This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Using EPIC to Find Conflicts, Inconsistencies, and Gaps in Department of Defense Policies

Carolyn Wong • Daniel Gonzales • Chad J. R. Ohlandt
Eric Landree • John Hollywood

NATIONAL DEFENSE RESEARCH INSTITUTE

TECHNICAL REPORT

Using EPIC to Find Conflicts, Inconsistencies, and Gaps in Department of Defense Policies

Carolyn Wong • Daniel Gonzales • Chad J. R. Ohlandt
Eric Landree • John Hollywood

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 Cataloging-in-Publication Data

Wong, Carolyn, 1952-
Using EPIC to find conflicts, inconsistencies, and gaps in Department of Defense policies / Carolyn Wong, Daniel Gonzales, Chad J. R. Ohlandt, Eric Landree, John Hollywood.
pages cm
Includes bibliographical references.
ISBN 978-0-8330-7676-2 (pbk. : alk. paper)
1. United States. Dept. of Defense—Personnel management—Data processing. 2. United States. Dept. of Defense—Officials and employees—Selection and appointment. 3. Manpower—United States. I. Title.

UB193.W66 2013
355'.033573028553—dc23

2013014095

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

RAND® is a registered trademark.

Published 2013 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 report presents a technique for analyzing the consistency and completeness of the roles and responsibilities (R&R) assigned to government executives in U.S. government policy. The technique is composed of a framework and a methodology.

The framework relates executive positions to roles and responsibilities and the products that result from their execution. The methodology uses the framework to identify potential conflicts, ambiguities, gaps, inconsistencies, and redundancies in defense policy. We developed a new tool that automates one step of the methodology. We describe the framework, methodology, and new software-based tool and demonstrate with case studies how the technique can be used to analyze large numbers of policy guidance directives for completeness and consistency in the R&R assigned to Department of Defense (DoD) executives.

This technique was developed coincident with research sponsored by the Assistant Secretary of the Navy, Research, Development, and Acquisition Chief Systems Engineer (ASN RDA CHSENG). This study builds on previous RAND research for ASN RDA CHSENG that examined the R&R of defense acquisition executives and chief information officers. This work was documented in *Are Law and Policy Clear and Consistent? Roles and Responsibilities of the Defense Acquisition Executive and the Chief Information Officer* (Daniel R. Gonzales, Carolyn Wong, Eric Landree, and Leland Joe, MG-958-NAVY, 2010).

This research should be of interest to DoD officials responsible for formulating, reviewing, or implementing DoD policy. It should also be of interest to those who play a role in the development of legislation dealing with DoD weapon system, aircraft, ship, information technology, and national security system acquisition programs. This report reflects a possible advantage that a policy analysis tool might provide to help identify policy flaws while in draft and early stages of review. Acquisition managers and policy managers would benefit if improvements can be made, conflicts adjudicated, and gaps filled before the release of new or amended guidance.

This research was 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 Intelligence Community.

For more information on RAND's ATPC, see http://www.rand.org/nsrd/about/atp.html or contact the director (contact information is provided on the web page). Comments or questions on this report should be addressed to the project leaders, Carolyn Wong and Daniel Gonzales, at wong@rand.org and gonzales@rand.org (310-393-0411 x7843 and 703-413-1100 x5281, respectively).

Contents

Figures

Tables

Summary

This report describes a new technique developed by RAND to efficiently analyze multiple policy documents to identify potential conflicts, ambiguities, gaps, and overlaps in the roles and responsibilities (R&R) assigned to Department of Defense (DoD) executives. The technique consists of a framework and methodology. This report describes the framework and methodology as well as a new software tool that automates one step of the methodology.

In this study, an R&R is defined as an activity, function, task, duty, job, or action assigned to a DoD official by an authoritative source. Authoritative sources of DoD R&R are federal law; Office of Management and Budget circulars and other issuances; Executive Orders; agency guidance documents including DoD directives, instructions, and memoranda; and pertinent non-DoD policies and issuances such as Office of Homeland Security issuances that address the R&R of DoD officials.

Background

A complex set of interconnected DoD capabilities and resources are managed by the senior executives of the department using complex processes that evolve and change as DoD policy changes and as directed by U.S. law. Effective and efficient management of these capabilities and resources can be accomplished only if each DoD executive clearly understands and executes his or her responsibilities and if this is done in a way that is complementary and not in conflict with the activities of other DoD executives and the organizations under them. Therefore, it is essential that the R&R of DoD executives be clearly articulated in DoD policy. Recent legislation and changes directed by the Secretary of Defense are both changing the organizational structure of the DoD and shifting the R&R of defense officials. Policies that establish the R&R of defense officials will need to be updated to reflect these actions. The updated policies need to be consistent with U.S. law and existing policies that are not affected, thus requiring that policymakers and reviewers analyze large numbers of policies for potential conflicts, ambiguities, gaps, and overlaps.

Purpose

The purpose of this research is to develop a technique to efficiently and effectively assess many defense policies for potential conflicts, inconsistencies, ambiguities, overlaps, and gaps in the R&R assigned to government executives.

The methods and tools developed in this study are designed to enhance the analysts' ability to detect gaps and areas of potential conflict early in the policy review process, thereby focusing attention on the clarifications and changes that will result in consistent, clear, and effective policy.

Approach

Our approach was to first develop a framework that relates executive positions to roles and responsibilities and the products that result from their execution. The framework then served as a paradigm to formulate a methodology, which, in tandem with the framework, consists of a technique for analysis of policy guidance related to R&R assigned to defense officials. One step of the methodology was suitable for automation. The software tool developed to automate that step of the methodology is named Electronic Policy Improvement Capability, or EPIC (©, ™, RAND, 2010). The technique affords a new semiautomated capability to analyze R&R assigned to defense executives.

We then applied the technique to three case studies to illustrate use of the technique, to serve as proof-of-concept demonstrations of the flexibility of the technique, and to validate and verify EPIC.

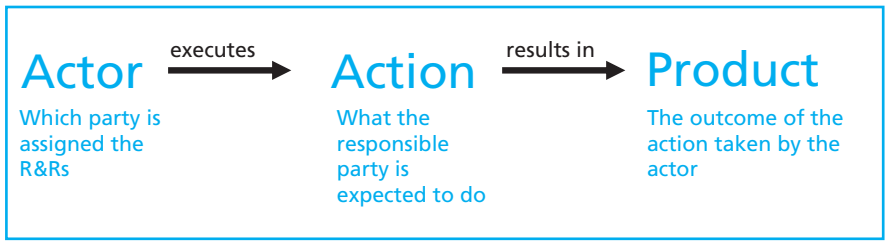
R&R Policy Analysis Framework and Methodology

Several pieces of information are needed to determine if potential conflicts, gaps, ambiguities, or overlaps exist in a collection of defense policies. We must know what parties are assigned R&R, what the policies direct the parties to do, and what output results when the parties execute the directed actions.

Framework

The roles and responsibilities analytic framework considers three primary components: the party who is assigned the R&R (termed the actor), what the actor is directed to do (termed the action), and the outcome of the action taken by the actor (termed the product). Figure S.1 shows this basic structure of the R&R analysis framework.

Figure S.1
R&R Policy Analysis Framework



RAND *TR1277-S.1*

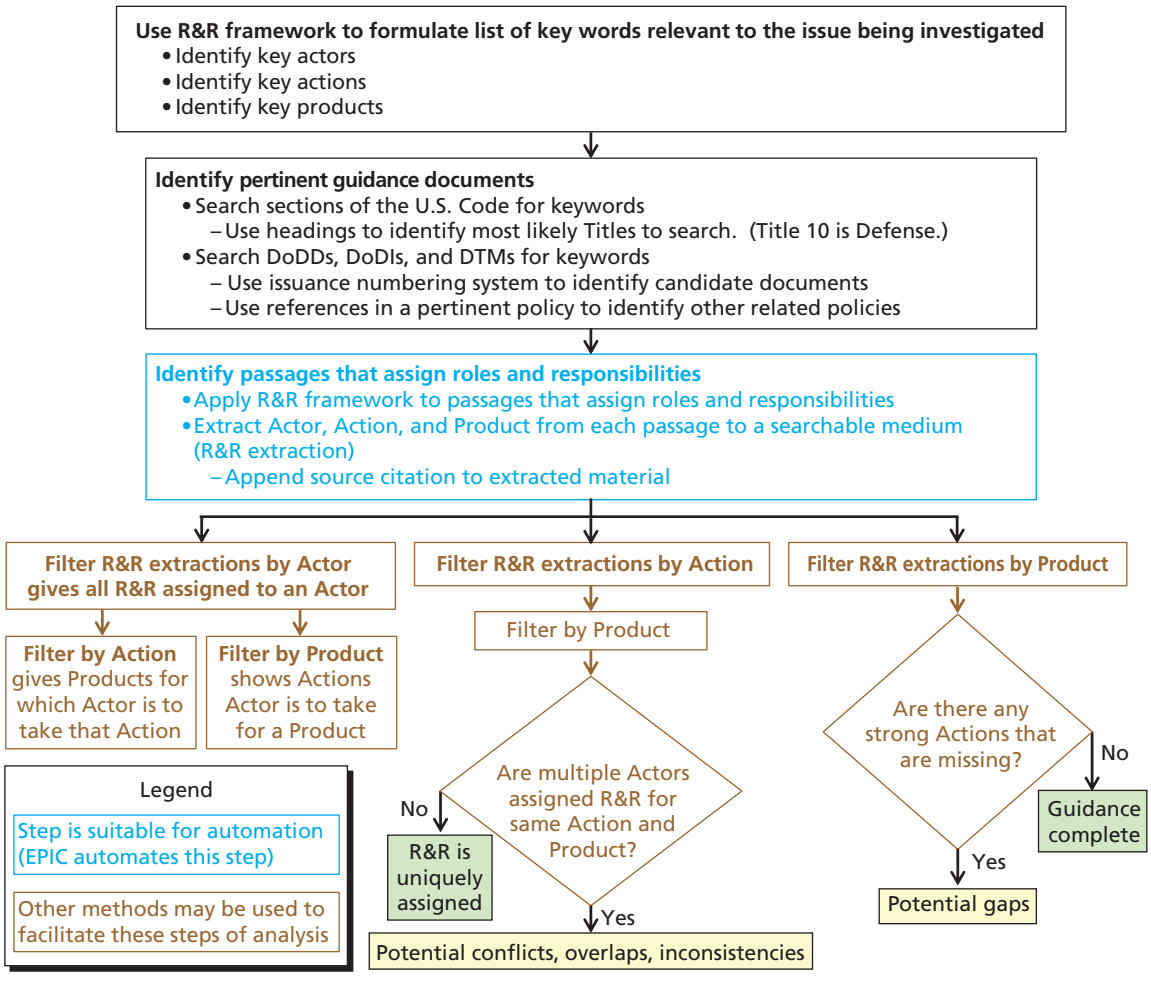
Methodology

Using the R&R policy analysis framework described above, analysts can examine related bodies of policy to compare the R&R assigned to defense executives. If more than one actor is assigned to take the same action on the same product, then a potential conflict exists in the body of policy. If, on the other hand, no executive is assigned to take action on a product, then there is a potential gap in the body of policy. Hence, the R&R framework lends itself to a methodology for identifying potential conflicts, inconsistencies, gaps, ambiguities, and redundancies in defense policy. The steps of such an R&R methodology are shown in Figure S.2.

Electronic Policy Improvement Capability

To use the policy analysis framework described above, the analyst needs to create a searchable file (such as a spreadsheet) that shows the actor, action, and product components of R&R assigned to defense officials in policies. Building R&R spreadsheets is labor-intensive and time-consuming. RAND has addressed this issue by developing and building EPIC to facilitate

Figure S.2
R&R Methodology



RAND *TR1277-S.2*

R&R analysis.[1] EPIC is an automated tool that uses the policy analysis framework to enable keyword searches of policy documents. EPIC searches for occurrences of user-selected keywords from built-in lists of actors, actions, and products in policy documents and automatically records sentences from the document that contain combinations of the user-selected keywords in a MS Excel worksheet. The user can manually parse, sort, and filter through results relatively quickly to determine relevance. EPIC also outputs a version of the scanned policy as an Extensible Markup Language (XML) document with the actors, actions, and products of interest highlighted. An analyst can review the document to determine the completeness of the Excel results worksheet.

Program Manager R&R Case Study

Our program manager (PM) case study has a dual purpose: (1) to determine the purview of PM R&R, particularly as these R&R apply to the acquisition of weapon systems with national security system or information technology elements, and (2) to validate the EPIC tool via a concrete indication of how R&R found by EPIC compare with R&R found by manual examination.

We ran EPIC on 21 key policy documents relevant to PMs, specifying the term "program manager" and all of its variants as the single actor of interest. EPIC extracted sentences from 11 of the 21 documents indicating that PMs are assigned R&R in 11 of the 21 policies examined. Once duplicates were eliminated, there were 136 unique extractions, 111 of which were from Department of Defense Instruction (DoDI) 5000.02. We found that 5 percent of the EPIC extractions from DoDI 5000.02 were false positives that did not actually contain PM R&R.

After manual refinement of the database, we found that EPIC helped identify 94 percent of the PM R&R in DoDI 5000.02. This shows that EPIC complements human analysis but does not replace it. While EPIC output can provide PM R&R insights to analysts of all experience levels, the identification of any remaining R&R not detected by EPIC will be less challenging for analysts already familiar with PM R&R.

Analysts used EPIC output to determine that the purview of PM R&R is extensive. PMs must be cognizant of the contents of at least 11 policy issuances, be thoroughly familiar with DoDI 5000.02, and execute at least 132 R&R in DoDI 5000.02 alone to perform PM functions.

Interoperability and Standards Case Study

The purpose of this case study was to demonstrate the utility of applying EPIC to four DoD policies across a broad array of topics related to interoperability and standards R&R to identify areas of potential conflict. In this case study, we focused on R&R that include decisionmaking authority, and we term such R&R as "strong" R&R. We used filtering on EPIC output to efficiently find potential R&R conflicts. EPIC reduced 243 pages of policy to 1,137 unique extractions. Filtering by analysts showed that 113 of the extractions were related to standards. Analy-

[1] The EPIC tool is a Microsoft (MS) Office–based program written in Visual Basic for Applications. It runs on the MS Windows platform with MS Office 2003 Professional or MS Office 2007. EPIC is described in detail in the appendix.

sis of the 113 standards-related extractions found that DoDD 5144.1 assigns strong R&R for intelligence standards to the DoD chief information officer (CIO), whereas DoDI 4630.8 and Chairman of the Joint Chiefs of Staff Instruction 6212.01E assign similar strong R&R for intelligence standards to the National Security Agency, the Defense Intelligence Agency, and the National Geospatial-Intelligence Agency (NGA) with no role for the DoD CIO. While strong R&R do not inherently lead to conflicts, the similarities among these assignments of R&R can lead to conflicts as the various officials execute their duties.

Analysis of the distribution of R&R in the four policies found that the strong R&R for information assurance (IA) are evenly distributed among three major actors—the Defense Information Systems Agency, NGA, and DoD CIO, creating a potential for conflicts to arise when these actors execute their assigned responsibilities.

Categorizing the EPIC output by topic revealed that only weak links exist between the development of interoperability standards/architectures and the determination of interoperability requirements, and that Net Ready-Key Performance Parameters requirements are inconsistent in defense policy.

Information Assurance Case Study

Entity relationship (ER) diagramming is a systematic method for defining relationships between specific entities such as actors, actions, and products. Applying ER diagramming to EPIC output allows analysts to quickly identify possible conflicts and inconsistencies for information assurance managers, PMs, designated approval authorities, and security managers across the DoD 8500-series documents. The inconsistencies found include issues pertaining to the accreditation status of those DoD information systems with a Category II weakness and an Interim Authority to Operate status, and to the setting and implementation of IA controls. We also identified possible inconsistencies in R&R for certification and accreditation across the DoD 8500-series issuances, and with regard to determining the applicability of DoDI 8581.1 for some legacy space systems.

