This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

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

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

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

Preface

This monograph summarizes research sponsored by the Assistant Secretary of the Navy, Research, Development and Acquisition, Chief Systems Engineer (ASN RDA CHSENG) on the roles and responsibilities (R&R) of the defense acquisition executives (DAEs) and chief information officers (CIOs) defined in the United States Code (USC). The purpose of the study was to identify DAE and CIO roles and responsibilities defined in the law and to examine how these R&R are articulated in Department of Defense (DoD) policy and how conflicts between executives may arise when these officials carry out their duties.

This research should be of interest to DoD officials responsible for formulating, reviewing, or implementing DoD policy that pertains to information technology (IT) or national security systems (NSS) or to the acquisition of weapon systems and platforms that contain IT and NSS. This monograph should also be of interest to members of Congress and congressional staff members who play a role in the development of legislation dealing with DoD weapon system, aircraft, ship, IT, and NSS acquisition programs.

This research was sponsored by the United States Navy and conducted within the Acquisition and Technology Policy Center (ATPC) of 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 Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on RAND's ATPC, contact the Director, Philip Antón, by email at ATPC-Director@rand.org; by phone at 310-393-0411, extension 7798; or by mail at the RAND Corporation, 1776 Main Street, P. O. Box 2138, Santa Monica, California 90407-2138. More information about RAND is available at www.rand.org.

Contents

Figures

Tables

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 decisionmaking 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), tri-

chaired 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.

Acknowledgments

The authors wish to thank Carl Siel, Chief Engineer, Deputy Assistant Secretary of the Navy for Research, Development and Acquisition, and Cheryl Walton, Director, Standards Policy and Guidelines, RDA CHSENG, for their guidance and support of this research. The authors also gratefully acknowledge the contributions of anonymous sources that enhanced our understanding of the complex legislative process and executive branch roles. In addition, we thank several of our colleagues at the RAND Corporation for their insightful observations and careful reviews: Philip Antón, director of the Acquisition and Technology Policy Center in RAND's National Defense Research Institute, Mark Arena, deputy director of the ATPC, Michael Wermuth, manager of RAND's domestic counterterrorism programs, and Ryan Henry, former Principal Deputy Under Secretary of Defense for Policy and current Senior Fellow in International Security Policy at RAND.

Finally, the authors wish to thank Meagan Smith and Sarah Harting for their expert help in preparing this manuscript for publication.

Abbreviations

ACAT	acquisition category
ACAT IAC	An acquisition category designating major automated information systems for which the milestone decision authority is the component CIO. The C refers to Component.
ACAT IAM	An acquisition category designating major automated information systems for which the milestone decision authority is the DoD CIO (the ASD (NII)). The M refers to the Major Automated Information Systems Review Council.
ACAT IC	An acquisition category designating a major defense acquisition program for which the milestone decision authority is the DoD component head or, if delegated, the Component Acquisition Executive (CAE)—Assistant Secretary of the Navy (Research, Development and Acquisition). The C refers to Component.
ACAT ID	An acquisition category designating a major defense acquisition program for which the milestone decision authority is the Under Secretary of Defense for Acquisition, Technology and Logistics. The D refers to the Defense Acquisition Board (DAB).
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ASN RDA CHSENG	Assistant Secretary of the Navy, Research, Development and Acquisition, Chief Systems Engineer
ATPC	Acquisition and Technology Policy Center
CAE	Component Acquisition Executive
CAIG	Cost Analysis Improvement Group

CAPE	cost assessment and program evaluation
CCA	Clinger Cohen Act
CIO	chief information officer
CMB	Configuration Management Board
COCOM	combatant command
DAE	defense acquisition executive
DDR&E	Director, Defense Research and Engineering
DEPSECDEF	Deputy Secretary of Defense
DIEA	Defense Information Enterprise Architecture
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DT&E	developmental test and evaluation
EA	enterprise architecture
GIG	Global Information Grid
GTG	Global Information Grid technical guidance
IA	information assurance
ICD	initial capabilities document
ISOP	IT Standards Oversight Panel
IT	information technology
JROC	Joint Requirements Oversight Council
KIP	key interface profile
MAIS	Major Automated Information System
MDA	milestone deision authority
MDAP	Major Defense Acquisition Program
MS	milestone

NR-KPP	net-ready key performance parameter
NSS	national security systems
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PA&E	program analysis and evaluation
PARCA	performance assessments and root cause analysis
PDR	preliminary design review
PM	program manager
R&R	roles and responsibilities
SAE	service acquisition executive
SDI	Strategic Defense Initiative
SE	systems engineering
SECDEF	Secretary of Defense
TRA	technology readiness assessment
USC	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(C)	Under Secretary of Defense, Comptroller
x USC §*y*	Title *x* United States Code Section *y*
WSARA	Weapon Systems Acquisition Reform Act

CHAPTER ONE

Introduction

This monograph summarizes the results of a research project sponsored by the Assistant Secretary of the Navy, Research, Development and Acquisition, Chief Systems Engineer (ASN RDA CHSENG). It presents an analysis of the legally assigned roles and responsibilities (R&R) of defense acquisition executives (DAEs) and chief information officers (CIOs) as specified in Titles 10, 40, and 44 of the United States Code (USC).

DAE R&R were originally specified in the Goldwater-Nichols Act of 1986;[1] CIO R&R were established later in the Clinger Cohen Act (CCA) in 1996.[2] The Goldwater-Nichols Act focused exclusively on the Department of Defense (DoD). It strengthened civilian oversight of the department by reorganizing DoD and establishing the joint command and control structure of the present day combatant commands. It also defined in broad terms the modern DoD acquisition process. On the other hand, the CCA provides a range of guidance as to how Information Technology (IT) should be managed in the U.S. government. Although the CCA does include passages that pertain specifically to DoD, the CCA is designed to apply more generally to the entire U.S. government, to include all departments and agencies, as well as U.S. government IT.

The objective of this study is to identify and analyze the R&R of the DAE, other acquisition officials, and CIOs as specified in Title 10, Title 40, and Title 44 of the USC for consistency of implementation in DoD policies; to identify potential conflicts in DoD executive R&R as implemented in DoD policies; and to formulate possible remedies to these potential conflicts if none can be found in applicable DoD policy.

For the purposes of this study, R&R are activities, actions, tasks, duties, jobs, or functions assigned to an executive by an authoritative source.[3] Authoritative sources

[1] The Goldwater-Nichols Department of Defense Reorganization Act was signed into law as Public Law 99-433 by President Ronald Reagan on October 1, 1986.

[2] The CCA is Public Law 104-106. The Information Technology Management Reform Act and the Federal Acquisition Reform Act, both signed into law by President William J. Clinton on February 10, 1996, are commonly known as the CCA.

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

include federal law, executive orders, Office of Management and Budget (OMB) circulars, and agency policy documents (in particular, DoD policy documents). As part of this analysis, we identify DAE and CIO R&R that are well defined and those that may be poorly defined or may lead to potential conflicts.

Because acquisition processes vary across U.S. government departments and agencies, and because of the broad, sweeping language typical of congressional law, it is not possible to develop a specific interpretation of IT acquisition, budget, and other processes referred to in the CCA on the basis of the CCA alone. The general nature of the law naturally leads to apparent overlaps and conflicts in executive authority, especially when the law is written to apply to all parts of the U.S. government. In cases where we determine a potential conflict in the USC between the R&R assigned to different DoD executives, we examined the principal DoD policies that established these positions in DoD to determine if and how they treat the potential conflicts.

Approach

The USC is a compilation of permanent federal statutes organized by subject matter. It consists of 50 major partitions called *titles*. The titles are numbered from 1 through 50, and each title addresses a particular subject matter. When new statutory authority is created or existing authorities are amended or rescinded, the USC is updated with historical notes to reflect the latest changes. For this study, we reviewed three pertinent titles of the USC, including the 6,101 pages of text constituting Title 10, "Armed Forces"; the 690 pages in Title 40, "Public Buildings, Property, and Works"; and the 458 pages in Title 44, "Public Printing and Documents." These three titles are the parts of the USC that specify R&R for DoD acquisition officials and CIOs. We used the latest versions of the USC available on the House of Representatives website (because these are typically newer versions than those referenced in many DoD briefings and policy documents). We documented any references in the USC to the DAE, other DoD acquisition officials, CIOs, and architectures, as well as the accompanying R&R.

Overviews of the three relevant titles of the USC are given below.

Title 10. "Armed Forces."[4] Title 10 focuses on the armed forces of the United States. Included in Title 10 are the laws specifying the organization and function of the Office of the Secretary of Defense (OSD). These laws specify the R&R of high-level DoD officials.

[4] The version of Title 10 used in this monograph is the 2008 version, dated October 5, 2009. It was the version of Title 10 available on the House of Representatives website on December 21, 2009.

Title 40. "Public Buildings, Property, and Works."[5] Title 40 concerns procurement and operation of public property. For the purposes of this monograph, the relevant sections of Title 40 deal with the acquisition of information technologies. These sections include previously passed legislation known as the Clinger Cohen Act.

Title 44. "Public Printing and Documents."[6] Title 44 focuses on the laws governing the acquisition of information and public access to that information. Part of Title 40 describes federal information policy, including policies for the acquisition of federal information systems.

DoD acquisition officials and CIOs have myriad responsibilities and play many roles. Our review focused on R&R that are pertinent to IT and national security systems (NSS). We 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 information technology components. As such, we compared the results of our USC analysis to the R&R outlined in Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System,* Department of Defense Directive (DoDD) 5144, *Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO)* and in other selected DoD policy documents.

Information Technology and National Security Systems

Before we consider the R&R of DAEs and CIOs in detail, it is worth pointing out in general terms the types of systems for which these two classes of executives are responsible.

The acquisition authorities of DAEs are broad and comprehensive. DAEs and their duly designated subordinates are responsible for the acquisition of any type of DoD system or platform the U.S. military procures—including ships, aircraft, weapons, command and control, communications, intelligence, and IT business systems. In contrast, the R&R of CIOs are generally restricted to IT and NSS. It is therefore useful to consider how IT and NSS are defined in U.S. law.

Federal law contains two fundamental definitions of the term *information technology.* These two definitions differ by an important related term pertinent to DoD. That term is *national security systems*, which is also defined in the USC. One fundamental definition of IT is found in Title 40, Section 11101; the other is found in Title 44, Section 3502. The difference between these two definitions is that the definition

---

[5] The version of Title 40 used in this report is the 2007 version, dated June 18, 2009. It was the version of Title 40 available on the House of Representatives website on December 21, 2009.

[6] The version of Title 44 used in this report is the 2007 version, dated July 20, 2009. It was the version of Title 44 available on the House of Representatives website on December 21, 2009.

in Title 40 includes NSS by implication, while the definition in Title 44 specifically excludes NSS as defined in Section 11103 of Title 40.

In this monograph, we define IT according to the fundamental definition found in Title 40, Section 11101 (40 USC §11101), the progenitor of all such definitions found in the USC. 40 USC §11101 defines *information technology* as follows:

> (6) Information technology. - The term "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.

Title 44 (44 USC §3502) defines the term IT in a more restrictive manner that explicitly excludes NSS:

> (9) the term "information technology" has the meaning given that term in section 11101 of title 40 but does not include national security systems as defined in section 11103 of title 40;

How does the law define NSS? This question does not have a single answer. There are three distinct definitions of this term in U.S. law. In this monograph, we use the term *national security system* as defined in Title 40, Section 11103:

> (1) National security system. - In this section, the term "national security system" means 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) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

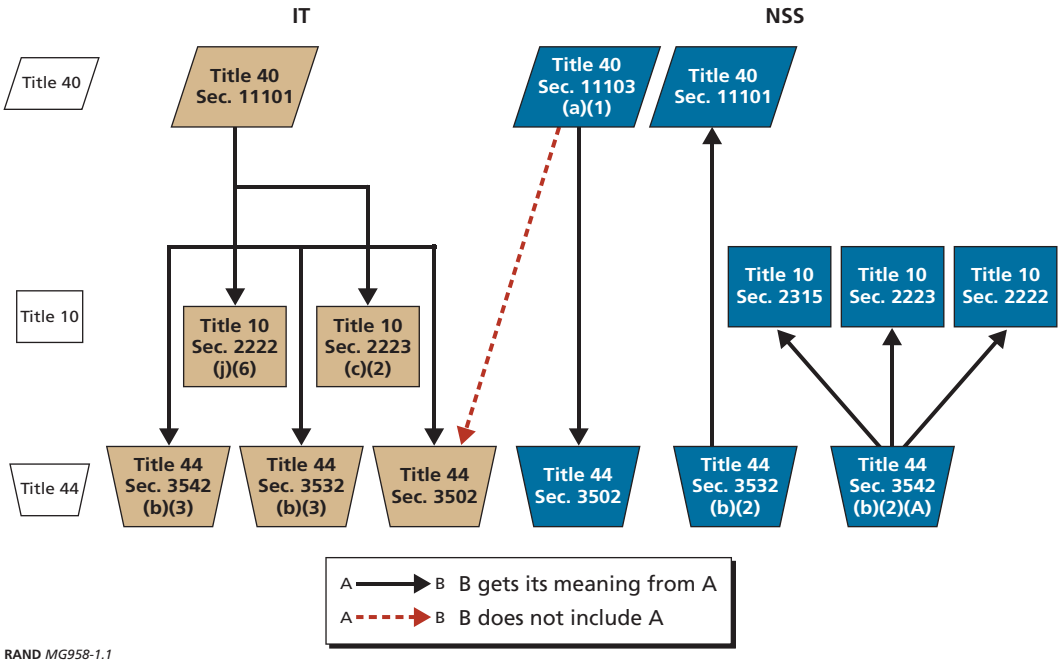
(2) Limitation. - Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Figure 1.1 shows where these different definitions of IT and NSS are found in the USC and the relationships among the definitions. The IT portion of the diagram on the left side shows that the definitions of IT in the USC are for the most part consistent and flow from Title 40 to both Title 10 and Title 44.

The NSS portion of Figure 1.1 shows that there are three definitions of NSS. One definition of NSS is in 40 USC §11103; this definition is also used in 44 USC §3502.[7] A second definition of NSS is in 44 USC §3532 and is also used in 40 USC §11331. The third definition of NSS is in 44 USC §3542. This definition is used in 10 USC §2315, §2222, and §2223. These three definitions are similar in broad terms, but not identical. As shown above, the definition of a national security system in 40 USC §11103 specifies that it is a "telecommunications or information system operated by the Federal Government" and satisfies the five conditions listed. The definition of national security system in 44 USC §3532 includes systems that must satisfy the same five conditions, but national security system in this definition can include systems operated by contractors on behalf of government agencies as well as by the federal government. The definition of national security system in 44 USC §3542 includes all information systems included in the definition of national security system in 44 USC §3532, as well as any information system that "is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy." These differences in definition mean that executive R&R that pertain to NSS could span different collections of systems depending on which

[7] The most common form of codification for the USC is *x* USC §*y*. Hence, Title 44, Section 3502, is 44 USC §3502.

Figure 1.1
Definitions of IT and NSS in the USC



RAND *MG958-1.1*

definition of NSS applies to the R&R. The USC specifies which definitions of IT and/or NSS apply to which sections of the USC.

