



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000

APR 02 2007

CHIEF INFORMATION OFFICER

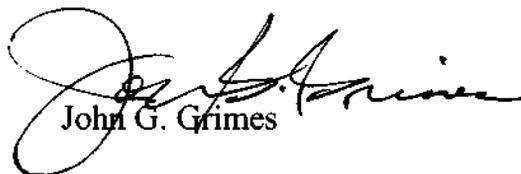
MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF THE MILITARY  
DEPARTMENTS  
CHIEF INFORMATION OFFICERS OF THE DEFENSE  
AGENCIES  
CHIEF INFORMATION OFFICERS OF THE DOD FIELD  
ACTIVITIES

SUBJECT: Risk-based Oversight for Subtitle III of Title 40 [Clinger-Cohen Act  
(CCA)] Compliance

This policy memorandum implements a risk-based approach for oversight of the requirements of Subtitle III of Title 40 of the United States Code (40 U.S.C. 11101 et seq.) [formerly Division E of the Clinger-Cohen Act of 1996] (hereinafter referred to as "Title 40/CCA") for Major Automated Information Systems (MAISs) and Major Defense Acquisition Programs (MDAPs) in the Department of Defense (DoD). This policy is part of the evolving implementation of Title 40/CCA aimed at de-centralizing oversight, maximizing up-front involvement in the Information Technology (IT) investment process, and alleviating redundancies.

Under this risk-based oversight process, the DoD Chief Information Officer (CIO) will defer oversight of Title 40/CCA for selected programs when a Component CIO has shown the capability to conduct oversight. Component CIOs shall complete the attached Title 40/CCA Capability Assessment and provide a copy to the Director, Commercial Information Technology Policy (CITP) not later than 90 days from the date of this policy. The next step will be a feedback meeting between the CITP staff and the Component CIO representatives. Title 40/CCA oversight deferrals will be determined for selected programs based on the Component capability and program risk.

My point of contact for this action is Mr. Edward Wingfield, DoD CIO,  
Commercial Information Technology Policy Directorate at (703) 601-4729 x127 or  
edward.wingfield@osd.mil.

  
John G. Grimes

Attachment:  
As stated



# **PROCEDURE FOR RISK-BASED OVERSIGHT OF SUBTITLE III OF TITLE 40 [CLINGER-COHEN ACT (Title 40/CCA)] COMPLIANCE**

## **BACKGROUND**

The DoD Component Chief Information Officers (CIOs) are responsible for implementing and overseeing the effective use of the best practices of Subtitle III of Title 40, reference (a), hereinafter referred to as “Title 40/CCA”), for all Information Technology/National Security System (IT/NSS) investments being proposed, acquired and maintained within their Agency or as the lead Agency of a joint investment.

Since the initiation of statutory certification requirements, DoD CIO, reference (b) has conducted detailed oversight of Title 40/CCA compliance of acquisition category (ACAT) I MDAPs and MAISs programs under DODI 5000.2, reference (c) and DoD CIO memoranda implementing annual Defense Appropriations Act certification requirements, reference (d). Under this policy of risk-based oversight of CCA compliance, it is my objective to defer the level of DoD CIO oversight by using the following procedures.

## **PURPOSE**

The purpose of the risk-based oversight policy is to enable the DoD CIO to identify and implement a cost-effective means for ensuring CCA compliance, by increasing reliance on oversight by the Component CIOs. The Component CIOs will oversee programs within their portfolios commensurate with their demonstrated level of capability.

## **APPLICABILITY**

These procedures apply to the Chief Information Offices (CIOs) of the Military Departments, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense with an established Chief Information Office (hereafter referred to collectively as “the Component CIOs”).

These procedures are applicable to all Major Automated Information Systems (MAIS) and Major Defense Acquisition Programs (MDAP), including those deferred to the Components. These procedures are intended to be consistent with DoD Instruction 5000.2.

## PROCESS

The process for executing this risk-based oversight of Title 40/CCA compliance is depicted in Figure 1.