Study Products

Aside from the potential conflicts discovered in the policy documents examined in the case studies, the framework, methodology, and EPIC are the primary products of this study. The framework provides the basis of the methodology, and EPIC automates one step of the methodology. Analysis of EPIC output is still required to identify gaps, overlaps, and areas of potential conflict in the R&R assigned to defense executives. As the case studies show, a variety of methods can be used to facilitate analysis of EPIC output to identify potential conflicts, inconsistencies, gaps, redundancies, ambiguities, and overlaps in a collection of policy documents.

Potential Next Steps

This study demonstrates the potential and promise of a new technique for policy analysis. The new technique should facilitate policy analyses suggested by DoD officials such as the following:

- Investigate potential conflicts identified in the case studies. Detailed investigations into the potential conflicts identified in the case studies are required to determine whether actual conflicts exist and to recommend actions to correct policy if actual conflicts are found.
- Develop a process to identify the origins of R&R conflicts. This would involve developing a technique that would allow for full-spectrum analysis of R&R from their origins in U.S. law to DoD-level policy and finally to Service-level implementation documents. Such research would help identify the root causes of R&R conflicts. Extending the automated policy format and processing capabilities of EPIC is a candidate approach.
- Use EPIC to review draft DoD and Navy policies. EPIC can help analysts determine if R&R in draft policy is internally consistent as well as consistent with the R&R found in existing policy.

The technique developed in this study provide policymakers and reviewers with new capabilities for identifying gaps, ambiguities, overlaps, inconsistencies, and areas of potential conflict in policy. This new capability can result in better and more consistent defense policy.

Acknowledgments

The authors wish to thank the following for their guidance and support of this research: Carl Siel, Chief Engineer, Assistant Secretary of the Navy for Research, Development, and Acquisition (RDA), when this study commenced; Ricardo Cabrera, Deputy Chief Engineer and then Acting Chief Systems Engineer (CHSENG), RDA; Dr. Cheryl Walton, former Director, Standards, Policy, and Guidance (SPG), RDA CHSENG; Lynn Petersen, current Director, Systems Engineering and Policy (SE&P), Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation (DASN RDT&E); Kenneth Ives, current Deputy Director, SPG, DASN RDT&E SE&P; and Kevin Lowther, current Technical Director, Policy and Standards, SPG, DASN RDT&E SE&P. The authors also acknowledge, with gratitude, the contributions of team members John Fitzpatrick, Carroll Gainier, and Jin Yi, whose collective contributions in coding, testing, and providing material for various versions of user's guides were all instrumental to the development of EPIC. In addition, the authors thank several colleagues at RAND for their insightful observations and careful reviews: Philip Antón, director of the Acquisition and Technology Policy Center (ATPC) in the RAND National Defense Research Institute, and Mark Arena, deputy director of the ATPC at the time this study commenced; Cynthia Cook, current director of ATPC; and Jim Bartis and Jeff Drezner, reviewers of this report.

Abbreviations

ACAT	acquisition category
ACTD	Advanced Concepts Technology Demonstration
ADM	Acquisition Decision Memorandum
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ASN RDA CHENG	Assistant Secretary of the Navy, Research, Development, and Acquisition Chief Systems Engineer
ATPC	Acquisition and Technology Policy Center
AV	all view
C&A	Certification and Accreditation
CA	certification authority
CAIG	Cost Analysis Improvement Group
CAT	category
CDD	Capability Development Document
CDP	Capability Development Plan
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CL	Confidentiality Level
COCOM	combatant command
COMSEC	communications security
COTS	commercial-off-the-shelf

CPD	Capability Production Document
C/S/A	components/Services/agencies
DAA	designated approving authority
DARS	DoD Architecture Registry System
DAS	Defense Acquisition System
DATO	Denial of Authorization to Operate
DBSMC	Defense Business Systems Management Committee
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DTM	Directive Type Memorandum
DUSD(A&T)	Deputy Under Secretary of Defense (Acquisition and Technology)
EPIC	Electronic Policy Improvement Capability
ER	entity relationship
FISMA	Federal Information Security Management Act
GEOINT	geospatial intelligence
GIG	Global Information Grid
HUMINT	human intelligence
I&S	interoperability and standards
IA	information assurance
IAM	information assurance manager
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
IEA	Information Enterprise Architecture
IP	Internet Protocol

IRB	Investment Review Board
IS	information system
ISP	Internet Service Provider
ISR	intelligence, surveillance, and reconnaissance
ISSE	information system security engineering
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
JFCOM	Joint Forces Command
JITC	Joint Interoperability Test Command
JTRS	Joint Tactical Radio System
KPP	Key Performance Parameters
MAC	Mission Assurance Category
MASINT	measurement and signatures intelligence
MDA	Milestone Decision Authority
MS	Microsoft
NCOW-RM	Net-Centric Operations and Warfare Reference Model
NGA	National Geospatial-Intelligence Agency
NII	Network and Information Integration
NR-KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
NSG	National System for Geospatial Intelligence
NSS	National Security System
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense
OV	operational view
PAA	Principal Accrediting Authority
PDF	Portable Document Format
PEO	program executive officer
PKE	Public Key Encryption
PKI	Public Key Infrastructure

PM	program manager
POA&M	Plan of Action and Milestones
R&R	roles and responsibilities
RTF	Rich Text Format
SAASM	Selective Availability Anti-Spoofing Module
SAIO	Senior Information Assurance Officer
SIGINT	signals intelligence
SM	security manager
SV	systems and services view
T&E	test and evaluation
TDL	Tactical Data Link
TEMP	Test and Evaluation Master Plan
TV	technical standards view
USD	Under Secretary of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)	Under Secretary of Defense (Comptroller)
USD(P)	Under Secretary of Defense for Policy
USSOCOM	U.S. Special Operations Command
USSTRATCOM	U.S. Strategic Command
XML	Extensible Markup Language

CHAPTER ONE

Introduction

This report presents a new technique that can be used by analysts to efficiently and effectively analyze large bodies of policies to identify potential conflicts, gaps, and overlaps in the roles and responsibilities (R&R) assigned to defense executives. This report describes the technique, which is composed of a framework and a methodology. It also describes a software-based tool developed by RAND that automates one step in the methodology. The report presents three case studies conducted using the new approach.

This study builds on a previous effort that examined the R&R of defense acquisition executives and chief information officers (CIOs).[1]

As in the previous study, R&R is defined as an activity, function, task, duty, job, or action assigned to a Department of Defense (DoD) official by an authoritative source. Authoritative sources of DoD R&R are federal law; Office of Management and Budget circulars and other issuances; Executive Orders; agency guidance documents, including DoD directives, instructions, and memoranda; and non-DoD policies and issuances.[2]

The new capability developed in this study will enhance analysts' ability to detect areas of potential conflict and alert policymakers to effect the necessary clarifications.

Background

The effective and efficient accomplishment of the DoD mission relies on a clear understanding and articulation of R&R assigned to defense officials in DoD policy. Recent legislation and changes directed by the Secretary of Defense are both changing the organizational structure of the Department of Defense and shifting the R&R of defense officials. For example, the Weapons Systems Acquisition Reform Act of 2009 established requirements that directly affect the operation of the Defense Acquisition System (DAS) and duties of key officials that support the DAS. Specifically, the Office of Program Assessment and Evaluation was transformed into a new office of Cost Assessment and Program Evaluation headed by a director and two newly created deputy director positions. Moreover, a new senior position, the Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, was created and is the focal point and principal advisor to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) for all practices, procedures, and workforce issues relating

[1] Daniel Gonzales, Carolyn Wong, Eric Landree, and Leland Joe, *Are Law and Policy Clear and Consistent? Roles and Responsibilities of the Defense Acquisition Executive and the Chief Information Officer,* Santa Monica, Calif.: RAND Corporation, MG-958-NAVY, 2010.

[2] Examples of non-DoD policies include Department of Homeland Security documents that affect the DoD and other such issuances by government agencies.

to developmental test and evaluation within the Department of Defense. Moreover, the Secretary of Defense directed disestablishment of the Office of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)). The ASD(NII) has been dual-hatted as DoD Chief Information Officer (DoD CIO). Some functions and duties of the ASD(NII) will be reassigned to the director of the Defense Information Systems Agency (DISA) while other ASD(NII) R&R will be retained by the DoD CIO. Furthermore, Congress has directed the Secretary of Defense to develop and implement a new acquisition process for information technology (IT). At the current time, the new IT acquisition process is being developed, and more shifts in R&R may occur as the process takes shape and DoD implements the new mandated process.

As these changes are being implemented, policies need to be updated and synchronized to reflect changes in the R&R of defense officials. The updated policies will need to be consistent with federal law, existing policies that are not changing, and yet-to-be-determined guidance that will implement the numerous changes that have been stipulated for the future. These factors point to the need for policymakers and their staffs to review and analyze large numbers of policies for potential conflicts, gaps, and overlaps of R&R. As DoD policy and DoD executive R&R become more complex and interwoven, such tasks become more difficult to carry out.

R&R of defense executives generally stem from language in the U.S. Code. Defense policies generally implement the legally prescribed defense executive R&R in a wide array of policies that address various aspects of defense interests. In this study, we focus on the R&R related to IT and the acquisition of defense systems that include IT. These R&R are found in a large collection of defense policies issued at different times and for different purposes. Hence, the number of policies that need to be examined to determine the purview of a defense executive's responsibilities can be quite large. In addition, since the policies are often, if not always, issued at different times, complete cross-referencing is often not present. These factors help create the current situation whereby a defense executive's R&R are assigned in many documents and may be articulated in ways that can lead to potential conflicts as executives attempt to execute their duties. This situation is further complicated by the multitude of changes being implemented as a result of recently enacted law or efforts to streamline defense operations to achieve increased efficiency. To effectively determine whether policies might lead to potential R&R conflicts, analysts must be thoroughly familiar with the precise language of many guidance issuances and analyze detailed accounts of the executive R&R assigned in a body of policy issuances. For example, to determine the purview of USD(AT&L) R&R, one must analyze the 71 DoD directives (DoDDs) and 111 DoD instructions (DODIs) that relate to the responsibilities of the office of the USD(AT&L).[3] These factors further confirm the need for policymakers and reviewers to analyze large numbers of policies for potential conflicts, gaps, and overlaps in R&R.

Purpose

This research develops a technique to efficiently and effectively assess many defense policies for potential conflicts, inconsistencies, overlaps, and gaps in the R&R assigned to government executives.

[3] See lists of Department of Defense issuances at Department of Defense, "DoD Issuances," website.

The methods and tools developed in this study are designed to enhance the analyst's ability to detect areas of potential conflicts, inconsistencies, overlaps, and gaps, to alert policymakers early in the policy review process to effect the necessary clarifications and changes that will result in consistent, clear, and effective approved policy.

Approach

Our approach was to first develop a framework that relates executive positions to roles and responsibilities and the products that result from their execution. Once the high-level framework was defined, successive lower layers were developed to further define the components of the framework. Key policy issuances were examined in detail to iteratively refine the definitional framework. The framework then served as a paradigm to guide a detailed analysis of several select policies to formulate a methodology that in tandem with the framework constitute a technique for analysis of policy guidance related to R&R assigned to defense officials.

Using the technique in the detailed analysis allowed the team to separate the steps of the methodology into those that are conducive to automation and those that require human analysis. We proceeded to automate the one step of the methodology that lent itself to automation. The automated portion of the methodology is named Electronic Policy Improvement Capability, or EPIC (©, ™, RAND, 2010). The technique affords a new semiautomated capability to analyze R&R assigned to defense executives.

We then applied the technique to three case studies to illustrate use of the technique, serve as proof-of-concept demonstrations of the flexibility of the technique, and to validate and verify EPIC.

Organization

Chapter Two describes the framework, the development of its components, and the methodology that uses the framework to form the new semiautomated policy analysis capability. Chapter Three describes the salient aspects of EPIC. Chapter Four presents the first case study, which examined the R&R assigned to DoD program managers. Chapter Five presents the second case study, which focused on interoperability and standards R&R. Chapter Six presents the third case study, which focused on information assurance R&R. Chapter Seven offers our closing remarks and recommendations. An appendix consists of a user's guide for the current version of EPIC.

CHAPTER TWO

The R&R Policy Analysis Framework and Methodology

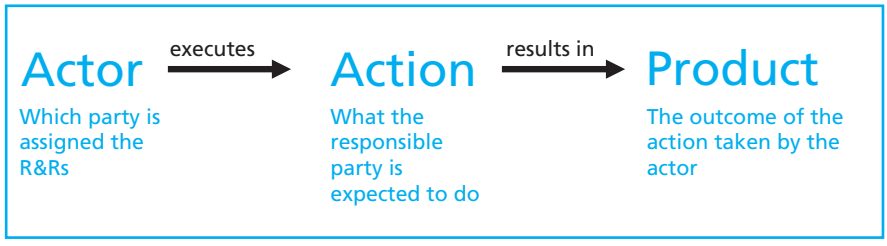
Several pieces of information are needed to determine if potential conflicts, inconsistencies, overlaps, and gaps exist in a collection of defense policy instruments. First, we must know which officials are assigned R&R. Second, we must know what the policy directs these officials to do. Third, we must know what output results when the officials execute the directed action. We can then compare who is responsible for what to determine if multiple officials appear to be responsible for the same thing—such a finding would indicate that conflicts may potentially arise as the multiple officials execute their assigned responsibilities. Similarly, if no official is assigned responsibility for a particular action or product, then a potential gap exists in the policy.

R&R Policy Analysis Framework

The framework developed to analyze the R&R of defense officials has the three primary components described above. The first component is the party who is assigned the R&R. We term this first component the *actor*. The second component is what the actor is directed to do to execute the R&R. We term this second component the *action*. The third component is the outcome of the action taken by the actor. We term this third component the *product*. Our basic R&R framework is shown in Figure 2.1.

The RAND team selected four key defense policy documents to guide the development of lower layers of the R&R framework. The four documents were selected based on their importance to information technology, National Security Systems (NSS), and acquisition. The selected policy documents are:

Figure 2.1
R&R Policy Analysis Framework



RAND *TR1277-2.1*

- **DoDD 5134.01,** *Under Secretary of Defense for Acquisition, Technology, and Logistics,* Director of Administration and Management, April 1, 2008
- **DoDD 5144.1,** *Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer,* Director of Administration and Management, May 2, 2005
- **DoDD 5000.1,** *The Defense Acquisition System*, Under Secretary of Defense for Acquisition, Technology, and Logistics, May 12, 2003
- **DoDI 5000.02,** *Operation of the Defense Acquisition System,* Under Secretary of Defense for Acquisition, Technology, and Logistics, December 2, 2008

The development of the framework components is described in the following sections.

Actor Component of the R&R Framework

Typically, an actor would be identified in authoritative guidance documents by the name of the office or the title held by the official. Examples include the Under Secretary of Defense for Acquisition, Logistics, and Technology and program manager (PM). Groups of individuals can also be specified in policy as actors, such as "Defense Business Systems Management Committee." In the case of actors identified by specific group names, the group as a whole is assumed responsible, so individuals in the group are expected to work together to execute the R&R. The responsible actor can also be identified by a general group name such as "senior officials." In this case, every member of the group (namely, every senior official) is assumed to be assigned the R&R.

The four key guidance documents were examined in detail to identify the actors assigned R&R. Table 2.1 shows 63 different terms for parties who are assigned R&R in the four key documents. Our examination of these actors showed that the same actor could be referred to by different names. For example, as Table 2.1 shows, the Cost Analysis Improvement Group is called CAIG as well as Office of the Secretary of Defense CAIG or OSD [Office of the Secretary of Defense] CAIG. During our examination of the four key documents, variations on names for the same actors were noted to ensure that R&R assigned to different names for the same actor would be attributed to a single actor.