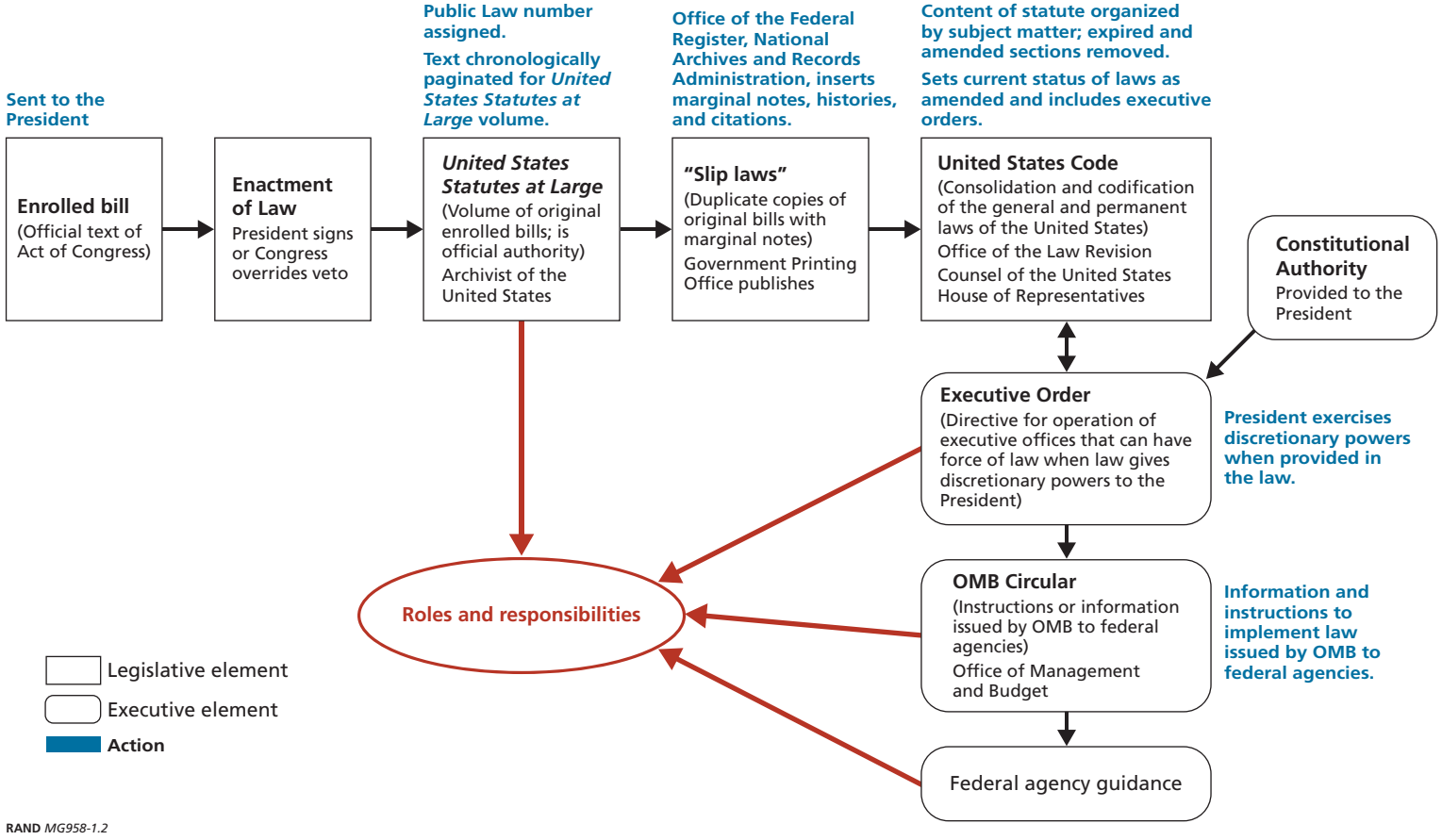
A more detailed analysis of the definitions of the IT and NSS is included in Appendix A.

Legal Process: Assignment of Roles and Responsibilities

Assignment of U.S. government executive R&R can stem from several elements of the legislative and executive processes. Figure 1.2 shows the possible origins of such R&R. These origins include the statute itself, Executive Orders derived either from the federal statutory or from Constitutional Authority provided to the President, OMB circulars, and guidance provided by the federal agencies themselves. Each origin is explained in detail in the following paragraphs.

The official text of an act of Congress, called an *enrolled bill*, can contain R&R. An enrolled bill is sent to the President for signature, and enactment into law occurs when the enrolled bill is signed by the President, the President's veto is overridden by Congress, or the President allows the enrolled bill to become law without his signature. The enactment document becomes the official authority and is forwarded to the

Figure 1.2
Assignment of Roles and Responsibilities



Archivist of the United States, who assigns a public law number to the document and chronologically places the document in *United States Statutes at Large*. This volume serves as the collection of official statutes and is the ultimate authority should any need for clarification arise.

The archivist authorizes the Government Printing Office to publish copies of the official authority document. These copies are then annotated with marginal notes of explanatory material, histories, and citations. The copies are known as *slip laws.* Slip laws are forwarded to the Office of Law Revision Counsel of the U.S. House of Representatives. This body partitions the slip laws by subject matter and inserts the portions of statute text along with any historical notes or explanatory information as appropriate in the United States Code. When the content of the statute is inserted in appropriate parts of the USC, any expired, rescinded, and amended parts of the USC are removed and the actions are noted in the statutory history. In particular, R&R specified in statutes are updated through this codification process. Moreover, the USC sets the status of current statutes through the codification process and, as such, is routinely used as a primary source of statutory legal citations.

An *executive order* is a directive issued by the President that implements law. Some executive orders, such as those issued in response to discretionary powers granted to the President through acts of Congress, have the force of law. Other executive orders, such as those issued to direct the operations of executive agencies by setting the policies that agencies must follow to carry out laws, do not necessarily have the force of law. Both types of executive orders can contain R&R.

The Office of Management and Budget resides within the Executive Office of the President. One of the functions of OMB is to oversee and coordinate federal policy. Hence, OMB has the responsibility to ensure that operations of federal agencies are in accordance with federal policies. Toward this end, OMB can issue circulars, which are instructions or information directing the operations of federal agencies. These circulars can also contain R&R.

Finally, the heads of federal agencies can assign R&R to agency officials. Such assignments are made in accordance with statutory authority, executive orders, OMB circulars, and other guidance provided to agency heads with regard to management practices.

Monograph Outline

This document is organized as follows. This chapter elaborates on the objective of the study, discusses our approach, and presents some background material to provide context for understanding the analysis. In the next chapter, we explain the roles and responsibilities of the DAE as set out in Titles 10, 40, and 44 of the United States Code. Chapter Three explains the roles and responsibilities of the CIO specified in

Titles 10, 40, and 44. Chapter Four presents detailed analyses that focus on how architectures are treated in Titles 10, 40, and 44. Chapter Five continues detailed analyses of selected issues—in particular, passages that could potentially lead to conflicts in R&R. Chapter Six presents our findings based on the analyses discussed in the previous chapters, and Chapter Seven presents our recommendations based on those findings. Appendix A provides a detailed analysis of the relationships between definitions of the terms of IT and NSS that appear in the U.S. Code. Appendix B provides an overview of DoD directives and instructions and describes which DoD executives have the authority to issue such policy documents. Appendix C summarizes two R&R that were not considered relevant to this study.

CHAPTER TWO

The Defense Acquisition Executive

This chapter describes the R&R of the DAE and other high-level DoD acquisition officials in the acquisition system. The chapter first presents the authorities of the DAE as defined by the U.S. Code and further specified by DoD policy. The chapter lists those R&R relevant to the acquisition system, and concludes with a detailed discussion of the Weapon Systems Acquisition Reform Act of 2009 (Public Law 111-23), which specifies more recent changes in organization and policies for the acquisition system.

Roles and Responsibilities of DoD Acquisition Officials

The DAE and other DoD acquisition officials derive their authority from the USC (Titles 10, 40, and 44). Subsequent DoD issuances provide more detailed directives and instructions on operations.

Table 2.1 lists relevant sections of the USC and summarizes which DoD official is identified and the R&R they are granted in the specific sections of the USC. Below, we examine many of these key sections of the law.

Section 139 of Title 10 establishes the position of Director, Operational Test and Evaluation (OT&E), which is the independent operational test authority for DoD acquisition programs. The director of OT&E (DOT&E) reports to the Secretary of Defense (SECDEF).

Similarly, Section 139a of Title 10 establishes the position of Director, Defense Research and Engineering (DDR&E), who reports to the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). The DDR&E position is concerned primarily with research and development (R&D) of new technologies. The majority of these R&D activities occur outside of and before the start of DoD acquisition programs, which are usually tasked with using mature technologies.

Table 2.1
Acquisition-Related R&R in the U.S. Code

Source	Section Heading	Party	Type of R&R
10 USC §133	Under Secretary of Defense for Acquisition, Technology, and Logistics	USD(AT&L)	Supervises the acquisition system
10 USC §133	Under Secretary of Defense for Acquisition, Technology, and Logistics	USD(AT&L)	Establishes policy
10 USC §133	Under Secretary of Defense for Acquisition, Technology, and Logistics	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
10 USC §133	Under Secretary of Defense for Acquisition, Technology, and Logistics	USD(AT&L)	Is designated the DAE
10 USC §133	Under Secretary of Defense for Acquisition, Technology, and Logistics	USD(AT&L)	Authorizes a senior acquisition official within the Office of USD(AT&L) to oversee the exercise of any DoD acquisition authority
10 USC §139	Director of Operational Test and Evaluation (OT&E)	DOT&E	Establishes DOT&E R&R as principal advisor to SECDEF on OT&E
10 USC §139a	Director of Defense Research and Engineering (DDR&E)	DDR&E	Establishes DDR&E R&R
10 USC §186	Defense Business System Management Committee	USD(AT&L)	Establishes committee with USD(AT&L) as a member, committee R&R
10 USC §1702	Under Secretary of Defense for Acquisition, Technology, and Logistics authorities and responsibilities	USD(AT&L)	Has all powers, duties, and functions over the acquisition workforce
10 USC §2430	Major Defense Acquisition Program (MDAP)	Secretary of Defense	Defines MDAP Grants authority to designate a MDAP program
10 USC §2445A	Major Automated Information System (MAIS) programs	Secretary of Defense	Defines MAIS Grants authority to designate a MAIS program
40 USC §11314	Authority to acquire and manage IT	Head of executive agency	Grants acquisition authority with particular attention to multi-agency IT acquisitions

NOTE: Although the official title of the USD(AT&L) is Under Secretary of Defense for Acquisition, Technology and Logistics, the statute adds a comma after the word "Technology": Under Secretary of Defense for Acquisition, Technology, and Logistics.

USC Acquisition Official R&R Assignments

Section 133 of Title 10 defines the R&R for USD(AT&L). One of the principal activities of USD(AT&L) is to oversee the DoD acquisition system. Title 10 specifically gives the USD(AT&L) the authority to set policies for the DoD acquisition system:

> (b) Subject to the authority, direction, and control of the Secretary of Defense, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall perform such duties and exercise such powers relating to acquisition as the Secretary of Defense may prescribe, including -
>
> (1) supervising Department of Defense acquisition;
>
> (2) establishing policies for acquisition (including procurement of goods and services, research and development, developmental testing, and contract administration) for all elements of the Department of Defense.

In addition, the USD(AT&L) is responsible for operation of the DoD acquisition system:

> (c) The Under Secretary -
>
> (1) is the senior procurement executive for the Department of Defense for the purposes of section 16(c) of the Office of Federal Procurement Policy Act (41 U.S.C. 414(c));
>
> (2) is the Defense Acquisition Executive for purposes of regulations and procedures of the Department providing for a Defense Acquisition Executive.

When other DoD combatant commands or agencies are given acquisition authority, the USD(AT&L) still performs an oversight function over those activities:

> The SECDEF designates a senior acquisition official within the Office of USD(AT&L) to oversee the exercise of acquisition authority by
>
> - any commander of a combatant command who is authorized to exercise acquisition authority
> - any head of a defense agency who is designated by the SECDEF to exercise acquisition authority.

In other words, all acquisition activities within DoD are designated to fall under the oversight of the USD(AT&L).

Service Acquisition Executive

Each service in turn designates a service acquisition executive (SAE) who acts for the respective military department. Because programs are usually managed by a service, the SAE is responsible for the management of the acquisition workforce, for monitoring of performance by the workforce, and for reporting to higher levels of the acquisition system.

With respect to management of the workforce, the SAE is responsible for appointment and performance reviews of the program manager and the deputy program manager. Service acquisition duties also include the education and training of the acquisition workforce:

- "Subject to the authority, direction, and control of the Secretary of the military department concerned, the service acquisition executive for each military department shall carry out all powers, functions, and duties of the Secretary concerned with respect to the acquisition workforce within the military department concerned. . . ." (10 USC §1704)
- "The Secretary of Defense shall issue regulations defining what constitutes major milestones for purposes of this section. The service acquisition executive of each military department shall establish major milestones at the beginning of a major defense acquisition program consistent with such regulations and shall use such milestones to determine the assignment period for program managers and deputy program managers. . . ." (10 USC §1734(c))
- "The Secretary of each military department, acting through the service acquisition executive for that department, shall establish and implement the education and training programs authorized by this subchapter." (10 USC §1741(c))

With regard to procurement, the SAE is responsible for contract services within the department:

- ". . . service acquisition executive of each military department shall be the senior official responsible for the management of acquisition of contract services for or on behalf of the military department." (10 USC §2330(a)(2))

The SAE is also responsible for notifying responsible authorities when significant cost overruns are incurred and Congress needs to be notified.

- ". . . the service acquisition executive shall determine whether the current program acquisition unit cost for the program or subprogram has increased by a percentage equal to or greater than the significant cost growth threshold, or the critical cost growth threshold, for the program or subprogram." (10 USC §2433(d)(2)

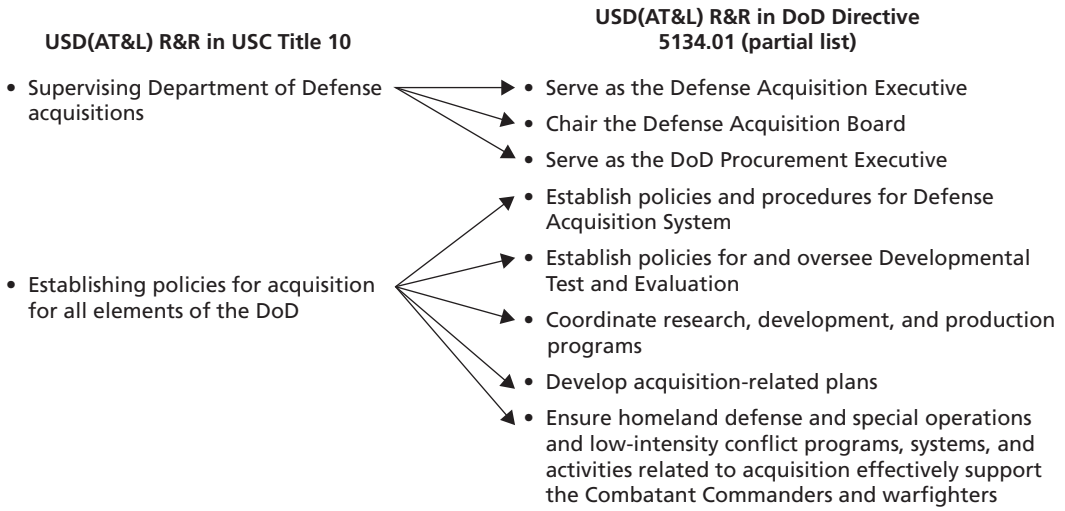
- "If, based upon the service acquisition executive's determination, the Secretary concerned determines that the current program acquisition unit cost has increased by a percentage equal to or greater than the significant cost growth threshold or critical cost growth threshold or that the procurement unit cost has increased by a percentage equal to or greater than the significant cost growth threshold or critical cost growth threshold, the Secretary shall notify Congress in writing of such determination and of the increase with respect to the program or subprogram concerned." (10 USC §2433(d)(3)).

DoD Policies Defining DoD Acquisition Executive R&R

High-level DoD policy is established in DoDDs and DoDIs. These DoD issuances are derived from pertinent provisions of the U.S. Code and provide more detailed guidance for implementation. An overview of DoDDs and DoDIs is provided in Appendix B.

DoD Directive 5134.01 further defines the R&R of USD(AT&L) including functions within the acquisition system. Figure 2.1 shows some of these functions and their derived authority from U.S. Code Title 10.

Figure 2.1
DoD Directives and Instructions Further Define the R&R Within the Acquisition System



RAND *MG958-2.1*

DoD Directive 5134.01 provides more detail specifying the R&R of the USD(AT&L) in the defense acquisition system, authority over other defense agencies, and the role in overseeing acquisition by other organizations with acquisition authority.

The operation of the defense acquisition system is further defined for specific program management. This specification is contained in USC Title 10 and DoDD 5000.01, *Defense Acquisition System*. These specify a hierarchy of management beginning with the DAE, who supervises the system; the milestone decision authority (MDA), who decides when a program is ready to move from one milestone to another; and the program manager, who manages the program to achieve objectives and is accountable for performance.