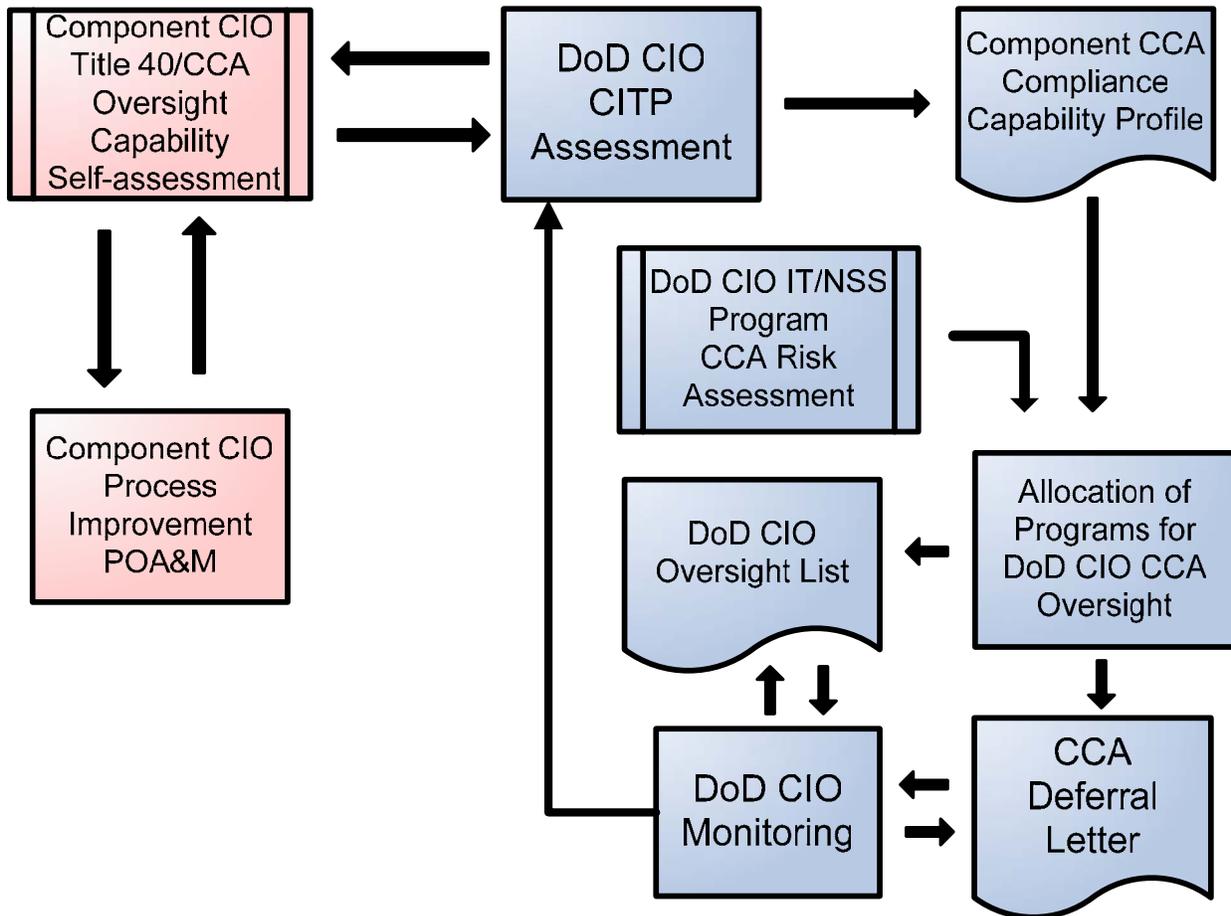


Figure 1. Title 40/CCA Risk-based Oversight Process

The process is initiated when the Component CIO conducts a self-assessment of Title 40/CCA compliance oversight capability using the attached Title 40/CCA Capability Assessment. Deficiencies uncovered by the self-assessment should be considered in the Component CIOs continuous process improvement (CPI) program, reference (e). The self-assessment is forwarded to Director, Commercial Information Technology Policy (CITP) office within the DoD CIO office for review. Representatives from the CITP office and Component CIO shall have a “feedback” meeting at which each will share the insights they have gained from the assessment process, and lay down a plan of action to gain the most benefit from mutually agreed findings. The CITP representatives, based on their review and insights gained in the feedback session, will rate the level of sufficiency of the DoD Component CIO in each of the four cornerstones of the assessment on a

continuum from “fully sufficient,” “partially sufficient,” to “not sufficient.” These terms are equivalent to the more familiar stoplight model of green, yellow and red where: 1) green means things are basically in good order, even if improvements are still possible; 2) yellow means that there are issues or action items that need to be addressed; and 3) red means that these issues are of a serious and/or urgent nature.

The DoD CIO will factor program risk into the review process by conducting a Title 40/CCA risk assessment, applying classification methods already established within the Joint Capabilities Integration and Development System (JCIDS), reference (f), and DoDI 5000.2, e.g., dollar magnitude of the program and JROC interest. As an example of a possible scenario, the DoD CIO might find a Component CIO capability to be partially sufficient, and would defer all programs except those of a certain size or of special interest. The DoD CIO Title40/CCA risk assessment, together with the Component’s CCA Compliance Capability Profile, may result in a list of programs deferred to the Component CIO.