Action Component of the R&R Framework

The action would typically be an action verb in guidance documents. Defense officials are assigned to perform a large range and scope of actions. For this reason, we separate the actions into two categories that reflect the level of decisionmaking authority the action includes. We term actions that encompass decisionmaking authorities that are not typically controlled or circumscribed by other actors as *strong* actions. Examples of strong actions are setting, establishing, and directing policy; overseeing the implementation of policy; and selecting among competing bids. Other actions that indicate more circumscribed decisionmaking authority, such as advising other officials or making recommendations to other executives who hold the decisionmaking power, are termed *advisory* actions.

While the context of the R&R needs to be considered in determining the exact scope and authority in the R&R, strong actions are of primary interest in this study because R&R expressed with strong actions are those that could potentially result in conflict with strong actions assigned to other officials. Advisory actions are less likely to conflict with R&R assigned

Table 2.1
Actors Assigned R&R in Key IT Acquisition Documents

Acquisition executive of DoD components	DUSD(A&T)
Acquisition managers	Executive agent
Acquisition participants	Information Technology Acquisition Board
ASD(NII)/DoD CIO	Integrated Product Team
ASD(C3I)	Investment Review Board (IRB)
Attorney	IRB chair
CAIG Chair	Joint Interoperability Test Command (JITC)
Chairman of Joint Chiefs of Staff (CJCS)	Lead DoD component
CIOs	Lead or Chief Engineer
Component Acquisition Executive (CAE)	Managers
Configuration Steering Board	Materiel developer
Contractor	Milestone Decision Authority (MDA)
Contractor employees	Military departments
CAIG	OSD CAIG
DBSMC chair	Office of Technology Assessment
Decision authorities	Overarching Integrated Product Team (OIPT) leader
Defense Acquisition Board	OSD officials
Defense acquisition executive	Others responsible for acquisition involving foreign governments
DBSMC	OIPT
Director, National Intelligence	Principal staff assistant
Director, Defense Procurement and Acquisition Policy, and Strategic Sourcing	PM
Director, Operational Test and Evaluation	Programs
Director, Program Analysis and Evaluation	Requirements and resources authorities
Director, Systems and Software Engineering	Responsible test organization
DoD	Secretaries of military departments
DoD component CIO	Senior officials
DoD component decision authorities	Service acquisition executive
DoD component heads	Subject matter experts
DoD component program executive officer (PEO)	USD(AT&L)
DoD component senior officials	Under Secretary of Defense (Comptroller) (USD(C))
DoD components	Under Secretary of Defense for Policy (USD(P))
	Users

SOURCES: Department of Defense Directive 5134.01, December 9, 2005; Department of Defense Directive 5144.1, May 2, 2005; Department of Defense Directive 5000.1, May 12, 2003; and Department of Defense Instruction 5000.02, December 2, 2008.

to other officials because advisory actions do not typically involve unique decisionmaking authority.

Strong actions include verbs that indicate responsibility to lead, ensure, establish, control, or integrate. Many verbs can convey responsibility to lead or responsibility to ensure or any of the other strong actions. For example, "chair," "direct," and "manage" can all convey a leadership role. We examined the four key policies to identify specific verbs that fall into the lead, ensure, establish, control, and integrate strong action subcategories. These verbs are shown in Table 2.2.

Advisory actions include verbs that convey responsibility to develop, perform, recommend, or communicate. Again, many verbs can convey responsibility to develop or responsibility to perform or any of the other advisory actions. For example, "execute," "exercise," and "undertake" can all convey a perform role. We examined the four key policies to identify specific verbs that fall into the develop, perform, recommend, and communicate advisory action subcategories. These verbs are also shown in Table 2.2.

In some cases, an official is assigned an R&R that is to be executed "in conjunction with" or "in collaboration with" one or more other parties. In these cases, all of the named officials are assumed to be assigned the R&R and are expected to work together to execute the action. In other words, all named parties are assumed to be assigned the R&R.

Sometimes, guidance issuances assign an R&R to an official and direct that the official execute the R&R "in consultation with" one or more other parties. In these cases, the official assigned the R&R is assumed to have the primary responsibility for the strong action and the parties that are to be consulted have advisory roles.

In the case of the action component of the framework, the separation of verbs into the strong and advisory actions are useful to understand the level of responsibility assigned to an actor and determine if potential conflicts might result.

Table 2.2
Strong and Advisory Actions

Category	Subcategory	Examples
Strong	Lead	Lead, be accountable, budget, chair, coordinate, determine, direct, enforce, manage, oversee, plan, pursue, resolve, serve, supervise
	Ensure	Ensure, encourage, preserve, require, set, structure
	Establish	Establish, assign, issue, prescribe, process, provide
	Control	Control, approve, authorize, certify, negotiate
	Integrate	Integrate, synchronize
Advisory	Develop	Develop, design, fuse, discover, enable, fulfill, implement, maintain, make, sponsor, tailor
	Perform	Perform, access, execute, exercise, program, retrieve, submit, undertake, use
	Advise	Advise, assess, assist, consult, evaluate, facilitate, recommend, report to, review, support
	Communicate	Communicate, address, advertise, convey, identify, notify, post, recognize

SOURCES: DoDD 5144.1, DoDD 5134.01, DoDD 5000.1, DoDI 5000.02.

Product Component of the R&R Framework

Products are the output resulting from the actor executing the action prescribed in a policy. Since defense officials are ultimately responsible for everything emanating from the DoD, the range of products is very large. For example, a product could be a policy or other guidance, a document, a decision, follow-up activities by other individuals, a communications exchange among officials, or any number of other outputs. A product categorization was developed to facilitate analysis of the scope of products for which individual defense officials carry responsibility. For the analysis of R&R related to IT and the acquisition of Navy systems that include IT, we identified 13 general product categories from the examination of the four policies listed above:

- guidance
- people
- process
- doctrine
- IT goods
- activities
- documents
- program
- non-program
- maintenance
- disposal
- reference other authority
- other.

Our examination of the key documents showed that some categories encompassed many individual products that could be classified as major subcategories within the generic list shown above. For example, the guidance category could be broken down into policy, standards, and architectures. Since officials assigned strong actions in the policy area would not likely conflict with officials assigned the same strong actions in the architectures area, breaking the general product categories into subcategories is useful in determining potential conflicts. The team used the actual products identified through detailed manual examination of the four key policy documents to break selected product categories into subcategories where appropriate. Table 2.3 shows the final categorization scheme developed for the product framework component.

R&R Methodology

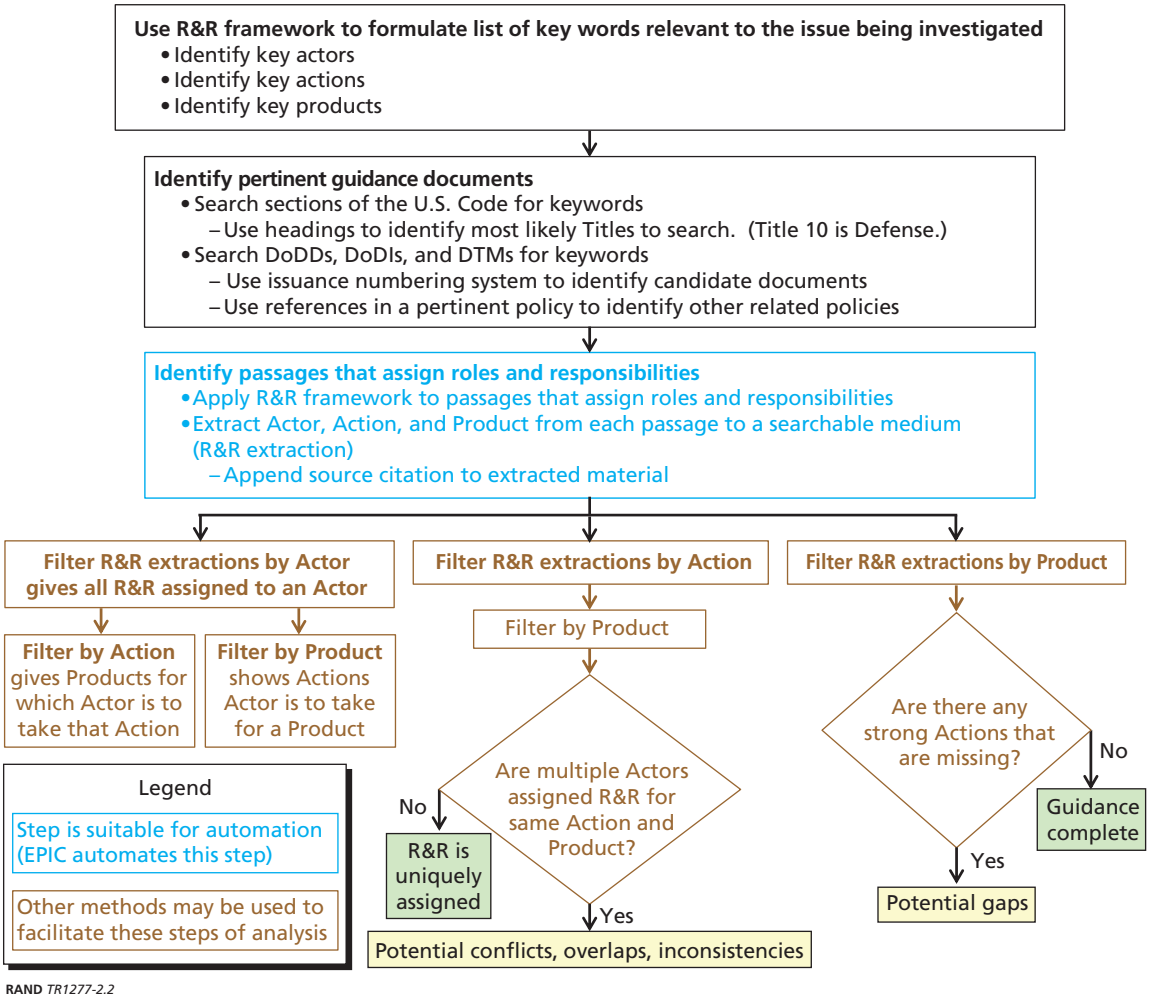
Using the R&R policy analysis framework described above, analysts can examine related bodies of policy to compare the R&R assigned to defense executives. If more than one actor is assigned to take the same action on the same product, then a potential conflict exists in the body of policy. If, on the other hand, no executive is assigned to take strong action on a product, then there is a potential gap in the body of policy. Hence, the R&R framework lends itself to a methodology for identifying potential conflicts, inconsistencies, gaps, and redundancies in defense policy. The steps of such an R&R methodology are detailed in the following paragraphs and illustrated in Figure 2.2.

Table 2.3
Product Categorization Scheme for R&R Related to IT and the Acquisition of Navy Systems That Include IT

Category	Subcategory	Examples
Guidance	Policy	Policy, strategies, procedures, plans, goals, measures, baselines, approaches, approval, agreements, guidance, oversight, compliance, cooperation, legal review, funding, objectives, alternatives, life cycle, law, international agreements, arrangements
	Information standards	Common set, interoperability, information assurance, standards, protocols, requirements, joint concepts, systems integration, interfaces, inventory, design criteria/standards
	Architectures	Structures, GIG, information networks, communications networks, governance of structures, technical views, Financial Management Enterprise Architecture, architectures, exchange, design
People	People	Sponsor, lines of responsibility
Process	Process	Management, practices, implementation, communications, tailoring in, reviews, system performance, systems management, transition, assessment, teaming, competition, costs, constraints, affordability, investment, contracts, management stucture, risk, projections, dollars, manpower
Doctrine	Doctrine	
IT goods	Spectrum	Electromagnetic spectrum
Activities	Training	Training
	Testing	Testing agency, testing and evaluation
	Operations	Operations, operational effectiveness, suitability, survivability
Documents	Definition documents	Preliminary design review, CDD, acquisition strategy, cost estimates, test plans, requirements documents, CDP, Technology Readiness Assessment, capability document, program documents
	Certification documents	Clinger-Cohen Act, IA certification and accreditation
	Direction issuances	ADM, MDA recommendations to cancel program, entry, decisions
	Miscellaneous issuances	
Program	Platforms	
	Ships	
	Information system hardware	
	Software	
	Facilities	
Non-program	Non-program related wares	Initiatives, COTS, ACTD, facilities, security support, safety, research, research and development, science and technology, system performance, knowledge, installations, environment, equipment, space matters, NII support, CIO support, commercially developed technologies, prototype efforts, activities, OSD study program
Maintenance	Maintenance, logistics, support	
Disposal	Disposal	Decommissions, preservation, scrap, recycle, elimination
Reference other authority	Reference other authority	Perform duties per authority
Other	Other	

SOURCES: DoDD 5144.1, DoDD 5134.01, DoDD 5000.1, and DoDI 5000.02.

Figure 2.2
R&R Methodology



Formulate Keywords

The first step analysts need to take to determine if R&R are complete and consistent with respect to a particular issue or topic is to use the basic R&R framework to identify keywords relevant to the issue or topic. The analysts need to specify the actors of interest, actions related to the issue or topic, and pertinent products. The combined lists of actors, actions, and products pertinent to the issue or topic are the keywords relevant to the issue. Once a set of key actors, actions, or products pertaining to a particular issue have been identified, these lists can be stored for future use, so an analyst need not formulate keywords from scratch for each subsequent R&R analysis. Rather, the analyst can peruse the existing lists, select those of interest, and add keywords as appropriate.

Identify Relevant Authoritative Documents

The second step analysts must take to assess the R&R of defense officials with respect to an issue or topic is to identify authoritative guidance documents relevant to what is being examined. Analysts can identify relevant issuances by searching documents for one or more key-

words. In addition, analysts can identify relevant documents by the title and headings in the documents or use the numbering schemes for Department of Defense directives, Department of Defense instructions, and Directive Type Memorandums to identify guidance related to the issue or topic being examined.[1] Once an analyst has identified a relevant document, the reference section of that document can be used to identify other issuances that might be related to the issue being examined.

Identify R&R Passages

Careful reading of each relevant document will allow analysts to identify specific passages in each document that assign roles and responsibilities to officials of interest and that are pertinent to the issue being addressed. Analysts can apply the basic R&R framework to identify the actors, actions, and products in the passages. Passages that include actors, actions, and products that match keywords of interest will be the R&R passages of interest. Analysts can then extract the actor, action, and product to a searchable medium such as a spreadsheet. By appending the source citation to the extracted material, analysts can create referenced searchable files that show the actor, action, and product components of R&R assigned to defense officials in policy issuances.

Determine the Purview of an Official's Authority

Separating the R&R extractions by actor will yield lists of actions and products that each actor is responsible for. The analysts are thus provided with a description of the purview of an actor's responsibilities with respect to the issue being examined. Subsequent filtering by action will show the products that each actor is to take for a particular action. Similarly, subsequent filtering by product will show all of the actions an actor is directed to take regarding a particular product.

Identify Potential Conflicts and Inconsistencies

The R&R extractions can also be first filtered by action and then by product. Filtering the R&R extractions in this order allows the analyst to compare action-product combinations to determine if multiple actors are assigned responsibility for the same action and product. If so, then there is potential R&R inconsistency and conflict because more than one actor has been assigned responsibility for the same action on the same product. The analyst would have to read the specific passages assigning the R&R to determine if a conflict actually exists. For example, if the hierarchy of the policy documents or the echelons of the organizations indicate an oversight relationship among the officials assigned similar R&R, there may not be an actual conflict. On the other hand, if two policies implement the same section of federal law with R&R assigned to different officials of equivalent rank, there may be a conflict in policy.

If more than one policy reiterates the same R&R for the same actor-action-product combination, then there is a potential redundancy or overlap. The analysts could then review the actual passages in the policies to determine if an actual redundancy or overlap exists.