Specifically, DoDD 5000.1 states (p. 4):

> The **Defense Acquisition Executive** (DAE) is the USD(AT&L) who has responsibility for supervising the Defense Acquisition System. The DAE takes precedence on all acquisition matters after the Secretary and the Deputy Secretary.
>
> The **Milestone Decision Authority** (MDA) is 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.
>
> The **Program Manager** (PM) is 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 MDA.

The MDA for any program is determined according to the category of the program as shown on Table 2.2.

Acquisition Categories (ACATs) range from level I to level III, depending mostly on the size of the program (in dollars) or whether there is special interest. These categories are specified in Title 10, and the MDA is identified in DoD Instruction 5000.02, *Operation of the Defense Acquisition System*. According to this categorization, the MDA could be

- for ACAT I programs, either the USD(AT&L) (ACAT ID) or the head of a DoD component or component acquisition executive (CAE) (ACAT IC). Designation of a program as ACAT IC is decided by the DAE. The latter authority cannot be further delegated
- for ACAT IA programs, either USD(AT&L) or a designee (ACAT IAM), or the head of a DoD component or CAE (ACAT IAC). The ACAT IA category is for MAIS. The USD(AT&L) has the discretion to designate the ASD(NII), who is also the DoD CIO, as the relevant MDA for programs in

Table 2.2
DoD Acquisition Program Categories

Acquisition Category	Reason for ACAT Designation	Decision Authority
ACAT I	Major Departmental Acquisition Program Total RDT&E more than $365 million Total procurement more than $2.190 billion MDA designation as special interest	ACAT ID: USD(AT&L) ACAT IC: Head of DoD component or CAE (not further delegable)
ACAT IA	Major Automated Information System (MAIS) Designated by the MDA Exceeds $32 million for definition, design, development, and deployment in any single year or $378 million (through life cycle of system) MDA designation as special interest	ACAT IAM: USD(AT&L) or designee ACAT IAC: Head of DoD component or CAE (not further delegable)
ACAT II	Does not meet criteria for ACAT I Major system total RDT&E expenditure is more than $140 million or procurement is more than $660 million MDA designation	CAE or individual designated by CAE
ACAT III	Does not meet criteria for ACAT II or above Is an automated information system that is not a MAIS	Designated by CAE

NOTES: All amounts in fiscal year (FY) 2000 dollars. See the abbreviations list for acquisition category definitions.

this category. The designation of a program as ACAT IAC is decided by the DAE, and that authority cannot be further delegated
- for ACAT II programs, the CAE or individual decided on by the CAE
- for ACAT III programs, designated by the CAE.

Note that the DAE is ultimately responsible for milestone decisions. For a MAIS program, authority can be delegated to the CIO. In lieu of this delegation, the unique authority of the CIO lies in providing standards for developing, maintaining, and implementing a Defense Information Enterprise Architecture (DIEA) that will ensure interoperability, as we will see in the next section.

Acquisition executives can and do overrule CIO-established standards if the proposed standards compromise the affordability, schedule, or other operational requirements of the acquisition program. In this respect, it is important to note that specific IT or NSS standards are usually associated with specific IT or NSS technologies and technology implementations. The review and approval of such technologies fall under the purview of the MDA. For example, such a review is the preliminary design review (PDR) for a program, which now must occur prior to Milestone B. Prior to PDR, the program office must submit a technology readiness assessment (TRA) to the MDA to ensure that all critical technologies are sufficiently mature to enable system develop-

ment. As noted earlier and established in DoDI 5000.02, the acquisition executive has the authority to balance cost, schedule, and requirements to ensure an executable program that will have the desired system outcome. The acquisition executive can rule out the use of any risky technology at a milestone decision if the technology is deemed immature or would compromise the overall cost schedule of the program. Consequently, because new IT standards may be associated with new technologies, decisions made by the acquisition authority or MDA for a program may conflict with IT standards established with the CIO.

Weapon Systems Acquisition Reform Act of 2009

In May 2009, Congress passed the Weapon Systems Acquisition Reform Act of 2009, Public Law 111-23. The intent of this act is to increase transparency in programmatic management of weapon system acquisition. The act was motivated by congressional concern over cost growth and difficulties in meeting technical requirements. The act specifically requires DoD to institute new organizations for review of program performance and adds reporting requirements to Congress.

The act requires the appointment of the senior official in OSD for performance assessments and root cause analysis (PARCA). This official is charged with conducting performance assessments of major acquisition programs to determine the underlying causes cost, schedule, or performance problems, and with issuing policies, procedures, and guidance for conducting such assessments, and with advising acquisition officials on the performance of major acquisition programs.

On January 4, 2010, the Deputy Secretary of Defense issued a memorandum on behalf of the SECDEF that established the Office of the Director for PARCA within the Office of the USD(AT&L), Office of the Assistant Secretary of Defense for Acquisition (ASD(A)), which thereby eliminates any potential conflict of PARCA R&R with the R&R of DoD acquisition executives.[1]

Appendix D presents a more detailed discussion of the provisions of the Weapon Systems Acquisition Reform Act of 2009.

---

[1] Deputy Secretary of Defense Memorandum, "Designation of the Senior DoD Official for Performance Assessments and Root Cause Analyses (PARCA) Within the Office of the Secretary of Defense," January 4, 2010.

CHAPTER THREE

Chief Information Officer

The position of CIO for each U.S. government agency is established in 44 USC §3506. This section of the USC specifies the positions of DoD CIO and service CIOs that should exist in DoD. Table 3.1 indicates who appoints people to these positions.

In DoD, R&R are assigned to CIOs to support and execute IT-related activities associated with the requirements process; the planning, programming, budgeting, and execution process; and the defense acquisition system. As such, CIO R&R govern these aspects of DoD IT, including, in some cases, warfighting systems, defense business systems, defense intelligence systems, as well as IT systems within the enterprise information environment and systems that implement joint capabilities.

Our examination of Titles 10, 40, and 44 indicates that these titles collectively specify 17 individual R&R for CIOs.

CIO R&R and Definitions of IT and NSS

Our analysis shows that some current CIO R&R apply only to IT and others to both IT and NSS.

For this analysis, we associate CIO R&R with the particular definitions of IT and NSS found or implied in the USC. Below, we discuss the complexity involved in this process. We analyzed the convoluted definitions of IT and NSS and the exact text that specifies current CIO R&R. Note that the definition of IT in 40 USC §11101 appears

Table 3.1
CIO Designation and Reporting Authority

Source	Section Heading	Party	Type of R&R
44 USC §3506	DoD CIO	Secretary of Defense	Designates the DoD CIO
44 USC §3506	Service CIO	Service Secretaries	Designates the service CIOs

to include NSS, but three different definitions of NSS occur in the USC.[1] Finally, sections of the USC that specify CIO R&R may use such terms as *information systems* or *information resources*, which usually include IT. However, definitions of information systems and information resources can also vary throughout the USC. Below, we describe CIO R&R and trace them to specific definitions of IT and NSS, concentrating on the nine CIO R&R that are applicable to both IT and NSS, and then on the six CIO R&R that are applicable to IT only. For completeness, we also mention the two additional CIO R&R that are in the USC but were not considered relevant for the purposes of this study. These two R&R are summarized in Appendix C.

The 15 current and relevant R&R are shown in Tables 3.2 and 3.3. Both tables follow the same format. In each table, the first column shows the section of the USC in which the R&R is found; the second column provides a short title of the R&R; the third lists the executives who are assigned the R&R by federal law; the fourth summarizes what the executive is charged with doing; the fifth lists the definition of IT that applies to this R&R (how the term IT is used in the description of the R&R in the USC); and the sixth column lists the definition of NSS that applies to the R&R.

CIO R&R Applicable to IT and NSS

Our evaluation shows that nine current CIO R&R are applicable to both IT and NSS. Of these nine, six current CIO R&R contain the terms *information technology* and *national security system*. In these six cases, each R&R explicitly specifies a reference for definitions of IT and NSS.

CIO R&R with Explicit Reference to IT and NSS Definitions

The six R&R that are applicable to both IT and NSS and that include specific definitions of these terms are

- DoD CIO in "Information Technology: Additional Responsibilities of Chief Information Officers—DoD CIO" in 10 USC §2223
- Military department CIOs in "Information Technology: Additional Responsibilities of Chief Information Officers—Military Department CIOs" in 10 USC §2223
- Agency CIO in "Federal Information Technology—Create agency Chief Information Officers" in 40 USC §11101

[1] For instance, the definition of NSS in 44 USC §3542 applies to use of the term in 44 USC §3542 through 44 USC §3549 unless otherwise specified. Moreover, even if a section of the USC that describes CIO R&R does not specifically use the terms *information technology* or *national security system,* that R&R may still apply to IT or NSS through references to other portions of the USC that do apply to IT or NSS.

Table 3.2
Summary of CIO R&R Applicable to IT and NSS

USC Source	Section Heading	Party	Nature of R&R	Definition of IT	Definition of NSS
10 USC §2223	IT: DoD CIO	DoD CIO	Ensure that IT, NSS are interoperable Ensure that IT, NSS standards are prescribed for all DoD	40 USC §11101	40 USC §11103
10 USC §2223	IT: Military department CIOs	Military department CIO	Ensure that military department IT and NSS are interoperable Ensure that systems comply with DoD standards	40 USC §11101	40 USC §11103
40 USC §11101	Federal IT: Create agency CIOs	Agency CIO	Advisor for accountability for information resource management	40 USC §11101	NSS not in text, but 40 USC §11101 definition of IT may include NSS
40 USC §11101	Federal IT: Establish CIO Council	DoD CIOs Military department CIOs	Participate in forum to improve IT resource management	40 USC §11101	NSS not in text, but 40 USC §11101 definition of IT may include NSS
44 USC §3534	Information Security	Agency CIO	Develop and maintain agency-wide information security program and policies	40 USC §11101	44 USC §3532
44 USC §3544	Information security protection	Agency CIO	Report annually on effectiveness of information security programs	40 USC §11101	44 USC §3542
40 USC §11315	Agency CIO	Agency CIO	Develop secure integrated IT architecture Promote effective design of information resources management processes	40 USC §11101	NSS not in text, but 40 USC §11101 definition of IT may include NSS
40 USC §11101	Computer software piracy in Executive Order 13103	CIO Council	Make recommendations to prevent use of unauthorized software	40 USC §11101	NSS not in text but 40 USC §11101 definition of IT may include NSS
40 USC §11316	Accountability	Agency CIO	Agency head consults CIO on policies for information systems that provide financial data to agency	IT part of "information systems" per 44 USC §3502	Applies to NSS via 40 USC §11103

Table 3.3
Summary of CIO R&R Applicable to IT Only

USC Source	Section Heading	Party	Nature of R&R	Definition of IT	Definition of NSS
10 USC §2222	Defense business systems: architecture, accountability and modernization	ASD(NII) DoD CIO	Responsible and accountable for defense business for IT or IA	40 USC §11101	NSS explicitly excluded
44 USC §3506	Information resources management	DoD, Military department CIOs	Ensure agency compliance with implementing agency information policy	IT not in text, but definition of information resources in 44 USC 3502 includes IT	NSS not in text and definition of IT in 44 USC §3502 excludes NSS
44 USC §3603	Chief Information Officers Council	CIO Council	Promote use of common performance measures for info resources management	IT not in text, but definition of information resources in 44 USC §3502 includes IT	NSS not in text and definition of IT in 44 USC §3502 excludes NSS
10 USC §185	Financial Management Modernization Executive Committee	DoD CIO	Member of Financial Management Modernization Executive Committee	IT not in text, but Financial Management System can be IT	NSS not in text
44 USC §3601	Electronic government (e-Government)	CIO Council	Provide recommendations on e-Government to administrator of Office of Electronic Government	IT not in text, but definition of information resources in 44 USC §3502 includes IT	NSS not in text and definition of IT in 44 USC §3502 excludes NSS
44 USC §3602	Management and promotion of electronic government	CIO Council	Provide recommendations on e-Government to administrator of Office of Electronic Government	IT not in text, but definition of information resources in 44 USC §3502 includes IT	NSS not in text and definition of IT in 44 USC §3502 excludes NSS

- DoD CIO and military department CIOs in "Federal Information Technology—Establish CIO Council" in 40 USC §11101
- Agency CIO in "Federal Agency Responsibilities" in 44 USC §3534
- Agency CIO in "Federal Agency Responsibilities" in 44 USC §3544.

These CIO R&R are described in the following paragraphs.
The DoD CIO R&R specified in 10 USC §2223 charges the DoD CIO to

- ensure the interoperability of IT and NSS throughout DoD
- ensure the prescription of IT and NSS standards that apply throughout DoD

- provide for the elimination of duplicate IT and NSS in military departments and defense agencies
- maintain a consolidated inventory of DoD mission-critical and mission-essential information systems
- develop and maintain contingency plans for responding to a disruption to the operation of any of these systems
- review and provide recommendations to the Secretary of Defense on IT and NSS budget requests.

The R&R for the military department CIOs specified in 10 USC §2223 charges these CIOs to

- ensure that IT and NSS in their respective military departments are interoperable with all other relevant DoD and government IT and NSS
- ensure that IT and NSS within their respective departments comply with DoD and other government standards
- coordinate with the Joint Staff on IT and NSS
- review and provide recommendations within their respective departments on IT and NSS budget requests.

44 USC §3506(a)(2)(B) allows DoD to designate a CIO for the purpose of establishing clear accountability for information resources management.

44 USC §3603 establishes the Chief Information Officers Council (CIO Council) as the primary interagency forum dedicated to improving agency practices pertaining to the design, modernization, use, sharing, and performance of agency information resources. The CIO Council is charged to

- develop recommendations for information resources management policies and requirements
- identify opportunities and sponsor cooperation in using information resources as well as share ideas to improve management of information resources
- address personnel needs regarding information resource management
- make recommendations to OMB on the government-wide strategic plan for information resources that OMB is charged with developing.

The DoD CIO and military department CIOs are all members of the CIO Council and are required to participate in the council activities.

44 USC §3534 directs the Secretary of Defense to delegate to the DoD CIO the authority to ensure compliance with agency requirements included in Subchapter III, "Information Security," of Chapter 35, "Coordination of Federal Information Policy," in Title 44 of the USC. As such, the DoD CIO is charged to do the following:

- designate a senior DoD information security officer whose primary duty is DoD information security
- develop and maintain a DoD-wide information security program
- develop and maintain DoD-wide information security policies, procedures, and controls
- train and oversee information security personnel
- assist senior DoD officials in ensuring that information security is provided for the information and information systems that support DoD operations and assets.

44 USC §3544 repeats the direction to the Secretary of Defense to delegate to the DoD CIO the authority to ensure compliance with agency requirements included in Subchapter III, "Information Security," of Chapter 35, "Coordination of Federal Information Policy," in Title 44 of the USC. The DoD CIO is charged with the same R&R as stated in 44 USC §3534, with one additional duty. That additional duty is that the DoD CIO must also report annually to the Secretary of Defense on the effectiveness of the DoD information security program and progress on any remedial actions related to information security.

CIO IT and NSS R&R Without Explicit Reference to an NSS Definition

Three CIO R&R contain the term IT and do not contain the term NSS. However, in these cases, the USC specifies a reference for a definition of the term IT that includes NSS. Hence, these R&R are deemed applicable to NSS. Two of these CIO R&R are specified for the following:

- CIO in "Agency Chief Information Officer," 40 USC §11315
- CIO Council in Executive Order 1310.3. "Computer Software Piracy" is the title of Executive Order 13103.

The R&R specified for the agency CIO in the paragraph entitled "Agency Chief Information Officer" in 40 USC §11315 charges the agency CIO with responsibilities for IT architecture and IT resource management processes. As such, the agency CIO is charged to

- develop, maintain, and facilitate implementation of an agency IT architecture that is sound, secure, and integrated
- promote the effective and efficient design and operation of information resources management processes.

This part of federal law also explicitly states that information resources management duties are the primary responsibility of the agency CIO. These duties include monitoring and evaluating the performance of agency IT programs and advising the agency head on the continuation, modification, or termination of such programs. The

agency CIO is also required to perform assessments of agency IT personnel needs as part of an annual strategic planning and performance evaluation exercise on information resources.

