Are Law and Policy Clear and Consistent?

Roles and Responsibilities of the Defense Acquisition Executive and the Chief Information Officer

Daniel Gonzales, Carolyn Wong, Eric Landree, Leland Joe

Prepared for the United States Navy
Approved for public release; distribution unlimited

RAND NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was prepared for the United States Navy. The research was conducted in the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

Library of Congress Control Number: 2010932669

ISBN: 978-0-8330-4970-4

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published 2010 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

This monograph presents an analysis of the roles and responsibilities (R&R) assigned to defense acquisition executives (DAEs) and chief information officers (CIOs) by Titles 10, 40, and 44 of the United States Code (USC) and by DoD policy. Its objectives are to identify and analyze DAEs' and CIOs' R&R, identify the sources of potential conflicts that may occur between DoD executives when they carry out their duties in the DoD acquisition process, and to formulate remedies for these potential conflicts in the form of revisions to DoD policy.

Roles and Responsibilities (R&R)

For the purposes of this study, R&R refer to activities, actions, tasks, duties, jobs, or functions assigned to an executive by an authoritative source. Authoritative sources include federal law, executive orders, Office of Management and Budget (OMB) circulars, and DoD policy documents. Some R&R include high-level, unique decision-making authorities, such as setting, establishing, or directing policy or overseeing the implementation of policy, that are not at first glance controlled or potentially circumscribed by other DoD executives. We term these *strong* R&R.

Other CIO R&R have authorities that are more circumscribed, such as advising other officials or making recommendations to other executives who hold actual decisionmaking power. We term the latter *advisory* R&R.

Strong R&R are the ones of primary interest in this study because these are the R&R that could potentially result in conflict between government executives.

Information Technology and National Security Systems

The DAE's acquisition authorities are broad and comprehensive. The DAE and his or her duly designated subordinates are responsible for the acquisition of any type of DoD system or platform that the U.S. military procures, including ships, aircraft, weapons, command and control, communications, intelligence, and information technology (IT) systems. In contrast, CIO R&R are generally restricted to IT and national security systems. For this study, we reviewed how IT and NSS are defined in U.S. law.[1] The review focused on R&R that are pertinent to IT and NSS. We also sought to understand the R&R of these executives in the larger context of DoD policy guidance for the development and acquisition of weapon systems containing IT components.

Acquisition-Related R&R

Titles 10 and 40 of the USC contain seven strong DoD acquisition-related R&R, as indicated in Table S.1.

Six of these are assigned to the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). We found that the first six R&R listed in Table S.1 do not pose a risk of possible conflicts between the DAE and the DoD CIO when they exercise their duties in the defense acquisition system (we term these *process conflicts*).

Table S.1
Strong DoD Acquisition Executive R&R in the U.S. Code

USC Source	Party	Role and Responsibility	Source of Acquisition Process Conflict
10 USC §133	USD(AT&L)	Supervises the acquisition system	No
10 USC §133	USD(AT&L)	Establishes acquisition policy	No
10 USC §133	USD(AT&L)	Directs secretaries of military departments and heads of all other elements of DoD with regard to matters for which USD(AT&L) has responsibility	No
10 USC §133	USD(AT&L)	Is designated DAE	No
10 USC §133	USD(AT&L)	Authorizes a senior acquisition official within the Office of USD(AT&L) to oversee the exercise of any DoD acquisition authority	No
10 USC §1702	USD(AT&L)	Has all powers, duties, and functions over the acquisition workforce	No
40 USC §11314	Executive agency head	Has acquisition authority with particular attention to multi-agency IT acquisitions	No

[1] Precise legal definitions of IT and NSS can be found in the body of this monograph.

The last R&R listed in the table is assigned to the agency head (the Secretary of Defense in the case of DoD).[2] This R&R explicitly relates to IT (the authority to acquire and manage IT, which is assigned to the "Head of the Executive Agency").

Our analysis revealed that this R&R, as it applies to DoD, does not conflict with other parts of U.S. law and should not be a source of conflict in the DoD acquisition process between the DAE and the DoD CIO. This conclusion follows because the assignment of acquisition authority for DoD IT and NSS programs specified in relevant DoD policy (DoD Directives [DODDs] 5000.02 and 5144.1) clearly preserves the primacy of the DAE in acquisition matters.

DoD CIO R&R

Our analysis of CIO R&R shows that the USC specifies 15 current CIO R&R.[3] Of these, five are strong CIO R&R and are listed in Table S.2.

We found that three of these strong CIO R&R do not pose a risk of conflict in the DoD acquisition process. In other words, they do not pose a risk of process conflict.

Table S.2
Strong DoD CIO R&R in the U.S. Code Applicable to IT and NSS

USC Source	Party	Role and Responsibility	Source of Acquisition Process Conflict
10 USC §2223	DoD CIO	Ensure IT and NSS interoperability Ensure that IT and NSS standards are prescribed for all DoD	Yes
10 USC §2223	Military Department CIO	Ensure that military department IT & NSS are interoperable Ensure compliance with DoD standards	No
44 USC §3534	Agency CIO	Develop and maintain agency-wide information security program and policies	No
44 USC §3544	Agency CIO	Report annually on effectiveness of information security program	No
40 USC §11315	Agency CIO	Develop secure integrated IT architecture Promote effective design and operation of information management processes	No

[2] Although R&R is a plural noun, we often refer to it in the singular for the sake of convenience.