---

[1] For example, the Department of Defense Issuance numbering system is available online at http://www.dtic.mil/whs/directives/corres/writing/Issuance_Numbering.pdf. In addition, Joint Staff Manual 5701.01E, entitled Formats and Procedures for Development of CJCS, JS, and J Directorate Directives, September 19, 2011, provides guidance for the numbering scheme for joint issuances. Similarly, the Secretary of the Navy Manual SECNAV M5210.8 directs use of Navy Standard Subject Identification Codes.

It should be noted that other analytic methods may be used to facilitate the execution of this step. The benefits of using supplemental methods will depend on the specific issue being examined. The case studies will illustrate use of analytic methods such as mapping techniques, distribution analysis, and entity relationship diagramming.

Identify Potential Gaps

Analysts can separate the R&R extractions by product and then examine the actions that are to be taken for each product. If there are missing strong actions, then no actor has been assigned responsibility for a decision in the body of issuances examined, so there is a potential gap in the policy. In such a case, the analyst may search for additional issuances that may assign the missing responsibility. If no other guidance is found, then a gap exists in the R&R with respect to the issue being examined.

Once again, this step might be facilitated with use of supplemental analytic techniques. The advantages of supplemental techniques will depend on the issue being examined. The case studies will illustrate several supplemental methods such as mapping techniques, distribution analysis, and entity relationship diagramming.

CHAPTER THREE

The EPIC Tool[1]

Building the searchable R&R files for the body of policy issuances relevant to a particular issue would typically involve carefully examining every sentence in the relevant policies and manually building the database one component at a time. Thus, an analyst would have to identify a passage in a document that contains an actor, action, or product of interest and then enter the actor, action, and product in a searchable medium such as a spreadsheet. Clearly, creating such an R&R spreadsheet is a labor-intensive and time-consuming task. Such a task is also prone to error because the analyst would have to identify three pieces of information per relevant statement and accurately copy items to the appropriate place in a searchable medium. Fortunately, such tasks are also conducive to automation. In this chapter, we summarize the salient aspects of a tool developed for this study that performs the search, locate, and extract tasks. The tool is called Electronic Policy Improvement Capability, or EPIC. EPIC facilitates building spreadsheets that can be used by analysts to conduct R&R policy analysis.

Once R&R spreadsheets have been created, analysts can use them as databases to perform comparisons, to generate statistics, and to discover R&R that can potentially lead to conflicts or gaps in roles and responsibilities. Such analysis tasks are inherently human-oriented and not conducive to automation. The case studies presented in Chapters Four through Six demonstrate a variety of analysis methods that analysts can apply to spreadsheets generated by EPIC to gain insights into potential areas of R&R conflict and gaps in defense policy.

One primary motivation for developing EPIC was to facilitate the analysis of policy documents for which existing methods and tools were of limited use. An entirely manual analysis of policy documents is labor-intensive because of the length or complexity of the defense policy issuances. While a reader can analyze a single document, tracking issues across many documents simultaneously quickly becomes unmanageable.

Commonly used document readers, such as Adobe's Portable Document Format (PDF) and web-based document libraries, are capable of scanning a document for a single, specific search string; however, the ability to scan for a single search term does not necessarily facilitate the process of searching for and identifying potential roles and responsibility statements of interest where actor, action, and product must be simultaneously known. Also, the results from scanning a document with these traditional document tools are difficult to manipulate and edit, making application of analytic tools such as statistical routines difficult, if not impossible, to apply. In addition, the results from such document readers must be recorded and archived separately, further inhibiting necessary analysis across many policy documents.

[1] This chapter describes version 5.6.8.1 of EPIC.

Using native search tools in PDF or MS Word applications also makes it difficult to record when a search returns unnecessary portions of the document. For example, the term "plan" may be used as either a verb indicating an action or a noun indicating a product, but most tools do not record search results in a form that allows the user to mark which usages of the term "plan" are interesting and which were irrelevant to the user's purpose (e.g., the identification of areas of potential conflict).

EPIC addresses the need for a document-searching tool that can analyze, manipulate, and archive search results in a way that allows users to apply a variety of analytic methods to discover information and gain insights. EPIC is an automated tool that searches for syntactically specified occurrences of keywords in policy documents and catalogs policy statements found in those documents. The tool is an MS Office–based program written in Visual Basic for Applications. EPIC is stored as an MS Excel Workbook. It runs on MS Windows platforms with MS Office 2003 Professional or MS Office 2007.

Because EPIC scans a document with user-inputted keywords and the document is scanned for occurrences of combinations of the keywords, the tool searches for statements and phrases rather than single terms, which are potentially more relevant and of more interest to the user in performing the R&R analysis of the document. EPIC automatically records the results in an MS Excel worksheet, which allows the user to parse, sort, and filter through results relatively quickly and easily for relevancy of the result statements. EPIC also generates a marked-up version of the scanned document using Extensible Markup Language (XML). The analyst can visually examine the XML document to determine the completeness of the Excel results worksheet.

The appendix provides a detailed description of how EPIC works and shows examples of the output files.

CHAPTER FOUR

The Program Manager Case Study

Purpose

The program manager case study has a dual purpose. First, it is used to determine the purview of PM roles and responsibilities, particularly as these R&R apply to the acquisition of weapon systems with NSS or IT elements. To determine R&R purview, we identified and examined pertinent DoD policies, counted the R&R assigned to PMs in each document, and kept track of which documents contained PM R&R. The second purpose is to validate the EPIC tool. Specifically, we sought a concrete indication of how well EPIC finds R&R in terms of accuracy and completeness. For this case study, accuracy means how many PM R&R found by EPIC are truly PM roles and responsibilities. Completeness means the percentage of true PM R&R the EPIC tool was able to identify.

Approach

We identified 21 key policy documents as pertinent to DoD acquisition policy, program managers, NSS, and IT. Some of these documents were specified by the sponsor as policies of interest, others were known by the team as relevant policies, and some were identified by their titles. These policies were DoD directives and instructions and are shown in Table 4.1. We applied EPIC to each selected document. Since one of our purposes was to determine the purview of PM R&R, the PM was our single actor of interest for each of the 21 EPIC runs. The term "program manager" and all of its variants were used as the primary search terms under the actor category for each run. We chose all actions and all products to perform Actor and Action and Actor and Product searches.

EPIC extracted sentences from 11 of the 21 documents indicating that PMs are assigned R&R in 11 of the 21 policies we examined. The other ten documents are pertinent to acquisitions of IT and NSS but did not assign the PM roles and responsibilities. EPIC extracted a total 753 sentences from the scanned documents, including duplicates. DoDI 5000.02, *Operation of the Defense Acquisition System,* clearly dominated the field, with 475 extractions from that document alone. Once the duplicates were eliminated, there were 136 unique extractions, 111 of which were from DoDI 5000.02. Since DoDI 5000.02 contained nearly 82 percent of the R&R, this case study will focus on DoDI 5000.02. Table 4.1 shows a summary of the number of extractions made by EPIC and the number of unique extractions for each policy.

Table 4.1
Documents Searched for PM R&R by EPIC

Document Type and Number		Document Title	No. of EPIC Extractions	No. of Nonredundant Extractions
DoD Directive	3020.49	Orchestrating, Syncronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution	0	0
	3200.12	Dod Scientific and Technical Information (STI) Program (STIP)	3	1
	3222.4	Electronic Warfare and Command and Control Warfare (C2W) Countermeasures	4	1
	4630.05	Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	0	0
	4650.05	Positioning, Navigation, and Timing (PNT)	0	0
	5000.01	The Defense Acquisition System	93	7
	5000.59	DoD Modeling and Simulation (M&S) Management	0	0
	5134.01	Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))	6	1
	5144.1	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/(DoD CIO)	8	1
	8100.02	Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)	0	0
	8115.01	Information Technology Portfolio Management	0	0
	8320.03	Unique Identification (UID) Standards for a Net-Centric Department of Defense	0	0
	8500.01E	Information Assurance (IA)	0	0
	8570.01	Information Assurance (IA) Training, Certification, and Workforce Management	28	3
	8581.01	Information Assurance (IA) Policy for Space Systems Used by the Department of Defense	34	2
DoD Instruction	5000.02[a]	Operation of the Defense Acquisition System	475	111
	5000.35	Defense Acquisition Regulations (DAR) System	0	0
	5000.61	DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)	0	0
	8430.02	Netops for the Global Information Grid (GIG)	4	1
	8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	29	3
	8580.01	Information Assurance (IA) in the Defense Acquisition System	69	5
		Total	753	136

[a] This is the document examined in the case study.

EPIC Validation

In this case study, an analyst reviewed every sentence in DoDI 5000.02 and manually extracted PM R&R. The results of the analyst's examination were compared with the results of the EPIC search of DoDI 5000.02. The EPIC output was analyzed and refined as indicated by the manual review. This in-depth comparison is described below. The description indicates the utility of EPIC, shows the interface between tool and analyst, and demonstrates how policy analysis can be facilitated by EPIC.

False Positive Extractions Indicate EPIC Accuracy

A false positive extraction is defined as a sentence extracted by EPIC that does not actually contain a true PM R&R. False positive extractions would include sentences found in definitions or other descriptive material. For example, the EPIC extraction from Section 3e of Enclosure 10 in DoDI 5000.02 reads as follows:

> Acquisition program responsibilities for programs not assigned to a PEO or a direct-reporting PM shall be assigned to a commander of a systems, logistics, or materiel command.

The above extraction does not contain a true PM R&R because the sentence does not charge the PM with carrying out any role, nor does it direct the PM to assume any responsibility. The statement merely implies that another party shall assign program responsibilities not assigned to a PEO or to a direct-reporting PM. As such, this extraction is labeled a false positive extraction for PM R&R in DoDI 5000.02.

Separate reading of the document by an analyst showed that the EPIC output contained six false positive extractions out of 111 unique extractions, which translates to 5 percent of the EPIC output being false positive extractions for DoDI 5000.02. The six false positive extractions were manually removed by the analyst to refine the EPIC output into an accurate database of PM R&R in DoDI 5000.02.

Limited Extractions to Improve Completeness

A limited extraction is defined to be extracted text that requires that the analyst read additional nonextracted text to determine PM R&R not in the EPIC output. An example of a limited extraction from Section 1b of Enclosure 5 in DoDI 5000.02 reads as follows:

> The DoD Component Requirements Authority, in conjunction with the Acquisition Community, is accountable for actions 1–5 in Table 8; the PM is accountable for actions 6–11.

This extraction indicates to the analyst that the PM is accountable for actions 6–11 but does not offer enough information for the analyst to judge what R&R the PM has been assigned. The analyst must read items 6–11 in the actual document to make the determination of what R&R the PM actually has as a result of this sentence. Hence, this extraction is categorized as a limited extraction. In this example, the items referred to in the extraction did not contain an actor, so EPIC did not extract the actual R&R because the text specifying the R&R did not include any variant of the term "program manager," which was our primary search term. For instance, item 7 referred to by the extraction reads as indicated below and is clearly a PM R&R:

Develop clearly established measures and accountability for program progress.

The EPIC output contained four limited extractions, and from these four limited extractions, the analyst identified eight additional PM R&R not included in the EPIC output. The analyst manually added the eight additional PM R&R to further refine the PM R&R database.

We define R&R statements as follows: nonredundant extractions with the R&R pointed to by limited extractions added in, the false positives subtracted out, and each extraction reviewed, attributed to a single actor, and otherwise cleaned by the analyst. Since an extraction can contain more than one PM R&R, the analyst separates the multiple R&R to create the final list of PM R&R statements in the PM R&R database. The completion of these steps shows that EPIC output included 116 out of 132 PM R&R in DoDI 5000.02, or 88 percent of the total. If we give EPIC credit for the R&R identified through limited extractions, then EPIC extractions helped identify 94 percent of the PM R&R in DoDI 5000.02.

Summary of Program Manager Case Study Findings

As stated in Chapter Two, strong roles and responsibilities are those that include decisionmaking authority. R&R that do not include decisionmaking authority are advisory in nature and hence are unlikely to lead to conflicts when defense officials execute actions to fulfill the responsibilities assigned to them by policies. Strong R&R are characterized by statements that include strong actions such as those shown in Table 2.2.

Our analysis of the R&R in DoDI 5000.02 shows that this instruction contains 106 strong PM R&R. EPIC extractions contained 99 of these 106 strong R&R, or 93 percent. An additional seven strong PM R&R were identified by the analyst. DoDI 5000.02 also contains 26 advisory PM R&R. EPIC extractions contained all 26 advisory PM R&R in DoDI 5000.02, or 100 percent.

The program manager study case demonstrates that EPIC can expedite the identification of PM R&R. EPIC helped identify 94 percent of the PM R&R in DoDI 5000.02. EPIC output is also fairly accurate. For DoDI 5000.02 in the PM study case, only 5 percent of the extractions were false positives.

The PM study case also shows that the purview of PM R&R is widespread. Among the duties the PM is charged with in DoDI 5000.02 alone are R&R that pertain to establishing and controlling policy and other issuances related to acquisition; leading, developing, and training staff; executing the acquisition process, including producing definition and certification documents; and communicating doctrine, spectrum, and testing elements to other parties. PM R&R are written in at least 11 major acquisition policy issuances with DoDI 5000.02 alone containing 132 PM roles and responsibilities. Hence, a PM must keep current with nearly a dozen defense policies and have comprehensive knowledge and understanding of DoDI 5000.02 to execute the duties necessary to manage a defense program.

CHAPTER FIVE

The Interoperability and Standards Case Study

Purpose

The purpose of this case study is to demonstrate the utility of applying EPIC to a handful of DoD policies across a broad array of topics related to interoperability and standards R&R to identify areas of potential conflict. In this case study, we show how different analysis techniques can be applied to EPIC results to identify potential conflicts, inconsistencies, gaps, and overlaps. We demonstrate the use of filtering, distribution analysis, and classic text mapping techniques on a single set of EPIC output. As will be shown, each of these post-EPIC analytic tools yields a different perspective useful for identifying potential conflicts, inconsistencies, gaps, and overlaps in the R&R assigned to DoD officials. The analyst should select the post-EPIC analytic tool most applicable to the question the analyst is addressing.

Approach

EPIC was applied to four key defense policy issuances pertinent to defense IT and NSS interoperability and standards. The four documents used in this case study are as follows:

- **DoDD 5134.01**, *Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)),* April 1, 2008
- **DoDD 5144.1**, *Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO),* May 2, 2005
- **Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E**, *Interoperability and Supportability of Information Technology and National Security Systems,* December 15, 2008.
- **DoDI 4630.8**, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* June 30, 2004.

These four documents contain a total of 243 pages of text. While that is not an overwhelming amount of material, manually identifying interoperability- and standards-related R&R and creating a searchable database would be a labor-intensive and time-consuming task required before analysis of the R&R could commence to identify potential areas of conflict. To facilitate the task, EPIC searches were run on the four documents.

The scan criteria used for the EPIC searches of all four documents were USD(AT&L) and ASD(NII) for the actors of interest; strong actions in the lead, control, establish, and ensure action subcategories; and all products. USD(AT&L) and ASD(NII) were selected as the two

actors of interest because these two positions govern defense IT and NSS interoperability and standards. Only strong actions were specified because only strong actions are likely to lead to potential conflict in policies that assign R&R. All products were specified because, for this task, the goal was to identify areas of potential conflict regardless of product.

The EPIC search of DoDD 5134.01 resulted in 314 extractions, 77 of which were nonredundant. The EPIC search of DoDD 5144.1 resulted in 441 extractions, 52 of which were unique. CJCSI 6212.01E had 1,854 extractions, 489 of which were nonredundant. DoDI 4630.8 had 3,371 extractions, 519 of which were unique. The combined total of all four searches was 5,980 extractions, of which 1,137 were unique. The results of these four EPIC searches are summarized in Table 5.1.