Executive Order 13103 implements part of Chapter 111 of Title 40, which contains 40 USC §11101 and charges the CIO Council to

- provide recommendations (in an advisory role) for improving executive agency and OMB practices on the acquisition and use of computer software
- monitor and combat the use of unauthorized computer software.

The DoD CIO and military department CIOs take on this advisory role as members of the CIO Council.

The final current CIO R&R applicable to both IT and NSS is included in 40 USC §11316. This R&R provides a consulting role for the agency CIO to assist the agency head and agency chief financial officer with establishing policies and procedures to ensure agency information systems are designed, developed, maintained, and used effectively to provide agency financial and program performance data.

See Table 3.2 for a summary of the nine CIO R&R in Title 10, Title 40, and Title 44 of the United States Code that apply to both IT and NSS.

CIO R&R Applicable to IT Only

Our evaluation shows that six CIO R&R apply only to IT. These six CIO R&R are described in the following paragraphs and summarized in Table 3.3.

In 10 USC §2222, IT is defined as we define it in this monograph but with NSS explicitly excluded. In that R&R, the Secretary of Defense is required by law to delegate responsibility for review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of any defense business systems, the primary purpose of which is to support the information technology infrastructure or information assurance activities of DoD to the ASD(NII) and DoD CIO. This portion of the law makes the ASD(NII) and DoD CIO responsible and accountable for these defense business systems.

44 USC §3506 does not include the term IT but does include the term *information resources*, which in this case appears to include IT but explicitly excludes NSS. The CIO R&R in 44 USC §3506 charges the DoD CIO and military department CIOs with ensuring agency compliance with prompt, efficient, and effective implementation of the information policies and information resource management responsibilities in Subchapter I of Chapter 35 in Title 44. These policies and responsibilities include managing information resources to improve the integrity, quality, and utility of information to all users within and outside the agency. In addition, the CIOs are to serve in a

consulting role to program officials to define program information needs and develop strategies, systems, and capabilities to meet those needs.

Similarly, 44 USC §3603 does not include the term IT but does include the term *information resources,* which in this case does appear to include IT but also explicitly excludes NSS. The CIO R&R in 44 USC §3603 charges the CIO Council with promoting the development and use of common performance measures for agency information resources management. In addition, the CIO Council is to develop recommendations on information resources management policy; assist in the identification, development, and coordination of multi-agency projects to improve government performance through use of IT; and work as appropriate with the National Institute of Standards and Technology to develop recommendations for IT standards.

10 USC §185 does not include the terms IT or NSS. The R&R described in 10 USC §185 pertain to financial management systems (*financial management systems* is not defined). However, our interpretation of the definitions of the term IT leads us to conclude that all or major parts of financial management systems can be IT. Hence, we include the R&R in 10 USC §185 as an R&R applicable to IT. This R&R stipulates that the DoD CIO is a member of the Financial Management Modernization Executive Committee. This committee is accountable to the Senior Executive Council. The duties of the committee include establishing a process to ensure that critical DoD accounting, financial management, and data feeder systems are compliant with federal requirements; developing a management plan for the implementation of a compliance process; supervising and monitoring implementation of the management plan; ensuring that the financial management enterprise architecture and investments in the architecture are in accordance with the DoD financial management modernization process and the architecture framework for DoD command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) functions; and providing an annual account of all DoD financial management projects.

44 USC §3601 and 44 USC §3602 do not include the term IT, but do include the term *information resources,* which in this case does appear to include IT but explicitly excludes NSS. The CIO R&Rs in 44 USC §3601 and 44 USC §3601 state that the CIO Council will provide recommendations pertaining to e-Government to the director of the Office of Electronic Government. The DoD CIO and military department CIOs, as members of the CIO Council, shall participate in formulating these recommendations.

The R&R that apply to IT only are summarized in Table 3.3. The majority of these apply to nonwarfighting systems, such as defense business systems or financial management systems, or to e-Government initiatives.

Strong and Advisory CIO R&R

The 15 current DoD CIO R&R that are applicable to IT and NSS or only to IT span a spectrum of duties, actions, and functions. Some of these R&R include high-level, unique decisionmaking authorities, such as setting, establishing, or directing policy or overseeing the implementation of policy. These R&R are not at first glance controlled or potentially circumscribed by other DoD executives. We therefore term them *strong* R&R.

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

Strong R&R are of primary interest in this study because these are the R&R that could potentially result in conflict with the R&R of other government executives. Advisory R&R are unlikely to conflict with the R&R of other executives because advisory roles do not include unique decisionmaking authority.

Of the 15 current CIO R&R, only seven are strong R&R. Among the nine current CIO R&R that are applicable to both IT and NSS, five are strong R&R; and of the six current CIO R&R that are applicable to IT only, two are strong R&R.

Table 3.4 summarizes the seven current CIO R&R that are strong R&R.

DoD Policies Defining CIO R&R

DoD Directive 5144.1 further defines the R&R of the ASD(NII)/DoD CIO. This directive specifies that the DoD CIO will report directly to the Secretary and Deputy Secretary of Defense. It also assigns a number of roles and responsibilities to the CIO. We will not review all these R&R in this monograph and instead refer the reader to the directive itself. However, we do wish to point out that the R&R established in this directive follow closely those established in the USC. It is important to note that DoDD 5144.1 does assign the CIO two key acquisition authorities (pp. 6–7):

> 3.7. With respect to space: 3.7.2. Oversee the Space Major Defense Acquisition Program activities of the DoD Executive Agent for Space in coordination with the USD(AT&L), and in coordination with the USD(I) for space-based intelligence system acquisitions, as delegated by the USD(AT&L)
>
> . . .
>
> 3.9. With regard to systems acquisition:
>
> 3.9.1 Serve as the Milestone Decision Authority for Major Automated Information Systems and other acquisition programs, as delegated by the USD(AT&L), with responsibility for developing and enforcing the policies and practices of

Table 3.4
Summary of DoD CIO Strong R&R

USC Source	Section Heading	Party	Nature of R&R	Includes NSS
10 USC §2223	IT—DoD CIO	DoD CIO	Ensure IT and NSS interoperability Ensure that IT and NSS standards are prescribed for all DoD	Yes
10 USC §2223	IT—military department CIOs	Military department CIO	Ensure that military department IT & NSS are interoperable Ensure compliance with DoD standards	Yes
44 USC §3534	Information security	Agency CIO	Develop and maintain agency-wide information security program and policies	Yes
44 USC §3544	Information security protection	Agency CIO	Report annually on effectiveness information security program	Yes
40 USC §11315	Agency CIO	Agency CIO	Develop secure integrated IT architecture Promote effective design and operation of information management processes	NSS not in text, 40 USC §11101 definition of IT may include NSS
10 USC §2222	Defense business systems: architecture, accountability, and modernization	ASD(NII), DoD CIO	Responsible and accountable for defense business for IT or information assurance	No
44 USC §3506	Information resources management	DoD, military department CIOs	Ensure agency compliance with implementing agency information policy	No

> DoD Directive 5000.1 (reference (t)) for such programs, in coordination with the USD(AT&L) and the USD(I), as appropriate.

However, as noted in the directive itself, these authorities are only to be exercised if they are delegated by the USD(ATL), which is consistent with the acquisition authorities granted to the DAE in 10 USC §133.

DoDD 8000.01, *Management of the Department of Defense Information Enterprise,* assigns oversight responsibilities for DoD information management activities to the ASD(NII)/DoD CIO, consistent with DoDD 5144.1. It provides direction on "creating an information advantage for DoD personnel and mission partners," establishing and defining roles for CIOs at various levels within DoD, and establishing goals and

guidelines for information sharing and the DoD information enterprise architecture (DIEA).

DODD 8000.01 does not assign any explicit acquisition R&R to CIOs. However, it does direct unnamed executives in DoD to provide guidelines for the development of acquisition strategies for individual acquisition programs (per section 4.h.). The acquisition strategy document is one of 64 required documents that are reviewed by the DoD acquisition executive to make decisions when programs are under milestone review. In accordance with DoDI 5000.02, acquisition strategies are developed by individual programs for submission, review, and approval by the acquisition executive, not by the DoD CIO.

DoDD 8000.01 assigns the responsibility for leading the Defense Information Enterprise (DIE) to the ASD(NII)/DoD CIO. We discuss the implications of these broadly defined R&R below. DoDD 8000.01 also designates the CIO as the "senior official for information resources management matters."

The designation of the CIO as the senior official for information resources management is a new role. However, the directive assigns only two rather limited responsibilities to the CIO for this new role. According to Sections 1(3) and 1(4) of Enclosure 2 of DoDD 8000.01, these are to advise the SECDEF and Deputy Secretary of Defense (DEPSECDEF) on the information resource implications of strategic planning decisions and to develop a strategic plan for the same. We view these as advisory R&R that are not directly relevant to the DoD acquisition process and therefore are unlikely to conflict with the R&R assigned to DoD acquisition executives. We also note that these are not acquisition-related R&R. These R&R relate more directly to the DoD budget process and DoD information sharing policies, but not to acquisition processes for individual programs.

Section 1 of Enclosure 2 also assigns the DoD CIO the following R&R (p. 6):

> b. Provide standards for developing, maintaining, and implementing a DoD Enterprise Architecture. Establish mechanisms to ensure compliance with these standards.
>
> c. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.
>
> d. Ensure the integration and synchronization of the Department of Defense Information Enterprise activities.
>
> e. Establish mechanisms to facilitate organizationally-tiered compliance reviews for all IT investments to ensure they comply with all enterprise architectures, IT standards and related policy requirements; and act as the oversight authority for IT compliance.

It is important to note that the first R&R above applies only to the DIEA and not to IT or NSS that may be described in this architecture. To explain why this is the case, we momentarily digress to describe what an information or enterprise architecture is and how it is used in the specification of DoD systems that contain IT or NSS.

Interoperability criteria for IT and NSS are established using architectural views or products. The particular architectural views needed to assess the interoperability of an information system are specified in DoD policy (DoDI 4630 and CJCSI 6212.01E). These architectural views provide selected pieces of system design information. In previous versions of the DoD architecture framework, these architectural views were presented as images that could not be assessed or reused electronically. For this reason, older architectural views built according to older architectural standards have limited utility for the actual construction of information systems at the enterprise level or to compare the interoperability characteristics of two different information systems. Recently, well after the original DoD policies for information architectures were promulgated, a variety of new standards for architecture products were developed by commercial and DoD technical working groups. These new standards include metadata that enable these architecture products to be stored electronically and combined or federated using software programs. However, as with many new technology standards, a number of competing and potentially conflicting standards for information architecture products have been proposed.

Here, we note only that the specific new architecture-related R&R assigned to the CIO in DoDD 8000.01 are to determine specific and uniform architecture standards for the DIEA. Furthermore, DoDD 8000.01 does not explicitly grant the CIO the authority to develop the DIEA but only to specify the standards that guide its development. The standards for the DIEA have subsequently been promulgated by the CIO in the DoD architecture framework (DoDAF) version 2.0. DoDAF 2.0 is a significant technical achievement based on the DoD data strategy promulgated in DoDD 8320.02. While this may appear to be an arcane technical subject to some readers, the directive implicitly acknowledges that the CIO does not have the authority or capability to develop IT architectures alone. We discuss architecture R&R in detail in Chapter Four.

One other DoD directive in the 8000.01 series assigns R&R to the DoD CIO and to other DoD executives for IT. This is DoD Directive 8115.01, *Information Technology Portfolio Management*. This directive establishes policy and assigns responsibility for the management of DoD information technology investments as portfolios. We shall not review the content of this directive in detail here except to note that most of the R&R assigned in this directive pertain to investment decisions and budgeting for portfolios of IT programs. These activities fall under the planning, programming, budgeting, and execution (PPBE) process within DoD, and not within the DoD acquisition system. For this reason, this directive is of less interest in this investigation.

CHAPTER FOUR

Architecture R&R Defined in the United States Code

In this chapter, we examine DoD executive R&R for architectures assigned in the USC. We also compare architecture R&R with the R&R described in DoDI 5000.02 and DoDD 8000.01. Table 4.1 shows that architecture R&R are assigned to a wide array of DoD executives and in some cases to a committee of executives.

It is interesting to note that responsibility for financial management enterprise architecture is assigned in 10 USC §185 to the Financial Management Modernization Executive Committee, chaired by the Under Secretary of Defense (Comptroller) (USD(C)). However, this responsibility is assigned to the USD(C) in DoDI 5000.02. This may be a subtle difference, but it could be interpreted as a major difference in the authority the USD(C) has in this matter.

CIO Architecture R&R

Our examination of Titles 10, 40, and 44 of the USC shows that the statutes assign few architecture R&R to CIOs, as shown in Table 4.1. In fact, our examination revealed only one architecture R&R assigned to Agency CIOs: Title 40 assigns responsibility for IT architecture to executive agency CIOs. All other mentions of architecture R&R are associated with the Secretary of Defense, the Financial Management Modernization Executive Committee, the Chairman of the Joint Chiefs of Staff, the Defense Business Systems Management Committee, the Strategic Defense Initiative Federally Funded Research and Development Center, and the Administrator of the Office of Electronic Government within the OMB.

Architectures Relating to IT or NSS

Our evaluation of architecture responsibilities reveals that seven out of the 13 architectures discussed in the 52 occurrences of the term in Title 10 are not clearly related to IT, that five architectures are clearly IT-related, and one architecture is not related to IT. Furthermore, only three of the architectures are clearly related to NSS

Table 4.1
U.S. Code DoD Executive R&R for Architectures

U.S. Code	Type of Architecture	Responsible Party
Title 10 (52 occurrences)	Navy platform architecture for fleet	Secretary of Defense
	Financial management enterprise architecture	Financial Management Modernization Executive Committee
	Defense-wide architecture for C4I	Secretary of Defense
	Overarching common architecture for defense information systems	Chairman of the Joint Chiefs of Staff
	Architecture framework for department C4ISR	Financial Management Modernization Executive Committee
	Defense business enterprise architecture	Defense Business Systems Management Committee
	Ballistic missile defense architecture	Secretary of Defense
	(Space situational awareness) systems architecture	Secretary of Defense; Secretary of the Air Force
	National Security Space architecture	Secretary of Defense
	National Missile Defense System architecture	Secretary of Defense
	Theater missile defense architecture	Secretary of Defense
	Strategic Defense Initiative architecture	Strategic Defense Initiative Federally Funded Research and Development Center
	Naval architecture (ships)	President appoints Navy Officers
Title 40 (5 occurrences)	Information technology architecture	Agency CIO
Title 44 (5 occurrences)	Enterprise architecture	Administrator of the Office of Electronic Government within OMB
	Baseline architecture (part of enterprise architecture)	Administrator of the Office of Electronic Government within OMB
	Target architecture (part of enterprise architecture)	Administrator of the Office of Electronic Government within OMB

while two architectures are not related to NSS, and it is not clear whether the other eight architectures are NSS-related or not. As shown in Table 4.1, it is apparent that the USC assigns different parties in the DoD (the SECDEF, the Chairman of the Joint

Chiefs of Staff, and the DoD CIO) responsibilities for different architectures that all appear to be related to IT or NSS.

Title 40 mentions only one architecture, and that architecture is IT related. It is not explicitly stated in the statute whether this architecture is NSS related, but, as discussed in earlier sections, we conclude that this architecture probably does apply to NSS.

Title 44 mentions three architectures and all three are IT-related, but it is unclear whether any are NSS-related.

Table 4.2 summarizes the results of this analysis. Our analysis of architecture-related R&R assigned in the relevant federal statutes reveals that architecture R&R are distributed throughout DoD. Also, it is important to note that—even though the agency CIO, who is the DoD CIO in the case of DoD, is assigned the R&R to develop an IT architecture for the agency in the USC—the Secretary of Defense and the Joint Chiefs of Staff are assigned architecture R&R for C4I and defense information systems in different places in the USC.

IT- and NSS-Related Architecture R&R in DoD Policy

We now examine how IT- and NSS-related architectures are treated in DoD policy—specifically, DoDI 5000.02, DoDD 5144.1, DoDD 8000.01, and selected directive memoranda.