The DoD CIO will monitor the effectiveness of the risk-based oversight process. DoD CIO will engage in periodic consultations with the Component CIO offices; offer training, coaching, and consultation as appropriate, and will annually (at a minimum) revisit the list to determine if the deferred program list should be expanded or reduced. The Component CIOs may be required to periodically update their self-assessment.

Note: CCA Certification guidance is provided separately by the DoD CIO in response to annual Congressional Title 40/CCA certification mandate.

#### References:

- (a) Title 40 U.S.C. Subtitle III, Information Technology Management (Formerly known as the Clinger-Cohen Act of 1996)
- (b) DODD 5144.1, May 2, 2005, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief information Officer (ASD(NII)/DoD CIO)
- (c) DODI 5000.2, May 12, 2003, Operation of the Defense Acquisition System
- (d) Clinger-Cohen Act Compliance of Major Automated Information System (MAIS) for Fiscal Year (FY) 2007, dated January 10, 2007
- (e) Establishment of DoD-wide Continuous Process Improvement (CPI) Programs, dated May 11, 2006
- (f) CJCSI 3170.01E, Joint Capabilities Integration and Development System

Attachment: Title 40/CCA Capability Assessment: Component CIO Self-Assessment
---

## **Attachment**

### **Title 40/CCA Capability Assessment: Component CIO Self-Assessment**

This document asks a series of questions related to the implementation of oversight for Subtitle III of Title 40 [Clinger Cohen Act (Title 40/CCA)] within Department of Defense (DoD) Components. The primary audience for this assessment is the Component CIO. These questions were derived from a range of resources, including policy and guidance documents, feedback from a 2004-2005 Title 40/CCA Assessment sponsored by the Deputy CIO (DCIO) and USD(AT&L), and input from DoD personnel across multiple organizations and functions.

The primary goal of this assessment effort is to support the DCIO's transition to risk-based oversight of Title 40/CCA compliance. Risk-based oversight for Title 40/CCA is a process wherein the DCIO will use a Component CIO's self-assessment of capability to determine the degree of oversight deferral to the Component CIO, based both on the capability of the Component across Title 40/CCA areas and risk category of the program. This self-assessment will provide data to support the DCIO's capability evaluation of each Component. Additionally, the evaluation process is seen as generating ideas for improvement within the DoD CIO community.

Reference Document: This guide adopts the cornerstones (key framework elements) and general principles of a recently completed U.S. General Accountability Office report "Framework for Assessing the Acquisition Function at Federal Agencies," September 2005 [GAO-05-218G]. That document develops relevant assessment questions based upon four cornerstones:

- 1) Organizational Alignment and Leadership**
- 2) Policies and Processes**
- 3) Human Capital**
- 4) Knowledge and Information Management**

#### Steps in completing the Self-Assessment

1. Assign persons who will be responsible for completing the various part(s) of the self-assessment.
2. Write a response to each of the questions.
3. Assign one of the following values to each response based on processes and practices in place to meet the requirement: "Sufficient," "Partially Sufficient," or "Not Sufficient." Note: These terms are equivalent to the more familiar stoplight model of green, yellow and red where: 1) fully sufficient means that things are basically in good order, even if improvements are still possible; 2) partially sufficient means that there are issues or action items that need to be addressed; and 3) not sufficient means that the issues are of a serious and/or urgent nature.

## Cornerstone One: Organizational Alignment and Leadership

Organizational alignment is appropriate placement of the CIO function in the Component, with stakeholders having clearly defined roles and responsibilities. There is no single, optimal way to organize a Component's CIO function. Each Component must assess whether the current placement of its CIO function is meeting its organizational needs. Committed leadership enables officials to make strategic decisions that achieve enterprise-wide IT investment outcomes more effectively and efficiently.