Identifying Areas of Potential Conflict Using Filtering

For this task, the team sought to quickly identify areas of potential conflict in R&R related to IT and NSS interoperability and standards. Analysts used filtering by product keywords of interest to further reduce the amount of text required to be reviewed to identify potential areas of conflicts in R&R related to the keyword product areas of interest. For example, filtering the EPIC output by the keyword "IT" would cause Excel to display only those extractions that have the keyword "IT." The analyst would then need only review the extractions that have the keyword "IT," thus reducing the number of extractions that need to be examined.

Filtering on the 5,980 extractions by keywords substantially reduced the number of extracted sentences relevant to the keyword. Specifically, filtering the extractions by the keyword "IT" and variants of this keyword showed that 418 extractions are relevant to information technology, of which 230 were nonredundant. Similarly, filtering the EPIC extractions by the keyword "NSS" and the variants of the term "NSS" showed that 338 are relevant to NSS, of which 211 were nonredundant. Filtering by the terms "interoperability" showed that 1,261 are relevant to interoperability, of which 413 are nonredundant. Finally, filtering the extractions by the term "standards" showed that 199 extractions are relevant to standards, of which 113 are nonredundant. These single-term filtering results are summarized in Table 5.2.

Figure 5.1 shows the R&R analysis process for this task of the interoperability and standards case study.

A detailed analysis of the R&R contained in the four documents shows that DoDD 5144.1 not only describes the DoD CIO's authorities over IT and NSS but specifically calls out

Table 5.1
Summary of Results of EPIC Searches on DoDD 5134.01, DoDD 5144.1, CJCSI 6212.01E, and DoDI 4630.8

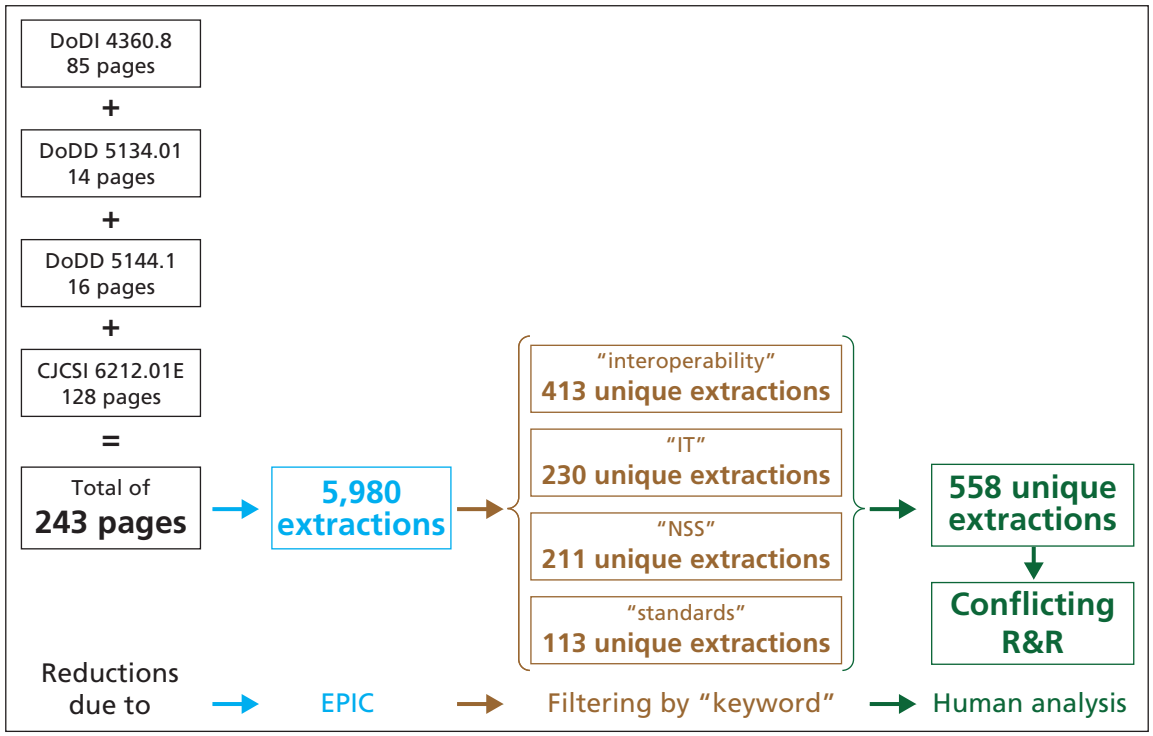
Policy	EPIC Extractions	Nonredundant Extractions
DoDD 5134.01	314	77
DoDD 5144.1	441	52
CJCSI 6212.01E	1,854	489
DoDI 4630.8	3,371	519
Combined total	5,980	1,137

Table 5.2
Results of First-Round Filtering by Keywords

Product Keyword Filter (Variants of Keyword Also Used)	EPIC Extractions	Nonredundant Extractions
IT	418	230
NSS	383	211
Interoperability	1,261	413
Standards	199	113
Combined filters	2,261	558[a]

[a] No overlaps.

Figure 5.1
Example of How EPIC Results Combined with Filtering Can Facilitate R&R Analysis



RAND *TR1277-5.1*

ASD(NII)/DoD CIO authorities as "including intelligence systems and architectures," citing Title 10 of the U.S. Code, Section 2223, derived from the Clinger-Cohen Act as the authoritative source. As the information architect, the ASD(NII)/DoD CIO appears to have broad and strong R&R over intelligence systems, architectures, and standards. However, DoDI 4630.8 and CJCSI 6212.01E assign intelligence standards R&R across the various DoD intelligence agencies (Defense Intelligence Agency [DIA], National Security Agency [NSA], and National Geospatial-Intelligence Agency [NGA]) and give DISA a clearly subsidiary role to assist and consult with the named intelligence agencies in standards development. Neither DoDI 4630.8

nor CJCSI 6212.01E assigns a specific role in IT and NSS standards to the ASD(NII)/DoD CIO.

Moreover, our review of DoDI 4630.08 found R&R that give the Under Secretary of Defense for Intelligence co-responsibility for intelligences systems interoperability and supportability with the ASD(NII)/DoD CIO, although DoDI 4630.08 does not include specifics about standards.

Filtering, then, allowed analysts to identify potential conflicts in the R&R assigned to the ASD(NII)/DoD CIO and the intelligence agencies (DIA, NSA, and NGA) regarding standards applicable to intelligence.

Identifying Areas of Potential Conflict Using Distribution Analysis

For this task, the team used the EPIC results and additional manual analysis on the four key documents to generate tables that show the distribution of IT and NSS interoperability and standards R&R. Table 5.3 shows that IT and NSS policy is shaped by both IT- and NSS-specific policy and general acquisition policy such that strong R&R are divided between two primary actors, the ASD(NII)/DoD CIO and the USD(AT&L). Other actors such as the White House Military Office, the J6, and agencies hold a single strong R&R each. It is a straightforward matter to check if the actors with single strong IT and NSS interoperability

Table 5.3
Distribution of Strong/Advisory R&R Statements by Actor and Policy

	IT- and NSS-Specific R&R Statements			General Acquisition R&R Statements
	Strong/Advisory			Strong/Advisory
	DoDD 5134.01	DoDD 5144.1	CJCSI 6212.01E	DoDD 5134.01
All OSD officials				0 / 1
ASD(NII)/DoD CIO		23 / 5		
USD(AT&L)	4 / 1	2 / 1		12 / 0
USD(C)				0 / 1
USD(P)				0 / 3
USD(P&R)		0 / 1		
General Counsel				0 / 1
Inspector General				0 / 1
Components, Services, and agencies			0 / 1	
Agencies				0 / 1
NSA			1 / 0	
Under Secretary of the Army			0 / 1	
J6			1 / 0	
White House Military Office		1 / 0		

and standards R&R have responsibilities that will conflict with each other or with the two primary players, the ASD(NII)/DoD CIO and the USD(AT&L). Our analysis found no areas of potential conflict.

A more complex undertaking is required to determine if the multiple strong R&R assigned to the USD(AT&L) and the ASD(NII)/DoD CIO potentially conflict. Our detailed analysis of EPIC results and subsequent examination of the policies in question revealed one area of conflicting R&R. Specifically, Section 3.7 of DoDD 5134.01 assigns USD(AT&L) policymaking responsibility to eliminate duplication of effort, which potentially conflicts with Section 3.3.17 of DoDD 5144.1, which assigns similar R&R to the ASD(NII)/DoD CIO, as shown in Figure 5.2.

We also generated an R&R distribution table that shows the distribution of IT and NSS interoperability and standards R&R by actor and type of R&R. Table 5.4 suggests two policy insights. First, the widely distributed nature of R&R related to intelligence standards as discussed above is again evident. Second, the strong R&R for information assurance are evenly distributed among three major actors—DISA, NSA, and DoD CIO.[1] Additionally, that distribution of authorities comes from different policy issuances. CJCSI 6212.01E assigns shared IA standards roles between DISA and NSA, and DoDD 5144.1 assigns IA standards roles to DoD CIO, as follows:

- Enclosure C of CJCSI 6212.01E —
  - Section 6p: DISA will "in coordination with NSA, review and define IA standards."
  - Section 8g: DIRNSA/C, CSS [Director National Security Agency, Central Security Service] will "in cooperation with the DISA, identify, evaluate, and select IA and related standards for inclusion in the DISR [DoD Information Standards and Profile Registry]."

Figure 5.2
Conflicting R&R in DoDD 5134.01 and DoDD 5144.1

[1] Currently, a single individual is the ASD(NII) and DoD CIO. However, federal law and policy often assigns R&R to only the ASD(NII) or only to the DoD CIO. This practice allows the law and policies to remain current if different individuals are ASD(NII) and DoD CIO. The recent direction by the Secretary of Defense to eliminate the office of the ASD(NII) and transfer the DoD CIO duties to DISA means that the R&R assigned by law or policy to the DoD CIO will automatically transfer to DISA, the new DoD CIO. Those R&R that are assigned solely to the ASD(NII) will require separate direction to transfer to parties as deemed appropriate by the Secretary of Defense.

Table 5.4
Distribution of Standards and Interoperability Roles and Responsibilities

		Intelligence Standards R&R Statements				Other Standards R&R Statements					Interoperability and Supportability R&R Statements		
		Strong/Advisory				Strong/Advisory					Strong/Advisory		
		SIGINT	GEOINT	HUMINT	MASINT	DISR	IA	International	C3	Organization-Unique	Joint	Special Operations	Cryptography
CJCSI 6212.01E	DISA	0 / 1	0 / 1			3 / 0	1 / 1				0 / 1		
	NSA	2 / 0					1 / 1						1 / 0
	NGA		4 / 0		0 / 1								
	DIA			1 / 0	2 / 0								
	Combatant commands										2 / 0		
	USSOCOM											1 / 0	
	USSTRATCOM						0 / 1						
	USD(AT&L) Defense Standardization Office					0 / 1				0 / 1			
	Components and Services			0 / 1									
DoDD 5144.1	DoD CIO						1 / 0	1 / 0	1 / 0				

- Section 3.3.7 of DoDD 5144.1 —
  - As the DoD CIO "develop and maintain the DoD IA program and associated policies, procedures, and standards required by section 2224 of reference (a),[2] chapter 35 of reference (e)[3] and DoD Directive S-3600.1 (reference (l)[4])."

The text passages above suggest that IA standards is an area where potential conflicts can occur as the DoD CIO attempts to develop and maintain the DoD IA program and associated policies, procedures, and standards, while the NSA and DISA attempt to execute their duties to review, defined, identify, evaluate, and select IA and related standards. At a minimum, the executives from NSA, DISA, and DoD CIO must coordinate closely with each other to avoid conflicts when exercising their decisionmaking authorities. Hence, whether actual conflicts occur depends on the specific implementation of these elements of interoperability policy. Investigating the specific implementation is beyond the scope of this study.

Exploration of Interoperability Policy Using Mapping

The last task in this case study was a classical textual policy analysis that leveraged EPIC results to rapidly identify relevant R&R distributed throughout hundreds of pages of policy. The objective was to analyze how policy directs the generation of interoperability requirements, testing, and reviews for programs, seeking to identify conflicts, gaps, ambiguities, and uncertainties. Table 5.2 shows that the EPIC scans of all four policies, DoDD 5134,01, DoDD 5144.1, CJCSI 6212.01E, and DoDI 4630.8, produced 413 nonredundant extractions relating to interoperability. The analyst reviewed those statements and developed a top-level map of interoperability requirements, which is shown in Table 5.5. The map of extracted interoperability requirements exposes potential conflicts or gaps in policy. With mapping-facilitated analysis, issues are identified and the analyst drills down into the original policy figures and language as needed.

Table 5.6 highlights some of the issues identified relating to policy on program interoperability. Perhaps the most important insight evident in the maps is a weak linkage between the development of interoperability standards/architectures and determining interoperability requirements. The lack of a bridge between creating and using architecture and standards makes the link weak. That is, the ASD(NII)/DoD CIO is charged with creating policy, guidance, and architectures and is responsible for ensuring that these are compliant with other policies, but guidance on what constitutes compliance is absent.[5] The disconnect on intelligence standards was discussed earlier. Side-by-side comparison of EPIC extractions highlighted differences between the two versions of the Net-Ready Key Performance Parameter (NR-KPP) in newer CJCSI 6212.01E and the older DoDI 4630.8.

---

[2] Reference (a) is Title 10 of the U.S. Code.

[3] Reference (e) is *E-Government Act of 2002*, Public Law 107-347, December 17, 2002.

[4] DoDD S-3600.1 was canceled in October 2001 by DoDD 3600.1.

[5] Emerging guidance such as the DoD Information Enterprise Architecture (IEA), currently in development, is poised to address these issues.