DoDI 5000.02 states:

> The capability needs and acquisition management systems shall use Joint Concepts, integrated architectures, and an analysis of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) in an integrated, collaborative process to define needed capabilities to guide the development of affordable systems. The Chairman of the Joint Chiefs of Staff, with the assistance of the Joint Requirements Oversight Council (JROC), shall assess and provide advice regarding military capability needs for defense acquisition programs. The process through which the Chairman provides advice is described in Chairman of the Joint Chiefs of Staff Instruction 3170.01 (Reference (h)). Representatives from multiple DoD communities shall assist in formulating broad, time-phased, operational goals, and describing requisite capabilities in the Initial Capabilities Document (ICD). They shall examine multiple concepts to optimize the way the Department of Defense provides these capabilities. (Enclosure 2, Section 3a, p. 14)

The wording of DoDI 5000.02 is consistent with the actual process for developing and validating the architectures used in program requirements documents. In this process, an individual program develops a draft set of architecture products.

Table 4.2
Relationship of USC Architectures to IT and NSS

U.S. Code	Type of Architecture	IT-Related	NSS-Related	Description of Architecture
Title 10	Navy platform architecture for fleet	Unclear	Unclear	SECDEF shall provide for . . . two independent studies of alternative future [Navy] fleet platform architectures.
	Defensewide architecture for C4I	Yes	Yes	SECDEF shall request . . . a comprehensive review of current and planned service and defense-wide programs for C4I . . .to include an assessment of the need for an overall defense-wide architecture for C4I.
	Overarching common architecture for defense information systems	Yes	Yes	JROC reports shall include assessment of progress made on development of overarching common architectures for defense information systems to ensure that common defense information systems are fully interoperable.
	Architecture framework for Department C4ISR	Yes	Unclear	Financial Management Modernization Executive Committee shall ensure a DoD financial management enterprise architecture is developed in accordance with . . . the architecture framework of the Department for command, control, communications, computers, intelligence, surveillance, and reconnaissance.
	Defense Business Enterprise Architecture	Yes	Unclear	The committee shall develop an enterprise architecture to cover all defense business systems . . . and a transition plan for implementing the enterprise architecture for defense business systems.
	Ballistic missile defense architecture	Unclear	Yes	National missile defense system architecture . . . shall consist of: (1) An interceptor system . . . (2) Ground-based radars; (3) Space-based sensors; and (4) Battle management, command, control, and communications.
	(Space situational awareness) systems architecture	Unclear	Unclear	The Space Situational Awareness Strategy shall include . . . a description of the systems architecture to implement the strategy that addresses current threats, desired effects, and required capabilities.

Table 4.2—Continued

U.S. Code	Type of Architecture	IT-Related	NSS-Related	Description of Architecture
Title 10	National Security Space	Unclear	Unclear	Proposals submitted to DoD regarding operationally responsive space technology need to . . . correlate with National Security Space Architecture.
	National Missile Defense System	Unclear	Unclear	Secretary of Defense shall ensure National Missile Defense Program is structured and programmed to support a test . . . representative of the national missile defense system architecture. . . .
	Theater Missile Defense	Unclear	Unclear	Articulates the core systems for the Theater Missile Defense architecture
	Strategic Defense Initiative (SDI)	Unclear	Unclear	Establish FFRDC as part of the SDI organization to provide critical evaluation . . . analysis of technologies, systems, and architectures.
	Naval (ships)	No	No	To promote a knowledge of naval engineering and naval architecture, the President . . . may detail a qualified Navy officer as a professor in a school or college.
Title 40	Information Technology	Yes	Unclear but likely Yes	Agency CIO R&R include developing, maintaining, and facilitating implementation of . . . integrated IT architecture for the executive agency. IT architecture defined as "an integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic goals and information resources management goals."
Title 44	Enterprise Architecture (EA)	Yes	Unclear	Administrator of OMB Office of Electronic Government shall . . . oversee implementation of e-Government: EA defined as: (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform mission; and (iv) transitional processes for implementing new technologies in response to changing mission needs; and includes (a) a baseline architecture; (b) target architecture; and (c) sequencing plan.
	Baseline (part of EA)	Yes	Unclear	No formal definition included in Title 44, but implies the current architecture.
	Target (part of EA)	Yes	Unclear	No formal definition included in Title 44, but implies the proposed architecture.

These products are included in the program ICD, which is reviewed by the sponsoring service, as well as by the joint community if the program is of joint interest. In this sense, integrated joint architectures are developed in a collaborative process that includes many parts of the DoD acquisition and requirements communities. No single organization is responsible for joint integrated architectures.

DoDD 5000.1 also states that integrated architectures are to be used to define system interoperability requirements:

> 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. (Enclosure, p. 5)

Title 40 assigns agency (DoD) CIO responsibility for information technology architecture. This intent of the law is reflected in one of the first issuances of DoD Global Information Grid (GIG) policy, signed in 2001, which is still in force. Under the direction of the Deputy Secretary of Defense, the DoD CIO develops, maintains, and enforces GIG architecture.[1]

This direction and unilateral assignment of architecture R&R to the DoD CIO does not appear to be consistent with DoDI 5000.02 and with the actual processes by which integrated architectures are developed and validated in the department.

DoDI 5000.02 sheds additional light on this issue by stating the following:

> The DoD Enterprise Architecture shall underpin all information architecture development. (Enclosure 2, Section 3d, p. 14)

This statement is consistent with the fact that the DoD CIO develops enterprise architecture standards and approaches that can be used to federate and combine architecture products developed by different organizations and also to test the compatibility of architecture products developed by different authors.[2]

DoDD 5144.1, Section 3.3.3, states that the DoD CIO is responsible for providing oversight and guidance for ensuring compliance to standards in order to achieve integrated and interoperable architectures across DoD. The DoD CIO is also assigned responsibility for ensuring that information assurance is integrated into DoD architectures as required by 40 USC and 44 USC. Section 3.3.3 of DoDD 5144.1 is consistent with DoDI 5000.02.

---

[1] Deputy Secretary of Defense, Memorandum 01-001, DoD, Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid Computing, April 6, 2001.

[2] Per DoDAF version 2.0 and DoDD 8000.01, as discussed in this chapter.

However, under Section 3.4 of DoDI 5144.1, which defines responsibilities separately from those outlined for the DoD CIO in Section 3.3.3, there is a more expansive list of responsibilities assigned regarding communications and information networks. They include to "develop and implement network-centric policies, architectures, practices, and processes . . . to enable Defense transformation," and providing "policies, oversight, guidance, architecture, and strategic approaches for all communications and information network programs and initiatives on an enterprise-wide basis across the Department, ensuring compliance with the Information assurance [IA] requirements as well as interoperability with national and alliance/coalition systems." One can interpret the responsibilities established in Section 3.4 to be consistent with the DoD CIO responsibilities defined in the 2001 DEPSECDEF memo.

In contrast, we interpret the DoD CIO responsibilities established in Section 3.3 to be consistent with those outlined in DoDI 5000.02. Although Section 3.4 of DoDI 5144.1 can be interpreted to be in conflict with other DoD policy, i.e., DoDI 5000.02, Section 3.4 appears to give the ASD(NII) the unilateral authority to develop "network centric architectures," while Section 3.3 does not assign the DoD CIO architecture R&R in such a unilateral fashion. In this regard, it is important to note that the DoD CIO is currently "dual hated" as the ASD(NII). So DoDD 5144.1 Sections 3.3. and 3.4 apply to the same DoD executive.

The newest high-level and relevant DoD policy regarding IT and NSS architecture R&R is DoDD 8000.01. DoDD 8000.01 further specifies that the ASD(NII)/DoD CIO is assigned the responsibility to provide standards for developing, maintaining, and implementing the DIEA and enforcing DIEA standards. In the broad context of DoD architecture policy, the DIEA can be equated with at least some of the architecture views contained in the broad set of joint integrated architecture products. As stated previously, it is important to note that DoDD 8000.01 does not assign the DoD CIO the responsibility for actually building the DIEA. Consistent with DoDI 5000.02, DoDD 8000.01 recognizes that this task is too large and complex for any one DoD organization. However, it does assign the DoD CIO the responsibility for guiding its development in a way that ensures that architecture products developed by different DoD organizations will be interoperable, shareable, and ultimately able to be federated into a single unified DIEA.

The ASD(NII)/DoD CIO is also named as the oversight authority for IT compliance, which at a minimum should include the assessment of compliance with DIEA development standards. Because DoDD 8000.01 is relatively recent (it was signed in February 2009), we consider it to be the authoritative statement on DIEA R&R. Consequently, we interpret it as superseding DoDD 5144.1 in this specific area. Under this interpretation of DoD policy, DoDD 8000.01 can be considered as removing any potential conflicts regarding IT architecture R&R found in the USC or among DoDD 5144.1, the 2001 DEPSECDEF directive memorandum, and DoDI 5000.02.

CHAPTER FIVE

Comparison of DAE and CIO Roles and Responsibilities

In this chapter, we compare the R&R assigned to the DoD acquisition executives and CIOs in U.S. law and in DoD policies and examine, on the basis of empirical evidence, whether conflicts may occur between DoD executives in these roles when they exercise their authorities. We focus on strong R&R because it is in executing these authorities that conflicts are most likely to occur. As before, we define *strong* R&R those that embody high-level, unique decisionmaking authorities—for example, setting or establishing policy or standards, directing a DoD management system such as the acquisition system, or overseeing the implementation of policy.

DAE Roles and Responsibilities

In Chapter Two, we examined acquisition-related R&R that are assigned to a range of DoD executives, including the USD(AT&L), SECDEF, and other officials responsible for research and development and operational test. We have already seen in Chapter Three that DoD CIOs are not given responsibilities for research and development or for operational test, so we do not consider these types of R&R further in this analysis.

As noted in Chapter Two, Title 10 assigns the USD(AT&L) a number of strong R&R, including oversight over nearly all aspects of the acquisition system. The USD(AT&L)'s strong R&R applicable to IT and NSS are listed in Table 5.1. The last column in the table indicates whether the USD(AT&L) may encounter a conflict with a DoD CIO in executing assigned R&R. We label this a *possible process conflict* because DoD executives typically carry out their duties when they participate in one or more of the major processes in the DoD. These major processes are acquisition, requirements, and budget processes. The last column in Table 5.1 summarizes our assessment—that conflicts between acquisition executives and CIOs are unlikely to arise in the acquisition process. The low likelihood of conflict for the R&R listed in Table 5.1 results from the careful coordination of DoD policies pertaining to the acquisition of IT and NSS, as described below. In these policies, the ultimate authority of the USD(AT&L) over acquisition matters is preserved, although it may be delegated to a CIO if the USD(AT&L) so directs.

Table 5.1
Strong DoD Acquisition Executive R&R in the U.S. Code

Source	Party	Role and Responsibility	Possible 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 the 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

The only case in which a possible acquisition process conflict could occur is for the last R&R indicated in the table. Title 40 assigns some acquisition authority to the head of U.S. government executive agencies, including the DoD. In particular, 40 USC §11314 states:

> (a) In General—The authority of the head of an executive agency to acquire information technology includes—
>
> (1) acquiring information technology as authorized by law;
>
> (2) making a contract that provides for multiagency acquisitions of information technology in accordance with guidance issued by the Director of the Office of Management and Budget; and
>
> (3) if the Director finds that it would be advantageous for the Federal Government to do so, making a multiagency contract for procurement of commercial items of information technology that requires each executive agency covered by the contract, when procuring those items, to procure the items under that contract or to justify an alternative procurement of the items.

Therefore, 40 USC §11314 assigns acquisition authority for IT acquisition within the DoD to the SECDEF. However, we draw the reader's attention to subsection (a)(1), which states that this acquisition authority is granted as authorized by law or within the limits of current law. In the case of DoD, 10 USC § 133 establishes the USD(AT&L) position and assigns the USD(AT&L) acquisition authority over all systems subject to the control, direction, and authority of the SECDEF. Hence, 40 USC §11314 assigns acquisition authority to the SECDEF, but 10 USC §133 provides for the SECDEF to delegate as much of that authority as he deems proper to the USD(AT&L).

An alternate view of 40 USC §11314 would be that the SECDEF could retain acquisition authority over IT and then presumably could assign that authority or delegate it to another DoD executive, such as the CIO (the CIO would be the natural designee of such an authority given other aspects of U.S. law, as we have already seen in Chapter Three). If this were the case, the SECDEF would delegate this acquisition authority in a relevant DoD policy or directive, which in this case would be DoDD 5144.1. In this respect, it is important to note that DoDD 5144.1 does not delegate IT acquisition authority to the DoD CIO to the exclusion of the USD(AT&L). This directive explicitly states, in Section 3.9, that acquisition authority over IT programs is granted to the CIO when it is delegated by the USD(AT&L) and the USD for Intelligence (USD(I)):

> 3.9. With regard to systems acquisition [the DoD CIO]:
>
> > 3.9.1 Serve as the Milestone Decision Authority for Major Automated Information Systems and other acquisition programs, as delegated by the USD(AT&L), with responsibility for developing and enforcing the policies and practices of DoD Directive 5000.1 (reference (t)) for such programs, in coordination with the USD(AT&L) and the USD(I), as appropriate.

Therefore, we can state that there is no conflict in U.S. law between 10 USC §133 and 40 USC § 11314 with regard to the assignment of acquisition authority for IT in the DoD.

It is also interesting to note that Title 10 does not explicitly assign the DAE or the USD(AT&L) any advisory R&R (i.e., R&R in which an executive is given circumscribed authorities, such as advising other officials or making recommendations to other executives who hold actual decisionmaking power).

CIO Roles and Responsibilities

The analysis of CIO R&R is more complex because the R&R given to CIOs in the USC are more specific and contain more elements than most R&R assigned to acquisition executives.

The strong R&R for DoD CIOs applicable to IT and NSS are listed in Table 5.2. The fourth column of Table 5.2 indicates that two current CIO R&R could potentially lead to conflicts with acquisition DoD executives when these executives execute their authorities in the acquisition process. The R&R with potential acquisition process conflicts are the DoD CIO R&R specified in "Information Technology: Additional Responsibilities of Chief Information Officers for DoD CIO" in 10 USC §2223; and the Agency CIO R&R specified in "Agency Chief Information Officer" in 40 USC §11315.

We examined how DoD policy interprets and implements the direction provided in the statutes to see whether the policy eliminates potential conflicts that might occur in the DoD acquisition process. The results of this analysis are shown in the fifth column of Table 5.2. We determined that DoD policy does in one case—R&R related to the development of IT architectures—resolve potential conflicts between DoD executives and their organizations in the acquisition process. These potential process conflicts are resolved by DoDD 8000.01, as described in the last section of this chapter. However, we have highlighted this determination for the last CIO R&R in Table 5.2 in yellow because not all DoD policy appears to be consistent with DoDD 8000.01. As described in Chapter Four, some older DoD policies are not consistent with DoDD 8000.01 and DoDI 5000.2.

Table 5.2
Strong CIO R&R Applicable to IT and NS

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

In contrast, we find that the potential process conflict identified in the first row of Table 5.2 is not resolved by current DoD policy. We examine this actual process conflict in detail later in this chapter. The remainder of this chapter examines each of the DoD CIO R&R listed in Table 5.2.

DoD CIO R&R in 10 USC §2223

The following additional responsibilities of DoD CIOs are identified in 10 USC §2223:

> Review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems, ensure the interoperability of information technology and national security systems throughout the Department of Defense, ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed, provide for the elimination and duplicate information technology and national security systems within and between the military departments and Defense Agencies and maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

Advisory R&R. Some DoD CIO R&R in 10 USC §2223 are advisory only. This section states that the DoD CIO is to review and provide recommendations to the Secretary of Defense on DoD budget requests for IT and NSS. This role is advisory because the DoD CIO may only make recommendations and not decisions that are reserved for the Secretary of Defense.

Strong but Broadly Defined R&R. In other areas, the DoD CIO is given strong but generally defined authorities. 10 USC §2223 states that the DoD CIO is to ensure the interoperability of IT and NSS systems throughout the DoD, but this section does not explicitly grant the DoD CIO acquisition authority or specify any particular procedures or processes to accomplish this task. In other words, the law assigns a goal to the DoD CIO to accomplish but does not specify any mechanism or specific authority for changing DoD acquisition programs or processes.

