategy page XX APB
The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards	APB (Interoperability KPP) C4ISP (IERS)
The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Information Assurance Strategy
To the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive blocks, each of which meets part of the mission need and delivers measurable benefit, independent of future blocks	Acquisition Strategy page XX
The system being acquired is registered	Registration Data Base

* 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

Attachment