Table 5.5
Map of Major Responsibilities for Program Interoperability

Policies/Standards/Architectures	Program/System Requirements	Interoperability Testing	Program/System/Reviews
ASD(NII)/DoD CIO Policies, guidance, and architecture for all DoD communications and IT programs/initiatives Facilitate/resolve issues for interfaces, security, standards, and protocols critical to end-to-end GIG operation **NSA with DISA** Tactical SIGINT architectures and standards **NGA with DISA, DIA** GEOINT standards (NSG) **DIA with DISA, NGA** MASINT standards HUMINT standards (DISA only)	**ASD(NII)/DoD CIO** *Net-Ready KPP, 6212.01E* architectures compliant with DoD IEA (14–16 views); comply with net-centric data and services strategies (except tactical and non-IP), GIG technical guidance, DoD IA requirements, and supportability requirements *NR KPP, 4630.8* comply with NCOW-RM, GIG key interface profiles, DoD IA requirements; include nine DoDAF 1.0 views **DoD Components** Provide an ISP for all IT/NSS acquisitions, even if non-ACAT (except some waivers); ISP includes documentation/compliance with NR-KPP NR-KPP in CDD and CPD	**DISA/JITC** Review T&E plans Lead and conduct interoperability testing Certify interoperability from test results (either JITC or C/S/A alternates) **C/S/A (Sponsoring)** Ensure program TEMPs include interoperability requirements (from NR-KPP) Planning and budgeting for interoperability testing Interoperability T&E criteria and plans Conduct interoperability tests (can leverage JFCOM and Army events)	**Joint Staff** Certifies interoperability (as part of I&S certifications) in JCIDS reviews Reviewers called out include COCOMs, JFCOM, USSTRATCOM (ISR, space operations, global strike), Air Force (space) **ASD(NII)/DoD CIO** Reviews ACAT I, IA, and special interest ISPs **C/S/A (Sponsoring)** Ensures required documentation (architecture view, etc.) is properly prepared before submittal

Table 5.6
Issues Raised by a Map of Interoperability-Related R&R Generated from EPIC Extractions

Lack of a bridge between creating and using architectures and standards

Differing versions of NR-KPP

Policies/Standards/Architectures	Program/System Requirements	Interoperability Testing	Program/System/Reviews
ASD(NII)/DoD CIO Policies, guidance, and architecture for all DoD communications and IT programs/initiatives Facilitate/resolve issues for interfaces, security, standards, and protocols critical to end-to-end GIG operation **NSA with DISA** Tactical SIGINT architectures and standards **NGA with DISA, DIA** GEOINT standards (NSG) **DIA with DISA, NGA** MASINT standards HUMINT standards (DISA only)	**ASD(NII)/DoD CIO** *Net-Ready KPP, 6212.01E* architectures compliant with DoD IEA (14–16 views); comply with net-centric data and services strategies (except tactical and non-IP), GIG technical guidance, DoD IA requirements, and supportability requirements *NR KPP, 4630.8* comply with NCOW-RM, GIG key interface profiles, DoD IA requirements; include nine DoDAF 1.0 views **DoD Components** Provide an ISP for all IT/NSS acquisitions, even if non-ACAT (except some waivers); ISP includes documentation/compliance with NR-KPP NR-KPP in CDD and CPD	**DISA/JITC** Review T&E plans Lead and conduct interoperability testing Certify interoperability from test results (either JITC or C/S/A alternates) **C/S/A (Sponsoring)** Ensure program TEMPs include interoperability requirements (from NR-KPP) Planning and budgeting for interoperability testing Interoperability T&E criteria and plans Conduct interoperability tests (can leverage JFCOM and Army events)	**Joint Staff** Certifies interoperability (as part of I&S certifications) in JCIDS reviews Reviewers called out include COCOMs, JFCOM, USSTRATCOM (ISR, space operations, global strike), Air Force (space) **ASD(NII)/DoD CIO** Reviews ACAT I, IA, and special interest ISPs **C/S/A (Sponsoring)** Ensures required documentation (architecture view, etc.) is properly prepared before submittal

Conflict over intelligence architectures (noted earlier)

NR-KPP interpretation across documents creates ambiguities

Minimal guidance in policy is given on how to determine interoperability requirements for NR-KPP including how to select elements of the DoD IEA or other architectures relevant to the program, how to select data models or military standards, or whom to consult when determining interoperability requirements. One clear exception is DoDI 4630.8, which advises that a Working Integrated Project Team of subject matter experts should prepare the ISP and should invite PMs of interfacing systems to attend (DoDI 4630.8, Section E4.4.1.1). This is in contrast to a great deal of policy focusing on reviews of the NR-KPP after it has been prepared.

Finally, the fact that the NR-KPP in CJCSI 6212.01E and DoDI 4630.8 are out of synchronization is clearly evident in Tables 5.6 and 5.7. Out of synchronization means that CJCSI 6212.01E is a much newer policy issued in 2008, whereas DoDI 4630.8 was issued in 2004, and, hence, some of the differences noted in Table 5.7 may be due to the fact that DoDI 4630.8 has not yet been updated to be consistent with newer policy. For example, as shown in Table 5.7, DoDI 4630.8 does not require that a program have an integrated dictionary (AV-2) or a concept graphic (OV-1). However, the newer CJCSI 6212.01E does require these two products. The reason these two products are included in the newer guidance but not in the older guidance might be because these two products were not deemed necessary or useful in 2004 when DoDI 4630.8 was issued but were considered necessary and useful in 2008 when CJCSI 6212.01E was issued. Table 5.7 shows that lack of synchronization among related policies can be the root of some potential R&R conflicts. For example, those charged with responsibilities related to compliance with GIG technical guidance may encounter some who cite required compliance with key interface profiles as directed by the older DoDI 4630.8. Both parties would be correct in the sense that compliance with both can be traced to current policy, although the newer policy would appear to have precedence in this case.

Summary of Interoperability and Standards Case Study Findings

The interoperability and standards case study demonstrates that analysts can apply a variety of analysis methods to EPIC output to identify gaps, overlaps, and areas of potential conflict in R&R related to interoperability and standards. The primary findings of this case study are as follows:

- DoDD 5144.1 assigns strong R&R for intelligence standards to the DoD CIO, whereas DoDI 4630.8 and CJCSI 6212.01E assign similarly strong R&R for intelligence standards to NSA, DIA, and NGA with no role for the DoD CIO. These apparently overlapping assignments of R&R can lead to conflicts as the various officials execute their duties.
- The strong R&R for IA are evenly distributed among three major actors—DISA, NGA, and DoD CIO, creating a potential for conflicts to arise when these actors execute their assigned responsibilities.
- Defense policy contains only weak links between the development of interoperability standards/architectures and the determination of interoperability requirements.
- NR-KPP requirements are out of synchronization in defense policy.

Table 5.7
Lack of Policy Synchronization for NR-KPP Requirements in DoDI 4630.8 and CJCSI 6212E

NR-KPP Requirement	DoDI 4630.8 (30 Jun 2004)	CJCSI 6212.01E (15 Dec 2008)
DoDAF Products (Using V 2.0 Names)		
AV-1, Overview and Summary	Y	Y (must be in DARS)
AV-2, Integrated Dictionary		Y
OV-1, Concept Graphic		Y
OV-2, Op Resource Flow Description	Y	Y
OV-3, Op Resource Flow Matrix		Y*
OV-4, Org Relationships Chart	Y	Y
OV-5, Op Activity Model (Now 5B)	Y	Y*
OV-6C, Event-Trace Description	Y	Y*
OV-7, Logical Data Model (Now Div-2)		Y (Milestone C only)
SV-1, Sys Interface Description		Y
SV-2, Sys Resource Flow Description		Y
SV-4, Sys Functionality Description	Y	Y*
SV-5, Op Activity to Sys Function Matrix	Y	Y*
SV-6, Sys Resource Flow Matrix	Y	Y*
SV-11, Physical Data Model (Now Div-3)		Y (Milestone C only)
TV-1, Standards Profile (Now Stdv-1)	Y	Y (via DISR; must be posted)[a]
TV-2, Standards Forecast (Now Stdv-2)		Y (via DISR; must be posted)
DoD-Wide Architecture Compliance	NCOW-RM	DoD Enterprise Info Architecture
GIG Standards Compliance	Key Interface Profiles	GIG Technical Guidance
IA Compliance	Y	Y
Net-Centric Data and Services Strategies Compliance		Y—described in Data/Service Exposure Sheets*
Supportability Compliance Declarations		Y—spectrum, JTRS, SAASM, TDL compliance, bandwidth analysis

[a] Products that the Joint Staff assesses to set NR-KPP "threshold Value" (CJCSI 6212.01E).

CHAPTER SIX

The Information Assurance Case Study

Purpose

The information assurance case study looks at the roles and responsibilities of four specific groups of individuals—program managers, information assurance managers (IAMs), designated approving authorities (DAAs), and security managers (SM). This case study identifies relevant policy statements connected to these four sets of actors to identify potential inconsistencies or conflicts.

Approach

We used EPIC searches to facilitate the identification of R&R relevant to IA. To improve the probability of extracting all relevant statements in a collection of IA-related guidance, the search criteria were designed to include all statements mentioning at least one of the four actors listed above and any action terms, or one of the four actors and any product. Hence, the EPIC search criteria specified the above four groups of actors, all actions, and all products to conduct Actor and Action and Actor and Product searches.

The current collection of DoD issuances related to IA consist of 12 DoD directives and DoD instructions that were issued over a five-year period. The most recent issuance was in April 2008 (i.e., DoDI 8523.01 "Communications Security (COMSEC)") and the oldest was published in February 2003 (i.e., DoDI 8500.2 "Information Assurance (IA) Implementation"). During this time period, numerous roles and responsibilities have been created and assigned. This case study demonstrates the utility of EPIC in helping to identify potential conflicts or inconsistencies among the roles and responsibilities assigned to a set of key individuals involved with implementing and managing IA.

To analyze the results, a method known as *entity relationship* (ER) *diagramming* was used on the EPIC output to identify possible conflicts or inconsistencies among the four different actors. The concepts underlying ER diagrams have been discussed in the literature for many years, dating back to before the 1970s.[1] Since its inception, ER diagramming has been used in computer-assisted software engineering and database design, as well as in other computer

[1] Peter Chen, "The Entity-Relationship Model—Toward a Unified View of Data," *ACM Transactions on Database Systems*, Vol. 1, 1976, pp. 9–36.

science–related fields.[2] ER diagramming produces a semantic data map that can be evaluated for inconsistencies.[3]

This case study will show how ER diagrams can be used to identify potential areas of conflict in the R&R within a single policy as well as across multiple policies.

The EPIC Search

Table 6.1 shows that the total number of raw extractions from the EPIC search in the second column from the left, entitled "EPIC Extractions." The process of reviewing and refining the raw results to arrive at the final number of R&R statements involved three steps.

The first step removed redundant extractions. As described in Chapter Three, EPIC will mark and extract the sentence every time it finds one of the four defined actors and any of the actions or products in the same sentence or phrase. For example, a sentence that includes one actor, two recognized actions, and one recognized product would result in three raw extractions of the same sentence. As with the other case studies, identifying and removing redundant statements is a relatively straightforward process.

The second step involved identifying limited extractions and adding any missed statements from the original document pointed to by the limited extractions as well as deleting false positive extractions. As demonstrated in the PM case study, accounting for limited extractions can result in some documents having more final R&R statements than the original number of EPIC extractions. For this IA case study, the results for DoDI 8551.01 portray this condition in Table 6.1. The original EPIC scan returned only three extracted statements, but on reviewing the spreadsheet, it became clear that certain statements were missed and the final number of R&R statements identified increased to six. No false positive extractions were found.

The final step involved checking to make sure that the spreadsheet had identified the proper actor. Each actor has an ontology of related terms by which the actor may be identified. For example, "DoD CIO" can also be referred to as "the Department of Defense CIO," "the DoD Chief Information Officer," etc. Similarly, to avoid missing key actors, certain terms include very generic terms in their ontology. For example, the term "manager" may be used to refer to either a "program manager" or an "information assurance manager." Therefore, it is necessary to review and correct any instances where an extracted statement incorrectly labeled the actor.

The six columns on the right of Table 6.1 include the total number of R&R statements after the refinements described above, as well as the number of R&R statements attributed to each actor, and a column titled "other." "Other" includes statements that meet the search criteria (i.e., it includes at least one of the four actors, plus any action or product) but that assign responsibility to an actor other than the four identified. An example of such a statement is the following from DoDD 8570.01: "5.2. The Director, Defense Information Systems Agency (DISA) shall provide: . . . 5.2.3. Baseline IA training, certification, and tracking program for

---

[2] Peter Chen, "Entity-Relationship Modeling: Historical Events, Future Trends, and Lessons Learned," in Manfred Broy and Ernst Denert, eds., *Software Pioneers: Contributions to Software Engineering,* Berlin and Heidelberg: Springer-Verlag, 2002, pp. 297–310.

[3] A review of ER literature can be found in Ingo Feinerer, *A Formal Treatment of UML Class Diagrams as an Efficient Method for Configuration Management,* Vienna, Austria: Vienna University of Technology, 2007.

Table 6.1
Results from EPIC Searches on 8500-Series Defense Policy Issuances on IA

Issuances	EPIC Extractions (IAM, PM, SM, DAA)	R&R Statements					
		Total	AM	PM	SM	DAA	Other[a]
DoDD 8500.1E Information Assurance	9	1				1	
DoDI 8500.2 1A	191	25	12			6	7
DoDI 8510.01 DIACAP	239	36	11	11		10	4
DoDI 8520.02 PKI and PKE	19	18		14			4
DoDD 8521.02E DoD Biometrics	4	1		1			
DoDI 8523.01 COMSEC	9	12		12			
DoDI 8551.01 Ports, Protocols, and Services Management	3	6				4	2
DoDI 8552.01 Use of Mobile Code Technologies in DoD Information Systems	6	1[a]			1[a]		
DoDD 8560.01 COMSEC Monitoring and IA Readiness Testing	11	0					
DoDD 8570.01 IA Training, Certification, and Workforce Management	65	9					9
DoDI 8580.1 IA in the Defense Acquisition System	90	10	9				1
DoDI 8581.1 IA Policy for Space Systems	63	10		1		1	8

[a] Security manager for this R&R is not IA-related.

Designated Approving Authorities (DAA)." This statement assigns responsibility to the director of DISA to provide IA training, certification, and tracking programs for the DAA but does not assign any specific R&R to the DAA. Hence, the DAA is being provided with IA capabilities, but the policies do not include an R&R that directs the DAA to use them. These statements were kept and included in the final analysis because of their potential effect on the four actors of interest.

It is also interesting to note that terminology across policy documents may vary. The term "security manager" was included among the list of actors because, according to Enclosure 2 in DoDI 8500.2 "Information Assurance (IA) Implementation" (February 6, 2003, p. 20), the term "Information Assurance Manager . . . may be used interchangeably with the IA title Information Systems Security Manager (ISSM)." Therefore, the actor "security manager" was added as its own term to see if it would reveal separate R&R that would conflict with those for IAMs. However, the results of the EPIC search revealed that other than the definition in Enclosure 2 of DoDI 8500.2, the only other use of the term "security manager" was in DoDI

8552.01 "Use of Mobile Code Technologies in DoD Information Systems," shown in Table 6.1. Analysis of the statement extracted from the document indicated that the term was referring to a piece of software code called a "security manager" and not to an individual or office with IA R&R.

Entity Relationship Diagrams

An approach to analyzing the final R&R statements resulting from the EPIC search and the refinement steps described above is to read all of the statements and then try to link or identify possible inconsistencies or conflicts. However, even after reviewing and cleaning up the raw extracted statements, the final refined database contained a total of 128 separate R&R statements spread across 12 policy documents. Such a situation is amenable to ER diagramming, which also offers a visual display of how the R&R may be interrelated.

ER diagramming offers a systematic method for defining relationships between specific entities. For each of the policies listed, each R&R statement was reviewed to identify the specific entity or entities contained therein (which were typically actors or products) and the relationship between the entities (which were typically the actions the actors are directed to take). Examples of the ER diagrams constructed for some of the policies will be provided in the following paragraphs.

Figures 6.1 and 6.2 illustrate two examples of potential conflicts and how they may appear using ER diagrams. The first example, in Figure 6.1, shows two different actors. Actor

Figure 6.1
ER Diagram Showing Multiple Actors with Relationships to the Same Product

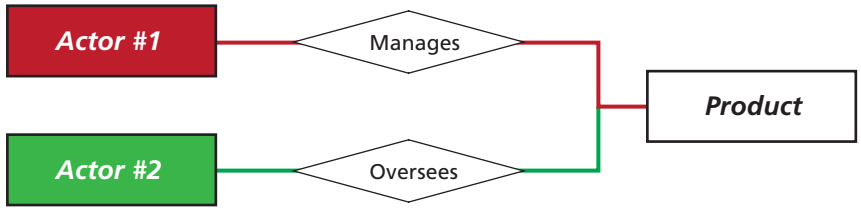
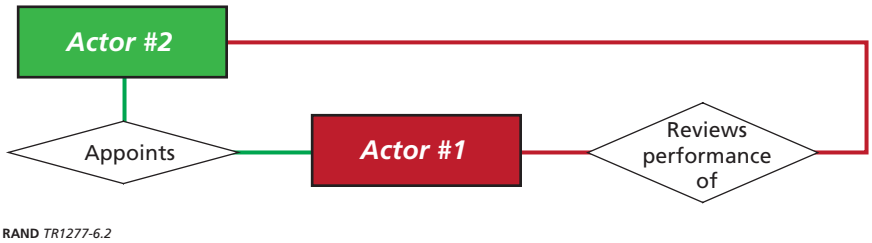


Figure 6.2
ER Diagram Showing Circular Relationships



#1 and Actor #2 both have a relationship with a particular product. Actor #1 *manages* the product, whereas Actor #2 *oversees* the product. Two different actors who have similar responsibilities for the same product could indicate a possible conflict or inconsistency regarding who is actually responsible or accountable. The second example shown in Figure 6.2 depicts a circular relationship. In this example, Actor #1 is responsible for *appointing* the person who is Actor #2. Indication of a possible conflict or inconsistency may occur if somehow Actor #2 has a relationship or responsibility for Actor #1. In Figure 6.2, Actor #2 *reviews the performance of* Actor #1. Hence, an ER diagram that has the form shown in Figure 6.2 could indicate a possible conflict or inconsistency.