Similarly, 10 USC §2223 charges the DoD CIO to provide for the elimination of duplicate IT and NSS within and between the military departments and defense agencies. Again, however, the statute does not explicitly grant the DoD CIO acquisition authority or specify any other procedures or processes to accomplish the stated elimination.

The "processes and procedures" in these two areas can be interpreted as derivative of the Secretary of Defense's overall authority and need not be specified in the statute. It is the responsibility of the Secretary of Defense to ensure these powers, procedures,

and processes are specified in DoD policy in ways that do not conflict with the R&R of other DoD executives as defined in the USC.

The USD(AT&L) is subject to the authority, control, and direction of the SECDEF. The DAE is also given authority over all DoD acquisition programs in 10 USC §133, including IT- and NSS-related programs. Consequently, the powers, procedures, and processes for ensuring interoperability and eliminating duplication in the IT and NSS executed by the DoD CIO—if not carefully prescribed by the Secretary of Defense and DoD policy—could be a source of policy overlap or conflict with the USD(AT&L) if they pertain to matters involving the acquisition of IT and NSS.

Although we find that the DoD CIO R&R defined in 10 USC §2223 can potentially conflict with the R&R of the USD(AT&L) defined in 10 USC §133, the law implies that this potential conflict can and should be resolved by the Secretary of Defense in the formulation of DoD policy. Below, we examine whether this is the case for all DoD CIO R&R specified in 10 USC §2223.

The R&R of the DoD CIO are further specified by the Secretary of Defense in DoDD 5144.1. This directive repeats the authorities specified in Title 10 concerning ensuring interoperability and the elimination of duplication; in other cases, it goes beyond the high-level statements found in the USC.[1] DoDD 5144.1 grants the DoD CIO several additional R&R, including the authority to develop "approaches, strategies, and policies, and guidance for IT and NSS."

DoDD 5144.1 also provides the DoD CIO with acquisition authorities in Sections 3.3.9, 3.7.1, 3.7.2, 3.9.1, and 3.9.2. These sections grant the DoD CIO acquisition R&R over major defense space programs and MAIS programs, in coordination with other offices of OSD, in particular USD(AT&L). In other words, the default procedure is for the DoD CIO to be the acquisition MDA for MAIS and major defense space programs.

However, it should be noted that DoDI 5000.02 provides the USD(AT&L) with mechanisms to withdraw the delegation of acquisition authorities from other DoD offices, including the DoD CIO, consistent with the preeminence of the USD(AT&L) in DoD acquisition matters, per 10 USC §133.

Empirical evidence suggests that over the last decade (2002–2010) the DAE has grown increasingly reluctant to use the default mechanism in DoDD 5144.1—that is, to delegate acquisition authority to the DoD CIO for MAIS programs.[2] Evidence of this reluctance is shown by the DAE's assumption of acquisition authority over some of the largest and most important MAIS programs from the DoD CIO in the last decade. Examples of such MAIS programs include the following:

- Network Enabled Command Capability (NECC)—cancelled in 2009
- Transformational Communications Satellite (TSAT)—cancelled in 2008

[1] See Sections 3.3.8 and 3.3.17 of DoDD 5144.1.

[2] Private communication with William Scott, USD(AT&L).

- Warfighter Information Network—Tactical (WIN-T)
- Joint Tactical Radio System (JTRS).

In Section 3.9.2, DoDD 5144.1 also provides the DoD CIO with additional advisory authorities regarding acquisition matters:

> Provide advice on issues related to all assigned responsibilities and functions to the Defense Acquisition Board and the Defense Space Acquisition Board.

This statement shows that the DoD CIO is given a role in defense acquisition matters of IT and NSS programs even if it is not designated the MDA. However, given the current process used for IT- and NSS-related acquisition programs described above, we regard this role as an advisory R&R and one that would likely not lead to conflicts in the acquisition process because final decisions over acquisition programs are reserved for the DAE according to DoD policy and the USC.

DoDD 5144.1 also states that the DoD CIO should review and provide recommendations to the Secretary of Defense and the heads of the DoD components on

> The performance of the Department's IT and NSS programs (to include monitoring and evaluating the performance of IT and NSS programs on the basis of all applicable performance measurements)
>
> The continuation, modification, or termination of an IT and/or NSS program or project pursuant to section 1425 of reference (c).

We also consider this an advisory R&R unlikely to lead to conflicts in the acquisition process.

Other Nonconflicting R&R. Finally, we note that 10 USC §2223 authorizes the DoD CIO to examine systems, create a consolidated inventory of mission-critical and essential information systems, and develop and maintain contingency plans for responding to disruption in the operation of these information systems. Thus, the DoD CIO appears to be legally charged with being knowledgeable about critical aspects of the entire collection of DoD information systems but has no explicit acquisition authority to effect the plans or otherwise improve the "big picture."

The above review of the USC and DoDD 5144.1 does not include a comprehensive review of all DoD policy that may resolve conflict between DoD CIO R&R and the R&R of other DoD offices. Whether DoDD 5144.1 and DoDI 5000.02 fully resolve the potential conflicts identified in 10 USC §133 and §2223 is beyond the scope of this investigation. (This question is being addressed in a follow-on study.) As a practical matter, however, we note that many solutions to interoperability problems require the attention of acquisition authorities. Typically, a decision must be made to modify one

system or another to ensure interoperability between systems. System modifications in many cases require changes in the acquisition baseline of the program.

DoD CIO R&R in 10 USC §2223: Set Information System Standards

10 USC §2223 includes one additional provision, which states that the DoD CIO shall "Ensure that information technology and national security systems standards that will apply throughout DoD are prescribed." Our interpretation of this statute is that the DoD CIO is given the authority to set standards for IT and NSS that will ensure the interoperability of these systems.

The analysis and empirical data that we present below indicate that this R&R can lead to actual conflicts between CIO and acquisition executives in the acquisition process. This argument is detailed in the following pages.

IT standards are essential requirements for programs related to IT and NSS. They specify the technical design of the system. If an outside authority dictates that certain IT standards are to be changed in such a program, this change could affect the cost schedule or performance of the program. Because it is the acquisition executive's responsibility to monitor and control the cost, schedule, and performance of acquisition programs and to adjust and balance these factors as necessary to ensure a successful acquisition, it is possible for the DoD CIO R&R to conflict with those of DoD acquisition executives in the acquisition process. Below, we examine whether current DoD policy can remove such potential conflicts.

We are not suggesting here that two different sections of the law (e.g., 10 USC §133 and §2223) are necessarily in conflict with one another or represent a "prima facie" conflict. However, we are pointing out that, because of the potentially widespread impact of IT standards, the DoD CIO R&R could potentially conflict with the R&R of the DAE in the acquisition process for certain IT- and NSS-related programs. It is the responsibility of the Secretary of Defense to minimize the potential of such conflicts by issuing appropriate DoD policy.

Consistent with the statute, Section 3.3.13 of DoDD 5144.1 states that the DoD CIO shall "ensure that IT, including NSS, standards that apply throughout the department are prescribed and enforced pursuant to" 10 USC §2223. However, neither 10 USC §2223 nor DoDD 5144.1 establishes specific processes or more-specific authorities for DoD standards setting processes.

At first glance, one might think that DoDD 8000.01 could play a role in this area. DoDD 8000.01 is consistent with 10 USC §2223, but it specifies a much more limited set of DoD CIO R&R in this area that pertain only to enterprise architecture products and not to end-user information systems (IT or NSS). It assigns the ASD(NII)/DoD CIO the responsibility to provide standards for developing, maintaining, and implementing the Defense Information Enterprise Architecture and establishing mechanisms to ensure compliance with those standards. In addition, the ASD(NII)/DoD CIO is charged with ensuring that information policy and functional requirements are

reflected in architectures and plans across the DoD enterprise and component levels as a means to ensure information sharing, visibility, assurance, and interoperability. In other words, program managers who develop IT and NSS must address interoperability and information sharing requirements in their architecture products, and these products must conform to DIEA standards. However, DoDD 8000.01 does not say that the DoD CIO should directly or unilaterally set standards for IT and NSS.

The discussion above indicates that DoDD 5144 and DoDD 8000 do not address conflicts that may arise between the DoD IT standard-setting and acquisition processes or between executives responsible for these processes. Below, we examine whether other more-specific DoD policy for IT standards addresses such possible conflicts. We also consider empirical evidence to determine whether current policy is effective in managing or preventing such conflicts.

Current DoD IT Standard-Setting Process—In Practice. What is the process by which IT and NSS standards are actually set in the DoD, and do conflicts occur between DoD executives in the execution of this process? First, it is important to note that other authorities in the DoD and the U.S. government besides the DoD CIO can and do set standards for information systems, including system developers in the military departments, the Joint Staff, and the USD(AT&L).[3]

The first example we investigated involves IT standards for communications. In 2008, the USD(AT&L) set standards for unmanned aerial system (UAS) communication links.[4] Conversations with DoD acquisition officials indicate that the reason USD(AT&L) took the initiative to establish these standards is that noninteroperable UASs were being fielded and used in current operations, and because other parts of the DoD, presumably including the DoD CIO, were not effective in setting or enforcing such standards. In effect, the IT standards that were established for UAS communications systems were deemed by UAS program managers to be inappropriate from an acquisition management standpoint, making DAE action on this issue essential.[5] We consider this an *actual* conflict with the DoD CIO IT standard-setting R&R because the standards chosen by the DAE for some UAS communications links do not conform to the standards selected by the DoD CIO for those systems—namely, the Common Data Link (CDL) set of standards.

We also found a second example of such a conflict. In the past, the DoD CIO has attempted to set standards for communications networks, sometimes without suc-

---

[3] See for example U.S. Department of the Navy, Program Executive Office for Command, Control, Communications, Computers, and Intelligence, "Net-Centric Enterprise Solutions for Interoperability (NESI) Net-Centric Implementation Framework," Version 1.3, 2006; See also Chairman of the Joint Chiefs of Staff Instruction, *Interoperability and Supportability of Information Technology and National Security Systems,* CJCSI 6212.01E, December 15, 2008.

[4] Unmanned Aerial System Task Force, Standards and Interoperability Integrated Product Team, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, October 15, 2008.

[5] Private communication with anonymous DoD acquisition officials.

cess. For example. the DoD CIO drafted three consecutive versions of the Net Centric Implementation Directives (NCIDs), which contained standards that all DoD communications systems were to adhere to. The NCIDs were submitted for approval through the DoD-wide SD-106 review process, which is also used to obtain DoD-wide and Secretary of Defense approval for DoD directives and instructions. In all three cases, the draft NCIDs were disapproved. The services objected to the NCIDs for a number of reasons. For example, they claimed that if certain proposed standards were implemented in tactical networks, warfighters would be unable to execute their mission without incurring serious operational risks.

This example illustrates how standards for IT and NSS may also be perceived as dictating or setting warfighter operational requirements. According to Title 10, the military services and the Joint Staff have the exclusive R&R to "Organize, Train, and Equip" U.S. military forces. The Joint Staff is designated to have the R&R for certifying that military IT and NSS programs meet interoperability standards, as expressed in CJCSI 6212.01E, including the net-ready key performance parameter (NR-KPP), and GIG key interface profiles (KIPs) referred to therein. The GIG KIPs are collections of interoperability standards that military acquisition programs must adhere to. Consequently, it is possible that DoD CIO R&R for prescribing standards may conflict with policy promulgated by the Joint Staff that is perceived to be consistent with other parts of Title 10. Potential policy conflicts between DoDD 5144.1, CJCSI 6212.01E, and other policies will be the subject of future RAND research.

The authors are also aware of a third more-general example of actual process conflicts between acquisition and CIO executive R&R. It is possible that the imposition of new interoperability standards on military programs in the middle of the acquisition process (for example, between Milestones B and C) could negatively affect the overall cost, schedule, and performance of the program. In other words, the program's acquisition baseline could be compromised by imposing new requirements (in this case, interoperability standards) on the program. For this reason, it is possible that the DoD CIO's standard-setting authorities could conflict with the USD(AT&L)'s R&R because of the possible effects that IT and NSS standards could have on acquisition programs.[6] This issue has been raised by acquisition officials in internal DoD meetings with officials from the office of the DoD CIO, and the authors have witnessed such discussions. In meetings over the past three years, this issue has been raised repeatedly and has yet to receive a satisfactory resolution between the two communities.

The SECDEF has responsibility for establishing policy guidance that avoids such potential conflicts. However, the empirical evidence cited above indicates that, in practice, conflicts can and do occur in the area of setting standards for IT and NSS and that current DoD policy is not sufficient for this purpose.

[6] This point has been made by anonymous DoD acquisition officials regarding proposed DoD CIO IT standards.

These potential conflicts between the R&R of the DoD CIO, USD(AT&L), and the Chairman of the Joint Chiefs of Staff were recognized and addressed in DoD policy in May 2004 by means of DoDD 5101.7, which defined the R&R for the DoD executive agent for IT standards. This directive designated the Defense Information Systems Agency (DISA) as the executive agent for IT standards. In Section 6.2.5, it also established a governance structure for identifying, prescribing, and implementing IT standards that apply throughout the DoD and set up an IT Standards Oversight Panel (ISOP), consisting of senior Department of Defense representatives, to provide direction, oversight, and priorities, and issue resolution for IT standards matters.

It should be noted that DoDD 5101.7 expired by its own terms in May 2007, three years after its promulgation. However, this directive was still considered to be in force by the Joint Staff, in CJCSI 8010.01B, as of September 26, 2008, perhaps because it is not readily apparent that it has been replaced by any new policy. In our review of DoD, we were unable to find a complete replacement for DoDD 5101.7 other than the matters covered in DoDD 5144.1 previously noted. A memorandum issued by the Deputy Secretary of Defense in May 2007 does cite DoDD 5101.7 and does establish 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.[7]

According to David Brown, the director of interface standards at DISA, the ISOP was still in existence as of October 2008 and was tri-chaired by the DoD CIO, USD(AT&L), and the Chairman of the Joint Chiefs of Staff.[8]

Section 6.2.6 of DoDD 5101.7 states that the DoD CIO will "serve, in coordination with the Under Secretary for Acquisition, Technology, and Logistics, and the Chairman of the Joint Chiefs of Staff, as the final resolution authority for DoD IT standards issues." This is consistent with the role the ISOP chairs would take in adjudicating IT standards for the GIG Technical Direction, as communicated at the Enterprise Documentation Framework working group meeting of October 21, 2008.[9]

This statement of policy recognized that conflicting views of IT standards may occur between DoD acquisition, operational requirements, and interoperability processes and that, to resolve these issues in a manner consistent with the various sections of Title 10, the directors of these processes should meet and resolve these issues together.

As noted previously, DoDD 8000.01 is silent on establishing a new mechanism for determining standards for IT and NSS in place of the ISOP. To assist the Chairman of the Joint Chiefs of Staff, DoDD 8000.01 directs the Chairman of the Joint

---

7 England, 2007.

8 David Brown, DISA GE33, Enterprise Documentation Framework Working Group (EDFWG), briefing, October 21, 2008.

9 Brown, 2008.

Chiefs of Staff to appoint a Joint Community CIO. Surprisingly, however, it does not assign the Joint Community CIO any responsibilities.

Military CIO R&R in 10 USC §2223

This section of the USC states that the Chief Information Officer of a military department shall review budget requests for all IT and NSS, ensure that information technology and national security systems are in compliance with standards of the government and DoD, ensure that IT and NSS are interoperable with other relevant IT and NSS of the government and DoD, and coordinate with the Joint Staff with respect to IT and NSS.[10]

This section of the USC does not state what constitutes "compliance" when clear compliance data may be missing. In particular, it is unclear whether each military department can independently determine what constitutes compliance. Many interoperability problems cross service and other organizational boundaries and may be difficult to achieve when clear compliance standards are not present, i.e., when clear technical standards have not been defined by the DoD CIO or adopted by the military services.

As stated previously, the Secretary of Defense is obligated to issue policy that is consistent with the USC and removes any potential ambiguities. 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 in the acquisition process.

Agency CIO R&R in 44 USC §3534

This section 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 capabilities of IT and NSS. The DoD policy governing these matters is contained in the 8500 series of directives and instructions. Pending the results of such assessments and tests, an IT or NSS developed by an acquisition program will be given an "authority to operate" designation by the appropriate approval authority. If the program fails these IA assessments, then the program would 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 of acquisition programs. Otherwise, there may be opportunities for

[10] 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.