[3] The full list of DoD CIO R&R is discussed in the body of this monograph.

However, two DoD CIO R&R, those in the first and last rows of Table S.2, contain language that could lead to potential conflicts in the DoD acquisition process if these are not resolved by specific guidance in DoD policy.

Our analysis revealed that the first R&R listed in the table, regarding the prescription of standards for IT and NSS, has led to actual process conflicts. We make this assertion on the basis of empirical evidence cited in the body of this monograph. This means that this R&R could lead to executive actions that might potentially complicate or delay the acquisition of DoD command and control, weapon, and intelligence systems.

Our analysis also revealed that the last R&R listed in the table, regarding the development of integrated IT architectures, could also potentially lead to conflicts in the acquisition process. However, in this case we found that the most recent relevant DoD policy, DoDD 8000.01, should eliminate any such potential conflicts. But we highlighted the last CIO R&R entry in Table S.2 in yellow because not all DoD policy appears to be consistent with DoDD 8000.01. As we describe in Chapter Four, some older DoD policies are not consistent with DoDD 8000.01 and with DoDI 5000.2.

We summarize our analysis of DoD CIO R&R below.

The first DoD CIO R&R shown in Table S.2 is from Section 2223 of Title 10 and contains a number of strong R&Rs. In our analysis of the defense acquisition process and the roles of the acquisition and CIO executives in that process, we found that one of these R&R poses a risk of process conflict.

DoD CIO R&R: Prescription of Information System Standards

10 USC §2223 includes one strong DoD CIO R&R:

> Ensure that information technology and NSS standards that will apply through out DoD are prescribed.

We found that process conflicts could and do occur between the DoD CIO, acquisition program milestone decision authorities (MDAs), and the Joint Staff. In the body of this monograph, we present empirical evidence that such process conflicts indeed occur. It is possible that the DoD CIO's standard-setting authorities established in USC 10 Section 2223 could conflict with the USD(AT&L)'s R&R established in USC 10 Section 133 when these executives or their representatives exercise their authorities in the DoD acquisition process. In our review of current DoD policy, we found that current policy does not address this potential process conflict adequately. Therefore we designate it an *actual* process conflict.

This particular process conflict was recognized and addressed in DoDD 5101.7, which defined the R&R for the DoD executive agent for IT standards and also established a governance structure for identifying, prescribing, and implementing IT standards. Most important, it established the IT Standards Oversight Panel (ISOP), trichaired by the DoD CIO, USD(AT&L), and the Vice Chairman of the Joint Chiefs of Staff, to provide direction, oversight, and priorities for IT standards matters and to resolve any issues that may arise. However, DoDD 5101.7 has expired.

To our knowledge, current DoD policy does not provide a complete replacement for DoDD 5101.7. A memorandum was issued by the Deputy Secretary of Defense in May 2007 that cites the expiration of DoDD 5101.7 and preserves the role of the Defense Information Systems Agency (DISA) as the DoD executive agent for IT standards, but it does not extend the tenure of the ISOP or provide any other detailed guidance for resolving conflicts on IT standards that may arise between the DoD CIO and the DAE or their representatives.[4]

Military Department CIO R&R: Ensure Compliance with DoD IT Standards

10 USC §2223 contains strong and advisory R&R for military department CIOs. As described above, we only consider potentially strong R&R to discern if process conflicts may arise between DoD executives.

The USC states that the CIO of a military department shall ensure that IT and NSS are in compliance with standards of the government and DoD.[5] It is important to note that DoD policy should state what constitutes "compliance" with government and DoD standards. The Secretary of Defense (SECDEF) is obligated to issue policy that is consistent with the USC and removes any potential ambiguities or conflicts as to what should constitute compliance with government or DoD standards. In this case, the SECDEF must ensure that adequate compliance data are available in the department for use by the different military services and defense agencies. Per DoDD 5144.1, the availability of these data is the responsibility of the DoD CIO. If that responsibility is carried out effectively, DoD policy should eliminate any potential sources of conflict between DoD executives and the CIOs of military departments in the acquisition process.

Agency CIO R&R: Information Security

The USC assigns the agency CIO the responsibility to develop information security policy and to establish and maintain an information security program. These R&R give the CIO the authority to establish procedures and mechanisms for classifying, assessing, and testing the information assurance (IA) capabilities of IT and NSS. Pending the results of such assessments and tests, IT or NSS developed by an acquisition program will be given an "authority to operate" designation by the appropriate IA approval authority. If the program fails these IA assessments, then the program would

[4] Gordon England, Deputy Secretary of Defense, "DoD Executive Agent for Information Technology (IT) Standards," memorandum, May 21, 2007.