ER diagrams were created for every policy document shown in Table 6.1 except for DoDI 8560.01.[4] The ER diagram for the policy with the most number of identified R&R statements, DoDI 8510.01 "DoD Information Assurance Certification and Accreditation Program (DIACAP)," is shown in Figures 6.3 and 6.4. The color-coding for the three actors (i.e., IAMs—blue, PMs—green, DAAs—red) shown in Figure 6.1 is also reflected in the ER diagram. Line colors represent the assignment of responsibility.

Using the rules we developed for identifying potential conflicts or inconsistencies, two examples in Figure 6.3 have more than one actor with responsibility for a given product. The first occurs at the top of the page, where both the DAA, and the certification authority (CA) are responsible for reviewing the DoD Information System (IS) statement produced by the IAM to determine the course of action with regard to Federal Information Security Management Act (FISMA). However, more than one entity (i.e., the CA and the DAA) reviewing a particular product (i.e., the IAM statement concerning FISMA) does not qualify as a conflict of roles or responsibilities because reviewing is an advisory action.

The second example is illustrated with the green lines and the entities the green lines connect in Figure 6.3. As with the first example discussed above, Figure 6.3 was generated by creating an ER diagram from the R&R statements in DoDI 8510.01. This second example has two different entities both with responsibilities regarding the "DoD IS statement required by FISMA." In this case, the PM is responsible for ensuring the annual review of the DoD IS statement as required by FISMA, and the IAM is responsible for providing the DoD IS statement that is then delivered to the CA and the DAA for review. As above, while there is more than one actor with a relationship to this product, it is not an indication of a potential conflict or inconsistency because only one R&R, that of ensuring, is a strong action.

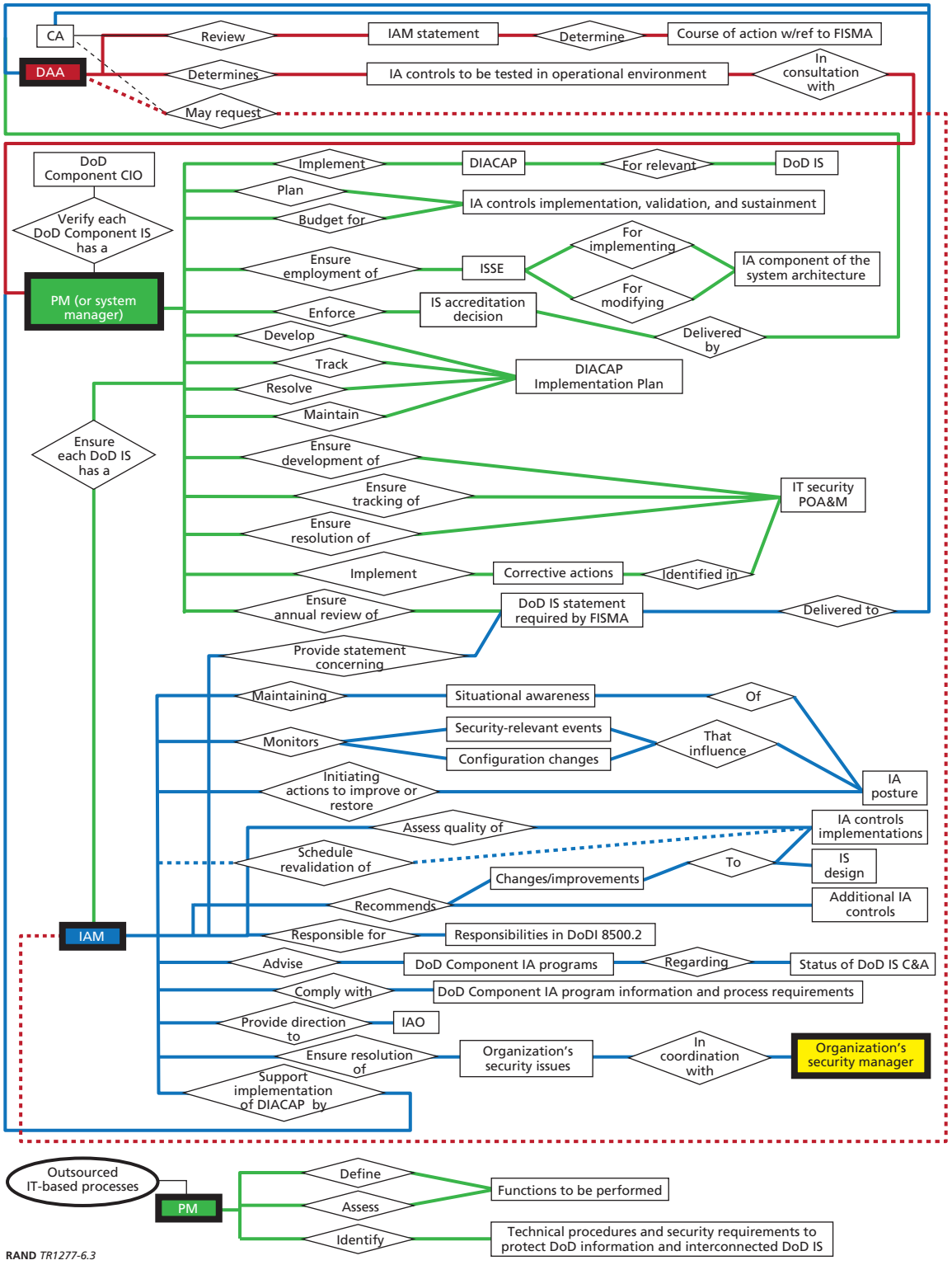
The dashed lines in Figure 6.3 are used to indicate a particular R&R for the IAM. Specifically, the DAA and CA may request (dashed red line) the IAM to schedule (dashed blue line) a revalidation of IA controls implementation for a particular system. However, The DAA and CAA's request does not apply to any of the other R&R defined for the IAM, shown on in Figure 6.3.

Finally, the roles and responsibilities for PMs identified in the main portion of Figure 6.3 apply to all PMs. However, additional specific roles and responsibilities also apply only to PMs for outsourced IT-based processes, and these additional R&R are shown at the bottom of Figure 6.3.

DoDI 8510.01 also contains the only other occurrence of the term "security manager" outside Enclosure 2 of DoDI 8500.2 and DoDI 8552.01. While it does not assign any respon-

[4] As shown in Table 6.1, after eliminating redundant statements and correcting misattribution of actors, there were no roles and responsibilities identified for the four actors of interest in DoDI 8560.01.

Figure 6.3
ER Diagram of DoDI 8510.01 Showing Potential Conflicts and Inconsistencies with IS Statements



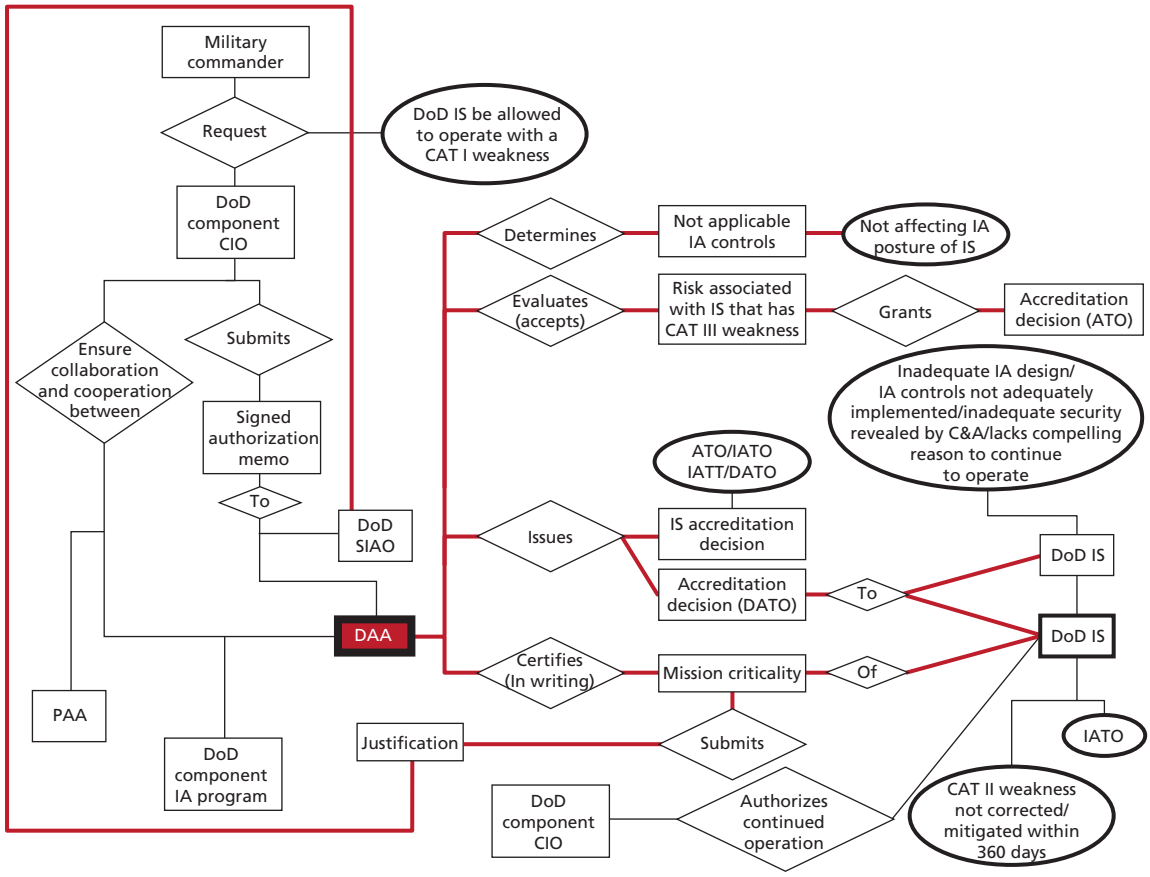
RAND *TR1277-6.3*

sibilities to the "security manager," it does state that the IAM is responsible for ensuring the resolution of any organization's security issues in coordination with that organization's "security manager."

Figure 6.4 presents an ER diagram for DoDI 8510.01 that focuses on the R&R for the DAA and highlights the number and complexity of the R&R contained in the document. Figure 6.4 also shows two different actors having responsibility for the same product. Specifically, in the lower right-hand corner, both the DAA and the DoD Component CIO have a relationship with DoD Information Systems that have an Interim Authorization to Operate (IATO) when a Category (CAT) II weakness is not corrected or mitigated within 360 days.

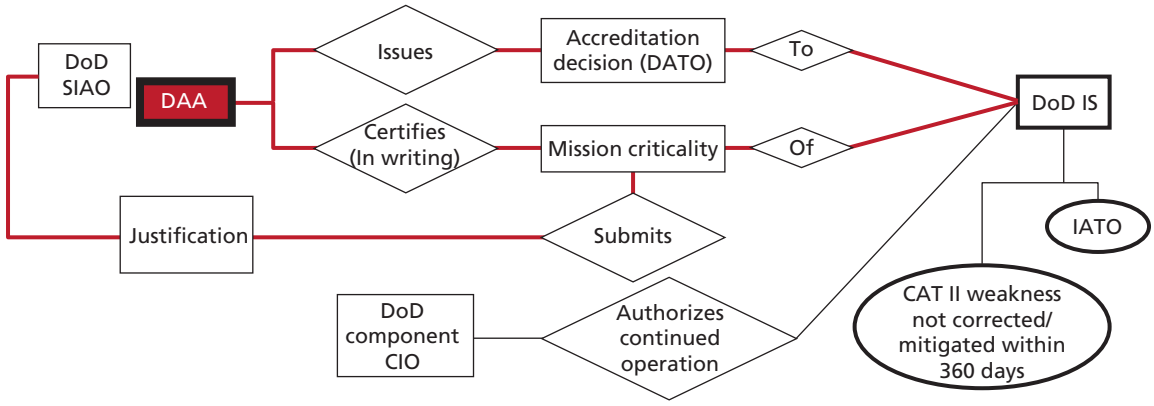
A portion of DoDI 8510.01 has been extracted and shown in Figure 6.5 for clarity. According to DoDI 8510.01, the DAA has the authority to issue a Denial of Authorization to Operate (DATO) to DoD IS with an IATO status and a CAT II weakness that has not been corrected or mitigated within 360 days. However, the same document states that the DoD component CIO can also authorize the continued operation of DoD IS with an IATO status and a CAT II weakness not corrected/mitigated within 360 days if it has in writing a letter of justification from the DAA that is transmitted to the DoD Senior Information Assurance Officer (SIAO). This indicates a possible conflict for R&R between the DAA and the DoD component

Figure 6.4
ER Diagram for DoDI 8510.01 Focusing on the R&R for the DAA



RAND *TR1277-6.4*

Figure 6.5
ER Extract Showing Possible Conflict in Determining Accreditation Status for Some DoD IS



RAND *TR1277-6.5*

CIO concerning who has the authority to continue operation of DoD IS that have an IATO and a CAT II weakness for more than 360 days.

As illustrated by the case shown in Figure 6.5, once ER diagrams have been constructed for all of the policy documents, it is possible to extract specific parts of the individual diagrams. The extracted parts can then be examined to make comparisons across policy documents.

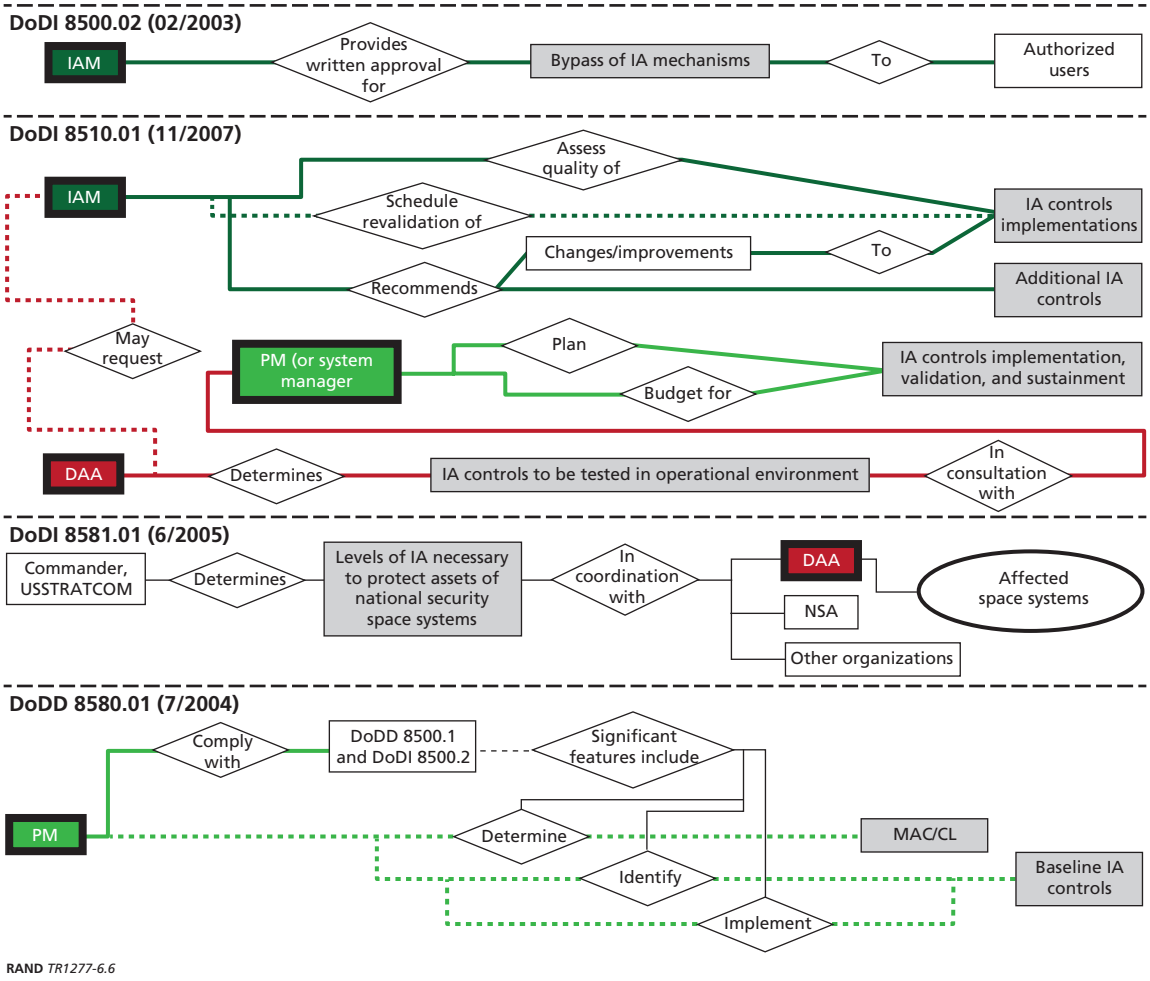
Figure 6.6 illustrates components of ER diagrams from DoDI 8500.02, DoDI 8510.01, DoDI 8581.01, and DoDD 8580.1 that are related to IA controls. Looking across the documents, several inconsistencies appear with respect to IA controls. In this case, the dotted lines are intended to represent an implied relationship. DoDD 8580.1 states that the PM is responsible for complying with the R&R outlined in DoDD 8500.1 and DoDI 8500.2. This document also states that significant features of compliance include determining Mission Assurance Category (MAC) and Confidentiality Levels (CL) as well as identifying and implementing baseline IA controls.