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 Identified in 44 USC §3544

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.

Executive Agency CIO R&R in 40 USC §11315

This section of the USC specifies that the CIO of an executive agency is responsible for

> (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this subtitle, consistent with Chapter 35 of Title 44 and the priorities established by the head of the executive agency;
>
> (2) developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency; and
>
> (3) promoting the effective and efficient design and operation of all major information resources management processes.

Advisory R&R. 40 USC §11315 assigns agency CIOs the responsibility to provide advice and assistance to the agency head and management to ensure that information technology is acquired and information resources are managed in a manner consistent with relevant statutory provisions and that the management of information resources reflects agency priorities.

Strong Architecture R&R. Agency CIOs are also charged with developing, maintaining, and facilitating the implementation of sound, secure, and integrated agency information technology architecture.

As discussed in Chapter Four, it is well-known that the actual way that architectures are now developed and validated in the DoD acquisition and requirements processes is quite different from that specified in 40 USC §11315, where it is stated that IT architectures should be developed by the agency CIO or, in the case of DoD, the DoD CIO. In the actual DoD process, an individual acquisition program will develop a draft set of architecture products. For programs that include IT and NSS, the program's requirements documents must contain an NR-KPP whose contents are specified in DoDI 4630 and CJCSI 6212.01E. The NR-KPP must contain a number of architecture views that correspond to the content of an IT architecture.

The NR-KPP is included in all the program's requirements documents, which are reviewed by the sponsoring service, the joint community (if the program is of joint interest), and the acquisition officials assigned oversight responsibilities for the program at each acquisition milestone decision. In this sense, integrated joint architectures are developed in a collaborative process that includes many parts of the DoD acquisition and requirements communities. Today, no single organization is responsible for joint integrated architectures, including joint architectures for programs that contain IT and NSS. This practice is followed not because any single DoD official has chosen to disregard U.S. law. Rather, it is due to the fact that the development of joint architectures is very difficult in DoD and best accomplished in a bottom-up approach, as opposed to the top-down approach implied in 40 USC §11315.

It should be remembered that this statute was written to apply to all executive agencies in the federal government, of which DoD is but one agency. The majority of executive agencies in the federal government are much smaller than DoD; therefore, a top-down approach for the development of an IT architecture is feasible in these cases. However, for a very large enterprise like DoD the development of an integrated architecture by one relatively small component of the overall agency becomes much more challenging. It is the view of the authors that senior decisionmakers within DoD have, over time, come to realize that it is not feasible for the DoD CIO or for any single office in DoD to develop an integrated IT architecture that would accurately reflect the information exchange requirements of the entire department.

As discussed in Chapter Four, DoDI 5000.02, DoDD 8000.01, and Section 3.3 of DoDD 5144.1 all recognize the decentralized nature of the DoD architecture development process.

And, as also stated in Chapter Four, DoDD 8000.01 assigns the DoD CIO the responsibility only for establishing standards for the DIEA. The ASD(NII)/DoD CIO is also named as the oversight authority for IT compliance, which at a minimum should include the assessment of compliance with DIEA development standards. We regard DoDD 8000.01 as the authoritative statement on DIEA (IT architecture) R&R and assess that this directive removes any potential conflicts regarding IT architecture R&R found in the USC or between DoDD 5144.1, DoDI 5000.02, and the relevant 2001 DEPSECDEF directive memorandum.

CHAPTER SIX

Findings

Our examination of DAE and CIO R&R covered all such R&R established in Titles 10, 40, and 44, as well as relevant DoD policies. Our findings are summarized in the following subsections.

Acquisition-Related R&R

Seven strong DoD acquisition-related R&R are contained in the law, as indicated in Table 6.1. Of these, six R&R are assigned to the USD(AT&L).

Table 6.1
Strong DoD Acquisition Executive R&R in the U.S. Code

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

The last R&R listed in the table is assigned to the agency head (the SECDEF in the case of DoD). 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 (DoDD 5000.02 and DoDD 5144.1) clearly preserves the primacy of the DAE in acquisition matters.

The Weapon Systems Acquisition Reform Act

The Weapon Systems Acquisition Reform Act (WSARA) increases the transparency of weapon system acquisition and provides for more-accurate independent assessments of cost and technical risks in DoD programs. The act reorganizes offices that report to the USD(AT&L) and creates the Office of Cost Assessment and Program Evaluation (CAPE). It makes changes to acquisition policy and requires the SECDEF to develop and implement mechanisms to improve trade-off analyses among cost, schedule, and performance objectives of acquisition programs. None of the changes specified in the act circumvent or reduce the authority of the DAE.

The act requires the appointment of a senior official in OSD for performance assessments and root cause analysis (PARCA). This official is charged with conducting performance assessments of major acquisition programs to determine the underlying causes of cost, schedule, or performance problems; issuing policies, procedures, and guidance for conducting such assessments; and advising acquisition officials on the performance of major acquisition programs.

On January 4, 2010, the Deputy Secretary of Defense issued a memorandum on behalf of the SECDEF that established the Office of the Director for PARCA within the Office of the USD(AT&L), Office of the Assistant Secretary of Defense for Acquisition (ASD(A)), which thereby eliminates any potential conflict of PARCA R&R with the R&R of DoD acquisition executives.

DoD CIO R&R

Our analysis indicates that the USC specifies 15 current CIO R&R. Of these, we found five strong R&R that apply to IT and NSS. They are listed in Table 6.2.

We found that four of these strong CIO R&R do not pose a risk of conflict in the DoD acquisition process. However, two DoD CIO R&R, those in the first and last rows of Table 6.2, contain language that could lead to potential conflicts in the DoD acquisition process if these conflicts are not resolved by specific guidance in DoD policy.

Table 6.2
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

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 Chapter Five. This means that they could lead to executive actions that could potentially complicate or delay the acquisition of DoD command and control, weapons, 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. However, we highlighted the last CIO R&R entry in Table 6.2 in yellow because not all DoD policy appears to be consistent with DoDD 8000.01. As described in Chapter Four, some older DoD policies are not consistent with DoDD 8000.01 and DoDI 5000.02.

Below, we summarize the analysis of the first and last DoD CIO R&R listed in Table 6.2.

DoD CIO R&R: Prescription of Information System Standards

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

> Ensure that information technology and national security systems standards are prescribed that will apply throughout DoD.

We found that conflicts could and do occur between the DoD CIO, acquisition program milestone decision authorities and the Joint Staff regarding the selection of

technical standards for IT and NSS. Earlier in this monograph, we presented empirical evidence that such process conflicts do occur. It is possible that the DoD CIO's standard-setting authorities established in 10 USC 10 §2223 could conflict with the USD(AT&L)'s R&R established in 10 USC §133 in the DoD acquisition process when these executives or their representatives exercise their authorities.

These potential conflicts were 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 an IT Standards Oversight Panel, tri-chaired by the DoD CIO, USD(AT&L), and the Vice Chairman of the Joint Chiefs of Staff, to provide direction, oversight, and priorities and to resolve issues concerning IT standards. 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 DISA's role as the DoD executive agent for IT standards, but it does not extend the tenure of the ISOP or provide any other detailed guidance.[1]

DoD CIO R&R: IT Architecture Development

In this analysis, we have identified potential conflicts between architecture development R&R specified in the USC and between DoD executives with oversight of the actual processes used to develop integrated architectures for DoD systems and programs. These apparent conflicts are resolved by recent changes to DoD policy, as indicated below, but not by older DoD policy that appears 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 that process, integrated joint architectures are developed in a collaborative manner that includes many parts of the DoD acquisition and requirements communities. No single organization is responsible for, or has the capability to develop, joint integrated architectures, nor does any single organization have the capability to develop the entire DIEA.

Most important, DoDD 8000.01 gives the ASD(NII)/DoD CIO the responsibility for providing standards for developing, maintaining, and implementing the DIEA but not for developing IT architectures based on the DIEA.

---

[1] England, 2007.

CHAPTER SEVEN

Recommendations

In summary, we found that DAE and DoD CIO R&R that apply to IT and NSS, as specified in the USC and DoD policy, do not directly conflict with each other. However, we did find that conflicts can potentially occur in practice in the DoD acquisition process. We termed them *potential process conflicts*. We found they 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. The following recommendations provide ways to minimize or avoid the first type of conflict in the DoD acquisition process.

Retain IT Standards Oversight Panel 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 across 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 GIG technical guidance 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. This difficulty 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 has 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 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 also 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 immediately before major milestone reviews. Just as with program technology readiness assessments, the review of the technical maturity of proposed IT standards would be conducted by DDR&E prior to 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, available to more than one contractor, and 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, 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.

Recommended Next Steps

While we have made concrete recommendations based on our review of the USC and several primary DoD policy documents, we did not conduct a comprehensive review of GIG policies and architecture guidance documents because of time and resource limitations. 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. Such tools could also be used to assess the consistency of DoD policy in other areas.

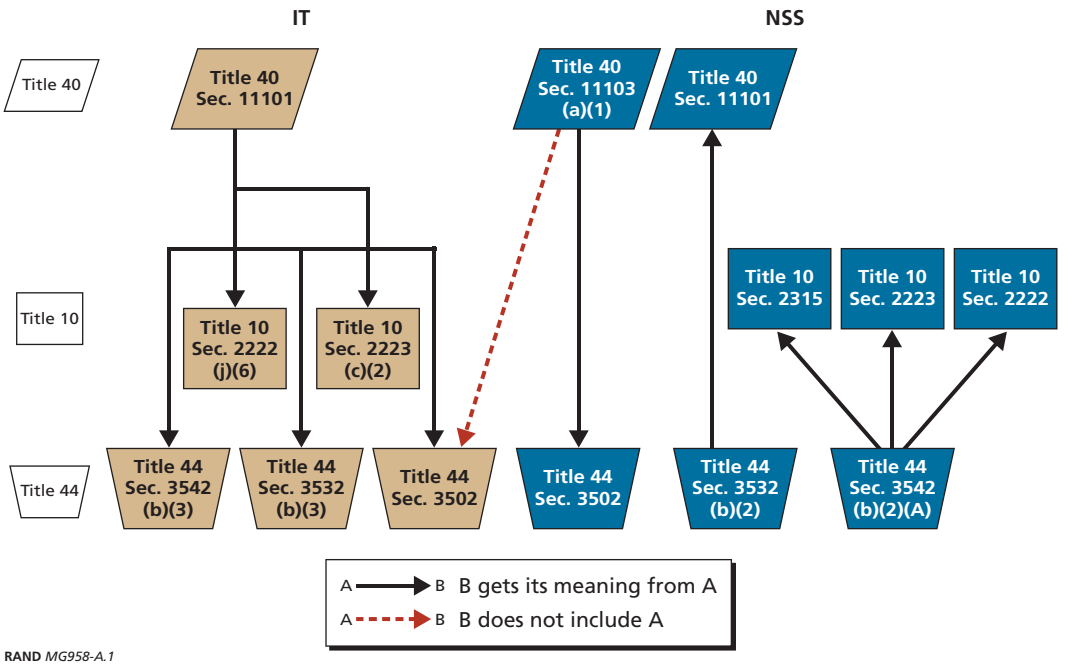
APPENDIX A

Definitions of IT and NSS in the USC

The USC contains multiple definitions of information technology and national security systems. Figure A.1 illustrates the relationships among the various definitions of these two terms. The USC specifies which definitions of IT and/or NSS apply to which sections of the USC. We note, however, as illustrated in Figure 1.1, there is not always a clear relationship between the terms IT and NSS in specific sections of the USC, even though many sections separately define IT and NSS.

Indeed, it is only in Title 44 where the relationship between IT and NSS is clear. In Title 10 the relationship between the two terms is not defined.

Figure A.1
Legal Definitions of IT and NSS



RAND *MG958-A.1*

In most cases, Title 10 uses the definition of information technology given in 40 USC §11101, which is the fundamental definition of IT assumed in this monograph. This definition is broad and comprehensive. It is plausible, therefore, that this definition of IT includes NSS as a subset of all IT. Indeed, much DoD policy issued by the DoD CIO appears to assume this relationship between IT and NSS, although this relationship is not established explicitly in Title 10.

Definitions of Information Technology

Federal law contains two basic definitions of information technology. One is found in 40 USC §11101; another is found in 44 USC §3502. The difference between these two definitions is that the definition in Title 40 implicitly includes national security systems and the definition in Title 44 specifically excludes national security systems.

40 USC §11101 defines information technology as follows:

> (6) Information technology. - The term "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.

Title 44 has more than one definition of information technology. 44 USC §3502 uses the Title 40 definition but explicitly excludes national security systems. 44 USC §3502 defines information technology as follows:

> (9) the term "information technology" has the meaning given that term in section 11101 of title 40 but does not include national security systems as defined in section 11103 of title 40;

44 USC §§3532 and 3542 use the term as defined in Title 40:

> (3) the term "information technology" has the meaning given that term in section 11101 of title 40

10 USC §2222 uses the definition of the term given in 40 USC §11101:

> (5) The terms "information system" and "information technology" have the meanings given those terms in section 11101 of title 40.

10 USC §2223 also uses the definition given in 40 USC §11101:

> (2) The term "information technology" has the meaning given that term by section 11101 of title 40.

Definitions of National Security System

The three definitions of the term *national security system* in the United States Code add to the complexity of R&R analysis. The NSS portion of Figure A.1 shows that there are three definitions of NSS. One definition of NSS is in 40 USC §11103; this definition is also used in 44 USC §3502. A second definition is in 44 USC §3532 and is also used in 40 USC §11331. The third definition is in 44 USC §3542. This definition is used in 10 USC §2222, §2223, and §2315. These three definitions are similar in broad terms but differ in potentially significant ways. As shown below, the definition of NSS in 40 USC §11103 specifies that NSS is a "telecommunications or information system operated by the Federal Government" and satisfies the five conditions listed. The definition of NSS in 44 USC §3532 includes systems that must satisfy the same five conditions, but NSS in this definition can be operated not only by the federal government but also by contractors on behalf of government agencies. The definition of NSS in 44 USC §3542 includes all information systems included in the definition of NSS in 44 USC §3532, as well as any information system that "is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy."

Slightly different meanings may in the majority of cases pose no consequence, but in some cases the consequence may be notable. For example, 10 USC §2223 charges the DoD CIO to ensure that IT and NSS are interoperable and that IT and NSS

standards are prescribed for all DoD. This DoD CIO R&R is applicable to NSS as defined in 40 USC §11103 and therefore applies only to telecommunications or information systems operated by the federal government. On the other hand, 44 USC §3544 charges the agency CIO with producing an annual report on the effectiveness of the agency information security program. The definition of NSS applicable to this Agency CIO R&R is in 44 USC §3542. Hence, the NSS that must be addressed in the annual report must include not only telecommunications and information systems operated by the federal government but also such systems operated by contractors on behalf of the federal government and any system that is continuously protected as classified by either an executive order or an act of Congress.

The detailed definitions of NSS are given below.

40 USC §11103 defines the term *national security system*:

> (1) National security system. - In this section, the term "national security system" means 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;
>
> (E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.
>
> (2) Limitation. - Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

40 USC §11331 uses the definition of national security system given in 44 USC §3532(b)(2):

> (2) Standards and guidelines for national security systems. -
>
> Standards and guidelines for national security systems, as defined under section 3532(3) of title 44, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

44 USC §3532(b)(2) defines national security system in a similar, but not identical manner as 40 USC §11103, as follows:

> (2) the term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, 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 provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

44 USC §3542(b)(2) offers a similar, but not identical, definition of the term:

(2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency

(i) the function, operation, or use of which -

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

10 USC §2222 uses the same definition as 44 USC §3542(b)(2):

(6) The term "national security system" has the meaning given that term in section 3542(b)(2) of title 44.

10 USC §2315 also uses the same definition as 44 USC §3542(b)(2):

> For purposes of subtitle III of title 40, the term "national security system," with respect to a telecommunications and information system operated by the Department of Defense, has the meaning given that term by section 3542(b)(2) of title 44.

10 USC §2223 uses the same definition:

> (3) The term "national security system" has the meaning given that term by section 3542(b)(2) of title 44.