[5] It is important to note that the DoD CIO and the military CIOs are distinct individuals in the DoD. DoDD 5144.1 assigns CIO R&R only to the DoD CIO.

have to take remedial measures to improve its IA status. As with operational testing, it is important to have an independent organization responsible for conducting IA assessments and tests of acquisition programs. Otherwise, there may be opportunities for conflicts of interest to arise in the test process. For these reasons, we do not believe that agency CIO R&R conflict with DAE R&R in the acquisition process.

Agency CIO R&R: Information Security Program Annual Report

This section assigns the agency CIO the responsibility to produce an annual report describing the effectiveness of the information security program. This R&R does not conflict with any DAE R&R.

DoD CIO R&R: IT Architecture Development

In this analysis, we identified potential architecture development R&R in the USC that pose the risk of conflicts in the DoD acquisition process. These apparent conflicts have been resolved by recent changes to DoD policy, as indicated below, but not by older DoD policies that appear to still be in force.

DoDD 8000.01 and DoDI 5000.02, both of which have been recently updated, are consistent with the actual process for developing and validating architectures used in the DoD acquisition process. In this process, integrated joint architectures are developed collaboratively by many parts of the DoD acquisition and requirements communities. No single organization is responsible for, or has the capability to develop, a joint integrated architecture, nor does any single organization have the capability to develop the entire Defense Information Enterprise Architecture (DIEA).

Most important, DoDD 8000.01 gives the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD CIO the responsibility for providing standards for developing, maintaining, and implementing the DIEA, but not for developing IT architectures based on DIEA standards. This means that DIEA standards specified by the DoD CIO can be used to electronically combine and deconflict architecture products developed by different DoD organizations, which is a major technical advance that should reduce the time and cost required to develop integrated architecture products in the decentralized manner now used for this task.

Recommendations

We found that potential process conflicts in the DoD acquisition process could occur in two areas:

- setting IT standards
- developing an IT architecture.

Recent updates to DoD policy, specifically DoDD 8000.01 and DoDI 5000.02, reduce the potential for the second type of process conflict. However, we note here that older DoD policy relevant to this issue, in particular DoDD 5144.1, should be updated to be consistent with DoDD 8000.01 and DoDI 5000.02.

The following recommendations provide ways to minimize or avoid the first type of conflict.

Retain the ISOP and Update DoDD 5101.7

An important role for DoD policy and the senior leaders of the department is to resolve conflicts as they arise. The ISOP, which was established in DoDD 5101.7, is an important organizational tool that enables collaboration among key stakeholder organizations in DoD. We recommend that the provisions of this directive be reissued and that the department (perhaps in this new policy) develop a revitalized organizational structure for reviewing and approving technical standards for IT and NSS.

The new Global Information Grid (GIG) technical guidance (GTG) Configuration Management Board (CMB) is an important step in this direction. The CMB should encourage collaborative development of IT standards with the participation of technical experts from the services who have experience with warfighting systems and their use in the wide range of operational environments characteristic of real-world military operations. IT standards may not be common across the entire range of operational environments found in air, ground, maritime, and space operations. Improved collaboration and conflict resolution mechanisms that can tap into this wide range of engineering and operational expertise should be developed and implemented at lower levels in the department to reduce the time needed by senior leaders to resolve such conflicts.

Screen IT Standards for Technical Maturity

We recommend that DoD screen IT standards for technical maturity because the department has encountered increasing difficulty in developing and reaching consensus on IT standards for military systems. Difficulties in reaching agreement on IT standards may be due to a lack of appreciation of the technical risks associated with implementing new standards or technologies that may have received relatively little vetting or independent review.

Congress has become concerned with increasing technical risk in DoD acquisition programs. This concern led to changes to the DoD acquisition process mandated by recent revisions to the law found in 10 USC §2366(b). One element of this new law requires that the Director of Defense Research and Engineering (DDR&E) review the technical maturity of critical technology elements of programs prior to major milestone reviews. An additional step that may reduce technical risk and help vet technical standards for inclusion in the joint technical architecture (or the GTG) would be a review of the technical maturity of proposed IT standards for DoD programs just prior to major milestone reviews. As with program technology readiness assessments, the review of the technical maturity of proposed IT standards would be conducted immediately before acquisition program milestone reviews. Programs would be required to present evidence that the new technical standards selected for the program are stable, precise, and specific; are available to more than one contractor; and have been successfully demonstrated in a relevant or operationally suitable environment. Such a review would enable the acquisition community to review IT standards proposed by individual programs, by the DoD CIO, or by other organizations. If this review process were conducted in a collaborative fashion, it could increase the level of trust and understanding between the acquisition and CIO communities.

Possible Next Steps

While we have made concrete recommendations based on our review of the USC and several primary DoD policy documents, time and resource limitations prevented us from conducting a comprehensive review of GIG policies and architecture guidance documents. Even in our limited review of GIG policy, we found an older policy memo that conflicts with DoDD 5000.02 and DoDD 8000.01. It is possible—even likely—that other older GIG policy conflicts with the new DIEA concept and approach identified in DoDD 8000.01. A comprehensive review of GIG policy should be conducted to identify conflicts between GIG and DoD policies. Because this body of policy is quite new, automated or semiautomated methods of policy analysis should be developed to facilitate such a policy review. These tools could also be used to assess the consistency of DoD policy in other areas.