SELECT ONE	1.1	Where does the CIO office fit within the current Component organizational structure?
SELECT ONE	1.2	What are the roles and responsibilities of the CIO and CIO personnel within the Component?
SELECT ONE	1.3	When was the last time that the Component assessed the CIO function and related controls? What were the assessment findings?
SELECT ONE	1.4	Describe how the CIO has appropriate influence within the Component to ensure its voice is heard at the highest leadership levels? How do you know it?
SELECT ONE	1.5	Describe how the CIO has appropriate influence within the cross-functional teams to assure that its voice is heard by all the team members? How do you know it?
SELECT ONE	1.6	Describe how the CIO office ensures that it stays aligned with the Component strategic plan/mission. Where is this process documented? Please provide documents relevant to this question (e.g., CIO strategic plan, process for aligning the CIO office with the strategic plan, and the like).
SELECT ONE	1.7	Identify the key metrics by which the Component measures the success of its IT investments? Describe how the Component uses these metrics to monitor the success of its IT investments. How well are these metrics understood across the Component?
SELECT ONE	1.8	How often and in what manner is the CIO generally involved in investment review activities at the Component level, the JCIDS process, and/or other efforts before a program is initiated (Pre-A & B decision-making processes)?
SELECT ONE	1.9	Describe how the Component is implementing Portfolio Management. Describe the CIO's role in portfolio evaluations and decision-making.
SELECT ONE	1.10	Describe the Component policy to identify acquisition programs from among all its IT investments. Provide a copy of that policy. If no policy exists, describe plans to write/implement such a policy.

## Cornerstone Two: Policies and Processes

Implementing strategic decisions to achieve desired enterprise-wide outcomes requires clear and transparent policies and processes that are implemented consistently. Policies establish expectations about the management of the acquisition function. Processes are the means by which management functions will be performed and implemented in support of agency missions. Effective policies and processes govern the oversight of IT investment efforts, with a focus on assuring that these efforts achieve intended results.

### 1) Program Compliance Assessment

*From DoDI 5000.2: "The MDA shall not approve program initiation or entry into any phase that requires milestone approval for an acquisition program (at any level) for a mission-critical or mission-essential IT system until the DoD Component CIO confirms (MDAPs) or certifies (for MAIS only) that the system is being developed in accordance with SubTitle III of Title 40 United States Code (Title 40/CCA). At a minimum, the DoD Component CIO's confirmation or certification shall include a written description of the three materiel questions of DoDI 5000.2, section 3.6.4 and the considerations in Table E4.T1." Table E4.T1 lists key elements that contribute to Title 40/CCA compliance, some of which echo the three materiel questions in section 3.6.4.*

In this section, please provide information about how the Component CIO ensures that each of the following elements are addressed through the Acquisition process – either through direct activity by the CIO, or by leveraging other organizations/offices with the requisite expertise to complete the requirement.

We are looking for evidence of CIO involvement or verified dependence on a third party based on their expertise during the acquisition process and decision-making – not simply the presence of compliance checks done later at the milestone. It is NOT necessary to complete both columns for each element – we are looking for an overview of how the CIO is either directly involved or leverages others to ensure CCA elements are addressed.

Where there are differences between how the Component gets involved in different types of programs, please delineate. Please distinguish among the following four types of programs: 1) ACAT I/IA acquisition programs, 2) less than ACAT I/IA programs, 3) Acquisition of Services, and 4) other IT investments. Please be specific in describing how the Component CIO has confirmed CCA compliance for all ACAT IIIs and below prior to awarding a contract.

			Describe actions taken directly by the Component CIO for the element. What evidence demonstrates or verifies the actions are done?	List other organizations/offices that the Component CIO relies on to ensure element is addressed. How do you confirm they are effective?
SELECT ONE	2.1.1	Make a determination that the acquisition supports core, priority functions of the Department.		
SELECT ONE	2.1.2	Establish outcome-based performance measures linked to strategic goals		
SELECT ONE	2.1.3	Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology.		
SELECT ONE	2.1.4	No Private Sector or Government source can better support the function (Also called "no alternative source")		
SELECT ONE	2.1.5	An analysis of alternatives has been conducted		
SELECT ONE	2.1.6	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		
SELECT ONE	2.1.7	There are clearly established measures / accountability for program progress		
SELECT ONE	2.1.8	The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards		
SELECT ONE	2.1.9	The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards		
SELECT ONE	2.1.10	To the maximum extent practicable, (1) modular contracting has been used, and		

			Describe actions taken directly by the Component CIO for the element. What evidence demonstrates or verifies the actions are done?	List other organizations/offices that the Component CIO relies on to ensure element is addressed. How do you confirm they are effective?
		(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		
SELECT ONE	2.1.11	The system being acquired is registered		
SELECT ONE	2.1.12	Post Implementation Reviews planned for and conducted		

Supplemental Questions:

SELECT ONE	2.1.13	What process is used to ensure that outcome-based performance measures, e.g., measures of effectiveness (MOEs) are developed and approved before the Concept Decision – how is the CIO involved in that process?
SELECT ONE	2.1.13a	After the program is established, what process determines how MOEs are used in the design and acquisition process?
SELECT ONE	2.1.14	What activities does Component CIO engage in to ensure that the use of COTS doesn't result in: (1) manual processes being simply automated, without evaluating them for needed change; (2) extensive COTS customization?
SELECT ONE	2.1.14a	How does the CIO evaluate COTS implementations?
SELECT ONE	2.1.15	Where are the specific criteria for Title 40/CCA compliance (confirmation/certification) laid out?
SELECT ONE	2.1.15a	How does the Component CIO articulate what "sufficient" Title 40/CCA compliance "looks like?"
	<p><b>2. Up-Front Involvement</b>  <i>The following questions cover a range of topics related to CCA implementation. In some cases, the CIO may be the lead agent for the activity; in others, the CIO may leverage or rely on other offices/organizations to complete. We are interested in the CIO's perceptions and activities – AND – a description of any reliance you place on others. If you rely on another group, please also describe how you ensure that the work by them is done effectively and</i></p>	

		<i>what criteria you use to determine that.</i>
SELECT ONE	2.2.1	What guidance and processes has the Component established for the conduct of a Capability-Based Assessment, as required under CJCS 3170?
SELECT ONE	2.2.2	What is the Component's CIO role in a Capability-Based Assessment?
SELECT ONE	2.2.3	What is the Component's process for conducting a DOTMLPF - Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities - evaluation? How does the Component CIO ensure that process redesign occurs in the DOTMLPF and ICD preparation processes - before a program is initiated?
SELECT ONE	2.2.4	What criteria does the Component CIO use to determine which IT programs require more Component CIO oversight/support than others? How does oversight vary between programs of different size, risk, visibility, or other variables?
SELECT ONE	2.2.5	How often does the Component identify a private sector or government alternative, and pursue that alternative rather than initiating a program? Can the Component point to a case study where this decision was made and implemented? What was the process?
		<b>3) Streamlining of Oversight Processes</b>
SELECT ONE	2.3.1	What steps has the Component CIO taken to ensure that the review processes are as streamlined, i.e., value-added and non-redundant, as possible?
SELECT ONE	2.3.2	Has the Component CIO recently (e.g., in last 2-3 years) assessed the reporting requirements to ensure that redundant reporting is minimized or eliminated? What were the assessment results?

### Cornerstone Three: Human Capital

The value of an organization and its ability to satisfy customers depends heavily on its people. Successfully executing the CIO responsibilities to help the Component meet its missions requires valuing and investing in the CIO workforce. Agencies must think strategically about attracting, developing, and retaining talent, and creating a results-oriented culture within the CIO workforce.

SELECT ONE	3.1	How many people does the CIO office have working to oversee the Components IT investments? Is this number of people sufficient to meet the overall oversight needs of the Component IT investments? If not, how many additional people are needed?
SELECT ONE	3.2	Describe the ratio of CIO oversight staff to active Acquisition programs (e.g., how many programs is each Component CIO oversight officer responsible for)?
SELECT ONE	3.3	Describe how the CIO function allocates its resources to support oversight of IT investments?
SELECT ONE	3.4	Describe how the organization goes about recruiting and maintaining qualified personnel for the CIO function. Describe the CIOs involvement in IT workforce planning.

SELECT ONE	3.5	Describe the training and mentoring that the CIO provides for its personnel related to Title 40/CCA compliance?
------------	-----	---

**Cornerstone Four: Knowledge and Information Management**

Effective knowledge and information management provides credible, reliable, and timely data to make IT investment decisions. Each stakeholder in the IT investment process --- Principal Staff Assistant, Joint Staff, program management personnel, CIO personnel, and others --- need meaningful data to perform their respective roles and responsibilities.

SELECT ONE	4.1	What does the Component CIO consider its key knowledge assets to be? How does the Component CIO manage those assets?
SELECT ONE	4.2	What performance support resources are made available by the Component CIO to the overall component for implementing Title 40/CCA? How is this being maintained?
SELECT ONE	4.3	What kind of benchmarking – both internal and external – is used to ensure that best practices are brought into the IT investment process?
SELECT ONE	4.4	What do you see as the Component’s strengths when considering Title 40/CCA? What is being done particularly well or successfully across the organization? What demonstrates that success?
SELECT ONE	4.5	Where does the Component need the most development when considering Title 40/CCA? What is not being done as well as the Component CIO would like? Where is more capability needed?
SELECT ONE	4.6	In what areas of expertise does the Component CIO rely on the DoD DCIO? What support from the DCIO is considered most helpful? Where could the DCIO be less involved, with no significant impact? Where is more DCIO help needed?

**What other comments do you have on any areas not covered by the questions above?**