APPENDIX B

Overview of DoD Directives and Instructions

DoD directives and instructions are the highest level of issuances. Directives and instructions are decisions by the signing authorities and are based on the U.S. Code or on other existing directives and instructions. There are two types of directives and two types of instructions. Direct oversight directives address R&R from the SECDEF and DEPSECDEF that are not delegable. Chartering directives establish OSD components, component leadership, and component functions. Policy instructions always refer to the relevant component charter and establish policy and R&R within the purview of the charter. Nonpolicy instructions implement DoD policy. Table B.1 summarizes the defining characteristics of directives and instructions. More-detailed descriptions of directives and instructions follow the table.

DoD Directives. Directives are signed by the SECDEF, DEPSECDEF, or by Undersecretaries of Defense when so chartered. Directives come in two types: direct oversight or chartering. Direct oversight directives address subjects that are nondelegable SECDEF or DEPSECDEF responsibilities and are used to assign functions among principal staff agencies, to designate responsibilities to executive agents, or for matters of special interest. Chartering directives assign missions, responsibilities, functions, relationships, and delegated authorities to subordinate organizations.

DoD Instructions. Instructions provide amplifying detail to directives. Policy instructions provide overarching policy or general procedures to implement policy as derived from broader chartering references (such as DoD chartering directives.) Nonpolicy instructions summarize policy and provide procedures for implementation.

Table B.1
Purposes and Authorities of DoD Directives and Instructions

Issuance	Type	Purpose	Authority
DoD directives	Direct oversight	Non-delegable SECDEF/DEPSECDEF responsibilities Assignment of functions/resources between/among PSAs and/or DoD components Designation of executive agents and assignment of related responsibilities and authorities or matters of SECDEF/DEPSECDEF special interest	Signed by the SECDEF or DEPSECDEF
	Chartering	Establish OSD component head, PSA official, defense agency, DoD field activity, or other major DoD or OSD component's official mission, responsibilities, functions, relationships and delegated authorities	Signed by the SECDEF or DEPSECDEF Signed by USDs delegated the authority in their charter for subordinate OSD PSA officials
DoD instructions	Policy	Establish policy and assign responsibilities within a functional area assigned in an OSD component head's charter May provide general procedures for implementing the policy Signed only by OSD component heads or their principal deputies Include OSD component's charter as a references	Signed only by OSD component heads or their principal deputies
	Nonpolicy	Implement policy established in a DoD directive or policy instruction Summarize policy Provide procedures for carrying out the policy Signed by OSD component heads, principal deputies, or other OSD PSA officials as authorized by their charters	Signed by OSD component heads, principal deputies, or other OSD PSA officials as authorized by their charters

NOTE: PSA = principal staff assistant.

APPENDIX C

CIO R&R in USC but Not Considered Relevant

Two current CIO R&R pertain to Year-2000 (Y2K) issues. Although it is likely that the software conversion tasks associated with these R&R have been completed, the R&Rs still remain part of active U.S. law. We did not consider these two R&R relevant, but we list them here for completeness.

In 10 USC §2302, the term IT is used, but no definition for IT is specified. This R&R charges the DoD CIO and military department CIOs with tasks related to Y2K software conversion.

44 USC §3506 does not include the term *information technology*, but does include the term *information resources*, which, in this case appears to include IT but explicitly excludes NSS. The CIO R&R in 44 USC §3603 charges the CIO Council with Y2K software conversion activities.

Table C.1 summarizes these two CIO R&R.

Table C.1
Summary of CIO R&R Not Considered Relevant

USC Source	Role and Responsibility	Party	Nature of R&R	Definition of IT	Definition of NSS
10 USC §2302	Year 2000 software conversion	DoD, military departtment CIOs	Y2K assessment	IT used but not defined	NSS not in text
44 USC §3506	Year 2000 conversion	CIO Council	Y2K support	IT not in text but definition of information resources in 44 USC §3502 includes IT	NSS not in text and definition of IT in 44 USC §3502 excludes NSS

APPENDIX D

Weapon Systems Acquisition Reform Act of 2009

The Weapon Systems Acquisition Reform Act of 2009 mandates changes to some existing offices and executive titles in DoD and the creation of some new positions. These changes are directed toward providing more accurate independent assessments of costs and technical risks in DoD programs.

Director of Cost Assessment and Program Evaluation

The act creates a new position, the Director of Cost Assessment and Program Evaluation (CAPE), which requires confirmation by the Senate. The CAPE director oversees an office that combines the prior Office of Program Analysis and Evaluation (PA&E) and the Cost Analysis Improvement Group (CAIG). The R&R of the director of CAPE is to act as the principal advisor to the Secretary of Defense and other senior officials of DoD for

- cost estimation of acquisition programs
- analysis and advice on matters relating to the planning and programming phases of the Planning, Programming, Budgeting and Execution System (PPBES)
- analysis and advice for resource discussions relating to requirements under consideration of the JROC
- formulation of study guidance for analyses of alternatives
- review, analysis, and evaluation of programs for executing approved strategies and policies
- assessment of special access and compartmented intelligence programs in coordination with USD(AT&L) and the Under Secretary of Defense for Intelligence
- assessment of alternative plans, programs, and policies with respect to acquisition programs
- leading development of improved analytic skills and competencies within the cost assessment and program evaluation workforce of DoD.

The CAPE director is authorized to "communicate views on matters within the responsibility of the Director directly to the Secretary of Defense and the Deputy Secretary of Defense without obtaining the approval or concurrence of any other official within the Department of Defense." In addition, an annual report summarizing cost estimation and cost analysis activities is to be submitted concurrently to the SECDEF, (USD(C)), USD(AT&L), and Congress.

Directors of DT&E and Systems Engineering

The act establishes new positions of directors of Developmental Test and Evaluation (DT&E) and of Systems Engineering (SE). The director of DT&E is the principal advisor to the SECDEF and USD(AT&L) on developmental test and evaluation. The director of SE is the principal advisor to the SECDEF and USD(AT&L) for systems engineering and development planning processes. Both directors are subject to the supervision of the USD(AT&L). Additionally, both directors are required to jointly submit to Congress a report to include a section on Major Defense Acquisition Programs (MDAPs) discussing

- the extent to which the MDAPs are fulfilling the objectives of their systems engineering master plans and DT&E plans
- waivers of and deviations from requirements in test and evaluation master plans, systems engineering master plans, and other testing requirements
- the organization and capabilities of DoD for systems engineering and developmental test and evaluation with respect to the programs.

Performance Assessments and Root Cause Analysis Official

The act requires the appointment of a senior official in OSD responsible for performance assessments and root cause analysis (PARCA). This official will not have program execution responsibilities but is responsible for

- performance assessments of MDAPs periodically or upon request
- assessment of the underlying cause or causes of shortcomings in cost, schedule, or performance of an MDAP
- issuing policies, procedures, and guidance governing the conduct of PARCA
- evaluating the utility of performance metrics used to measure cost, schedule, and performance of MDAPs
- advising acquisition officials on performance issues regarding MDAPs.

The official responsible for PARCA will submit an annual report to Congress on activities of the office.

Director DDR&E Assessment of Technological Maturity

The act requires the director, Defense Research and Engineering (DDR&E) to periodically review and assess the technology maturity and integration risk of critical technologies of MDAPs. The act requires an annual report to the SECDEF and Congress.

COCOM Commander R&R

The act requires the JROC to seek and consider input from the combatant command (COCOM) commanders for input regarding

- current or projected missions or threats that would inform assessment of a new joint military requirement
- necessity and sufficiency of a proposed joint military requirement in terms of current and projected missions or threats
- relative priority of a proposed joint military requirement in comparison with other military requirements
- ability of partner nations to assist in meeting joint military requirements.

New Service Acquisition Executive R&R

The WSARA of 2009 assigns additional responsibilities to the SAE:

- With regard to DT&E, the SAE is responsible for ensuring that sufficient resources are available for the testing process, that planning is proper and sufficient, and for overseeing the conduct of the test.
- With respect to systems engineering, the SAE is responsible for ensuring that there are adequate numbers of SE personnel and training for SE personnel to support milestone decisions; that reliability, availability, maintainability, and sustainability are considered; and that SE considerations are incorporated into contracts.
- The service acquisition executive is required to report to the directors of DT&E and SE on the extent to which the requirements of the WSARA are being implemented and what additional resources are required.

Acquisition Policy Changes

The act also specifies policies for the operation of the acquisition system.

Trade-Offs in Cost, Schedule, and Performance

The act requires the SECDEF to develop and implement mechanisms to require consideration of trade-offs among cost, schedule, and performance objectives by

- providing appropriate opportunities to develop estimates and raise cost and schedule matters before performance objectives are established
- structuring the process for requirements development to enable incremental, evolutionary, or spiral acquisition approaches.

The act entails no major changes to the current process. It explicitly specifies procedures that are part of the current version of DoDI 5000.02.

Ensuring Competition

The act requires the SECDEF to ensure that the acquisition strategy for each MDAP includes

- measures to ensure competition at both the prime contract and subcontract level
- adequate documentation of the rationale for the selection of the subcontract tier or tiers.

Prototyping Requirements for MDAPs

The act requires competitive prototyping of systems or critical subsystems before Milestone B approval unless waived by the MDA. The MDA can waive the requirement only if the cost of producing the prototypes exceeds the expected life cycle benefits of producing the prototypes or if the department would otherwise be unable to meet critical national security objectives. If a waiver is approved, the program is still required to develop a prototype before Milestone B approval.

Actions to Identify and Address Systemic Problems Prior to Milestone B

The act requires PM notification of failure to achieve Milestone A (MS A) certification if the program exceeds the cost estimate submitted at the time of certification by at least 25 percent or the PM determines that the period of time required for delivery of an initial operational capability is likely to exceed the schedule objective by more than 25 percent. In such cases, the MDA is required to determine the root cause of cost or schedule growth and to identify appropriate performance measures for the remainder

of the development program. The MDA is authorized to terminate or withdraw MS A approval if deemed in the interest of national defense.

Additional Requirements for Certain MDAPs

The act specifies additional requirements for certification of programs that have received MS B approval, but have not yet been approved for MS C. The act also requires semi-annual reviews of programs that experience critical cost growth under Nunn-McCurdy provisions.

Critical Cost Growth in MDAPs

The act requires determination of root cause for critical cost growth threshold breaches. After reassessment, the SECDEF shall terminate programs unless the SECDEF submits to Congress certification that

- continuation is critical to the national security
- there are no alternatives to the program that will provide acceptable capability
- new estimates of costs have been determined to be reasonable
- the program has higher priority than other programs whose funding have been reduced to accommodate cost growth in the program
- management structure is adequate to manage and control costs.

Both certification and termination actions require reports to Congress.

Organization Conflicts of Interest

The act requires revisions to acquisition regulations to provide uniform guidance and to tighten existing requirements for organizational conflicts of interest by contractors.

Additional Acquisition Provisions

The act has additional provisions for awards to DoD personnel for excellence in the acquisition of products and services, implementation of the Earned Value Management within DoD, expansion of national security objectives of the national technology and industrial base, and Comptroller General reports on costs and financial information regarding MDAPs.

New Required Reporting

The WSARA of 2009 adds additional DoD reporting requirements to Congress. These are summarized in Table D.1.

Table D.1
Additional Reports Required by WSARA of 2009

Report	From	To	Due Date
Assessment of previous year's cost estimation and analysis activities	CAPE	Concurrently to SECDEF USD(AT&L) USD(C) Congress	Annually within 10 days of President's budget submission
O&S costs for MDAPs	CAPE	SECDEF SECDEF to Congress	May 2010
Joint report on DT&E and SE activities	DT&E and SE	Congress	Annually; no later than March 31
Implementation of resource planning for DT&E and SE activities	CAEs with MDAPs	Congress	November 2009
PARCA activities	OSD (to be decided)	Congress	Annually no later than March 1
Technology maturity and integration risk of MDAPs	DDR&E	Congress	Annually no later than March 10
Resources needed to implement technology maturity and integration risk assessments	DDR&E	Congress	November 2009
Role of COCOMs in Joint Requirements process	GAO	Congress	May 2011
Notification of waiver for competitive prototyping due to excessive costs	MDA	Congress and GAO	30 days after waiver
Funding changes due to critical cost growth in MDAPs	OSD	Congress	First Selected Acquisition Report (SAR) in calendar year after program restructure
Growth in O&S costs of major systems	GAO	Congress	May 2010
Review of weaknesses in operations relating to financial information for MDAPs	GAO	Congress	May 2010

Bibliography

Brown, Bradford, "Weapon Systems Acquisition Reform Act of 2009," briefing, Defense Acquisition University, May 22, 2009.

Brown, David, DISA GE33, Enterprise Documentation Framework Working Group (EDFWG), briefing, October 21, 2008.

Chairman of the Joint Chiefs of Staff Instruction, *Joint Military Intelligence Requirements Certifications,* CJCSI 3312.01A, February 23, 2007. As of June 21, 2007: http://www.dtic.mil/cjcs_directives/cdata/unlimit/3312_01.pdf

———, *Interoperability and Supportability of Information Technology and National Security Systems,* CJCSI 6212.01E, December 15, 2008. As of March 15, 2010: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf

Clinger Cohen Act—Information Technology Management Reform Act and Federal Acquisition Reform Act, Public Law 104-106, 1996.

Department of Defense Architecture Framework (DoDAF) Version 2, Department of Defense Deputy Chief Information Officer. As of May 5, 2010: http://cio-nii.defense.gov/sites/dodaf20/

Department of Defense Directive 5000.1, *The Defense Acquisition System,* Under Secretary of Defense for Acquisition, Technology and Logistics, May 12, 2003.

Department of Defense Directive 5101.7, *DoD Executive Agent for Information Technology Standards,* Director of Administration and Management, May 21, 2004.

Department of Defense Directive 5144.1, *Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO),* Director of Administration and Management, May 2, 2005.

Department of Defense Directive 8000.01, *Management of the Department of Defense Information Enterprise,* Deputy Secretary of Defense, February 10, 2009.

Department of Defense Directive 8115.01, *Information Technology Portfolio Management*, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, October 10, 2005.

Department of Defense Directive 8320.02, *Data Sharing in a Net-Centric Department of Defense,* Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, April 23, 2007.

"Department of Defense Executive Agent (EA) for Information, Technology (IT) Standards," May 21, 2007 (extends DoDD 5101.7).

Department of Defense Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004.

Department of Defense Instruction 5000.2, *Operation of the Defense Acquisition System,* Under Secretary of Defense for Acquisition, Technology and Logistics, May 12, 2003.

Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System,* Under Secretary of Defense for Acquisition, Technology and Logistics, December 2, 2008.

Department of the Navy, Program Executive Office for Command, Control, Communications, Computers, and Intelligence, "U.S. Air Force Electronic Systems Center, and Defense Information Systems Agency, Net-Centric Enterprise Solutions for Interoperability (NESI) Net-Centric Implementation Framework," Version 1.3, 2006.

Deputy Secretary of Defense, Memorandum 01-001, DoD, Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid Computing, April 6, 2001.

Deputy Secretary of Defense Memorandum, "Designation of the Senior DoD Official for Performance Assessments and Root Cause Analyses (PARCA) Within the Office of the Secretary of Defense," January 4, 2010.

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

Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433, October 1, 1986.

Unmanned Aerial System Task Force, Standards and Interoperability Integrated Product Team, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, October 15, 2008.

U.S. Code, Title 10, Armed Forces, 2008 version, October 5, 2009. As of December 21, 2009: http://uscode.house.gov/pdf/2008/2008usc10.pdf

U.S. Code, Title 40, Public Buildings, Property, and Works, 2007 version, June 18, 2009. As of December 21, 2009:
http://uscode.house.gov/pdf/2007/2007usc40.pdf

U.S. Code, Title 44, Public Printing and Documents, 2007 version, July 20, 2009. As of December 21, 2009:
http://uscode.house.gov/pdf/2007/2007usc44.pdf

U.S. Department of the Navy, Program Executive Office for Command, Control, Communications, Computers, and Intelligence, "Net-Centric Enterprise Solutions for Interoperability (NESI) Net-Centric Implementation Framework," Version 1.3, 2006

Weapon Systems Acquisition Reform Act of 2009, Public Law 111-23, May 22, 2009.