However, the ER diagram in Figure 6.6 shows that none of the responsibilities implied for compliance are contained in DoDI 8500.2. Nor are IA controls even mentioned with the any of the actors of interest in DoDD 8500.1. Hence, DoDD 8580.1 at least implies R&R for DoD PMs that are inconsistent or at least are not reflected in other DoD issuances.

Similarly, an examination of the ER diagrams of DoDI 8500.02 and DoDI 8510.01 indicates that the R&R for PMs and IAMs seem poorly defined. Specifically, according to DoDI 8510.01, the PM is responsible for planning and budgeting for the implementation, validation, and sustainment of IA controls. However, the IAM is responsible for assessing the quality and scheduling the revalidation of IA control implementations and can also recommend additional IA controls and recommend changes to existing IA control implementations. These statements indicate potential inconsistencies and conflicts between the PM and the IAM with regard to setting IA controls and their implementations.

Also, while in DoDI 8500.02 and DoDI 8510.01 the IAM and PM seem to have most of the responsibility with regard to setting and implementing IA controls, according to DoDI 8581.01, the commander of USSTRATCOM is responsible for determining the levels of IA necessary to protect the assets of national security space systems. These statements can also be

Figure 6.6
ER Diagrams of IA Controls Across DoD 8500-Series Policies



interpreted as appearing to set up a potential conflict between the commander of USSTRATCOM and program IAMs and PMs with regard to setting up appropriate IA controls.

Summary of Information Assurance Case Study Findings

Using the combination of EPIC, along with a modified version of ER diagramming, it was possible to quickly identify possible conflicts and inconsistencies for IAMs, PMs, DAAs, and security managers across the DoD 8500-series documents.

Several examples of possible inconsistencies are illustrated using this approach, including issues pertaining to the accreditation status of some DoD information systems (those with a CAT II weakness and a IATO status) and the setting and implementation of IA controls.

This same method also identified possible inconsistencies with regard to R&R for certification and accreditation across the DoD 8500-series issuances, as well as possible inconsistencies with regard to determining the applicability of DoDI 8581.1 for some space systems.

CHAPTER SEVEN

Closing Remarks and Recommendations

Study Products

We have developed an analytic technique consisting of a framework and methodology to efficiently analyze many defense policies to identify potential conflicts, gaps, and overlaps with respect to the roles and responsibilities that defense policies assign to DoD executives. This capability uses a new automated tool called EPIC, which can be supplemented by various analysis methods carried out by analysts. The flexibility and utility of EPIC has been demonstrated in the three case studies whose results are described in previous chapters. Aside from the potential conflicts discovered in the policy documents examined in the case studies, the framework, methodology, and EPIC are the primary products of this study. The framework provides the basis of the methodology, and EPIC automates one step of the methodology. Analysis of EPIC output is still required to identify gaps, overlaps, and areas of potential conflict in the R&R assigned to defense executives. As the case studies show, a variety of methods can be used to facilitate analysis of EPIC output to identify potential conflicts, inconsistencies, gaps, redundancies, and overlaps in a collection of policy documents.

Potential Next Steps

This study demonstrates the potential and promise of a new capability for policy analysis. The new capability should facilitate policy analyses suggested by DoD officials, such as the following:

- Investigate potential conflicts identified in the case studies. Detailed investigations into the potential conflicts identified in the case studies are required to determine whether actual conflicts exist and to recommend actions to correct policy if conflicts are found.
- Develop a process to identify the origins of R&R conflicts. This would involve developing a technique that would allow full-spectrum analysis of R&R from their origins in U.S. law, to DoD-level policy, and finally to Service-level implementation documents. Such research would help identify the root causes of R&R conflicts. Extending the automated policy format and processing capabilities of EPIC is a candidate approach.
- Use EPIC to review draft DoD and Navy policies. EPIC can help analysts determine if R&R in draft policy is internally consistent as well as consistent with the R&R found in existing policy.

The technique and tool developed in this study provide policymakers and reviewers with new capabilities for identifying gaps, overlaps, inconsistencies, and areas of potential conflict in policy. This can result in better and more consistent defense policy.

APPENDIX

EPIC

This appendix describes EPIC in detail and contains a user's guide on how to run the tool.

Finding and Preparing a Document for EPIC Searches

Using EPIC to analyze a document requires preparation of the document's file format, as well as thinking about the kind of analysis that will be performed. The analyst needs to specify the documents of interest. DoD databases for policy documents provide some metadata that allow the user to find relevant documents. In particular, the Department of Defense Issuances website allows the user to search and browse issuances by their subject and issuing authority.[1] In addition, the reference section of key documents will offer additional candidate documents on the topic of interest.

After downloading or otherwise acquiring a library of documents of potential interest, the user should read through each document on the list both to make sure that each document is worth cataloguing and to make a note of any key actors, actions, or products that might not be included in EPIC's list of keywords (see Tables 2.1, 2.2, and 2.3 for keyword lists in the current version of EPIC). While the actors, actions, and products of interest may be known in advance, the user should also note any new terms or new or atypical conventions for common terms. For example, the user should note if "program manager" is abbreviated in an unusual way, such as "prog. mngr." If the user identifies any terms not already included in EPIC's keyword lists, the user can add them later using the *Select and Scan* tab of the EPIC interface.[2]

EPIC requires that the policy document be in Rich Text Format (RTF) or MS Word document format. However, in some cases, a policy document may only be downloaded in Adobe's PDF. Various software tools can convert documents from PDF to RTF. In the course of our research, we found that the freeware utility "Some PDF to Word Converter" works well on policy documents.[3]

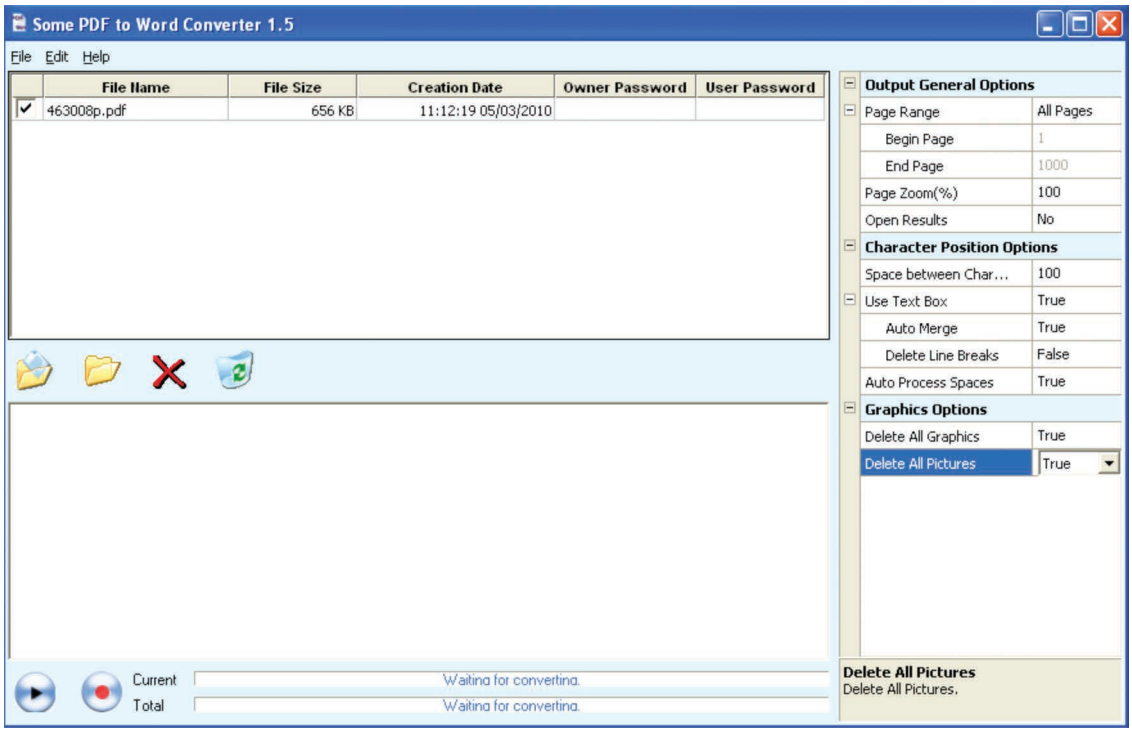
To use the Some PDF to Word Converter program to convert a PDF file of a policy document to RTF, the user first opens the program, which will open to the screenshot shown in Figure A.1. The user specifies the document to be converted to RTF by clicking on the icon of

[1] See the Department of Defense Issuances.

[2] The *Select and Scan* tab is explained below.

[3] The Some PDF to Word Converter freeware is available online. This utility gives the user the option of automatically deleting all graphics and pictures from the source PDF. This should be done to save the trouble of removing them manually later, because EPIC cannot read graphics or pictures.

Figure A.1
The Some PDF to Word Converter Interface



RAND *TR1277-A.1*

the paper-containing folder. This icon can be seen on the left side of the interface between the upper and lower white rectangles. To convert an entire directory of PDF documents, the user should click the icon of the plain folder. This icon is just to the right of the first. In either case, the user will be asked to browse to the input PDF files. An entry in the upper white rectangle will be created for every PDF the user selects. This entry will list file attributes, such as the name, size, and creation date.

Next, the user selects the desired output options by adjusting the settings in the table to the right of the two white rectangles (upper right-hand corner of the screenshot shown in Figure A.1). Most of the default settings can be left as is, but the user should change the *Delete All Graphics* and *Delete All Pictures* options to true because the current version of EPIC is not designed to scan graphics or pictures.

Finally, the user clicks the round button with the black triangle on it to begin the conversion. This button is at the far bottom left of the interface. During the conversion process, the interface screen will indicate progress via the progress bars at the bottom of the interface. When the process is complete, Windows will automatically open the new RTF file. The new RTF file is created in the same directory as the source file. The new RTF file is automatically saved in the same directory as the source file with the same name as the source file but with a different extension. For example, a source file named policydocument.pdf will be saved as policydocument.rtf.

Once the policy document is converted to a format readable by EPIC, the user should manually scan the RTF file before running EPIC. To expedite later analysis of EPIC output, the user should remove all parts of the RTF file that are known not to contain policy state-

ments. Typical sections of this kind include references, glossaries, releasability statements, any remaining graphical or tabular artifacts, and effective date.

Initiating AN EPIC Search

Launch EPIC

The user initiates a new search by opening the EPIC file. The Excel file will open to a worksheet named Launch. The user clicks the *Launch Policy Analysis Tool* button. A screenshot of the Launch worksheet is shown in Figure A.2.

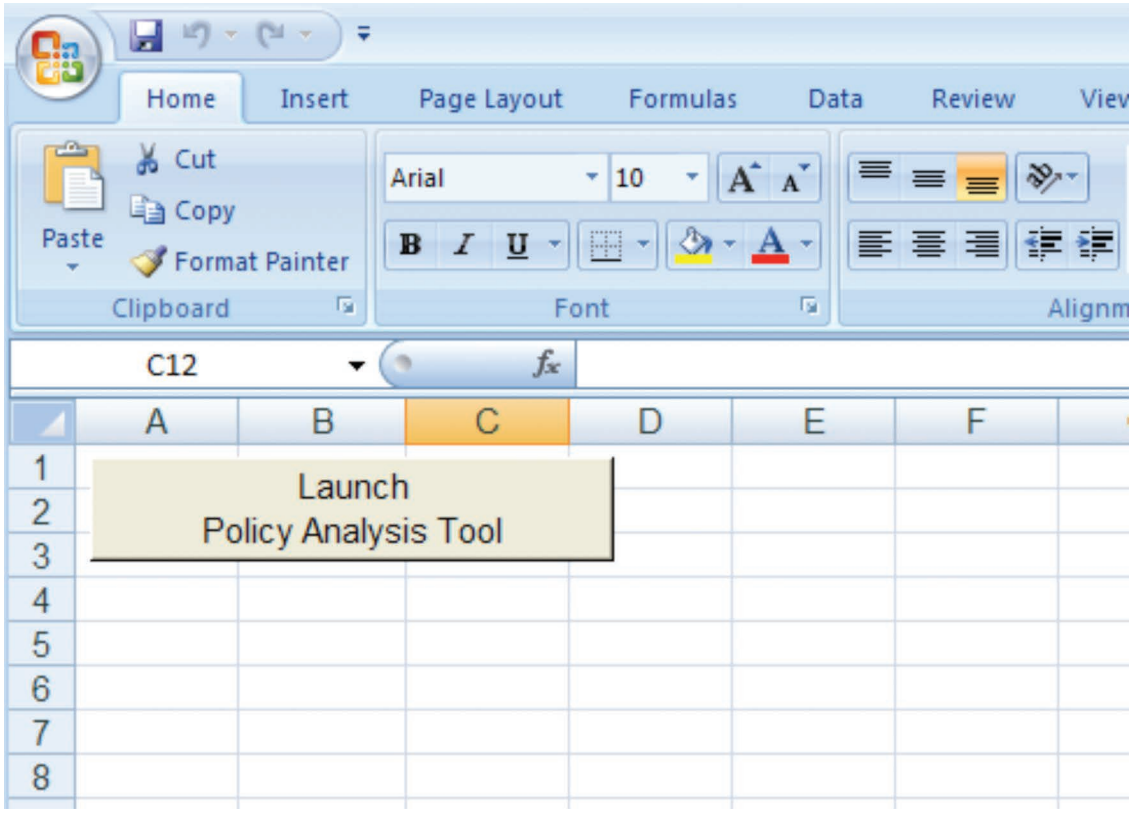
Specify Input Parameters

A small interface labeled "Policy Analysis Application" will appear with three tabs: *File Settings, Select and Scan,* and *Tag Controls*. These tabs control the parameters of the scan that the tool will perform. Figure A.3 shows a screenshot of this interface.

The *File Settings* Tab

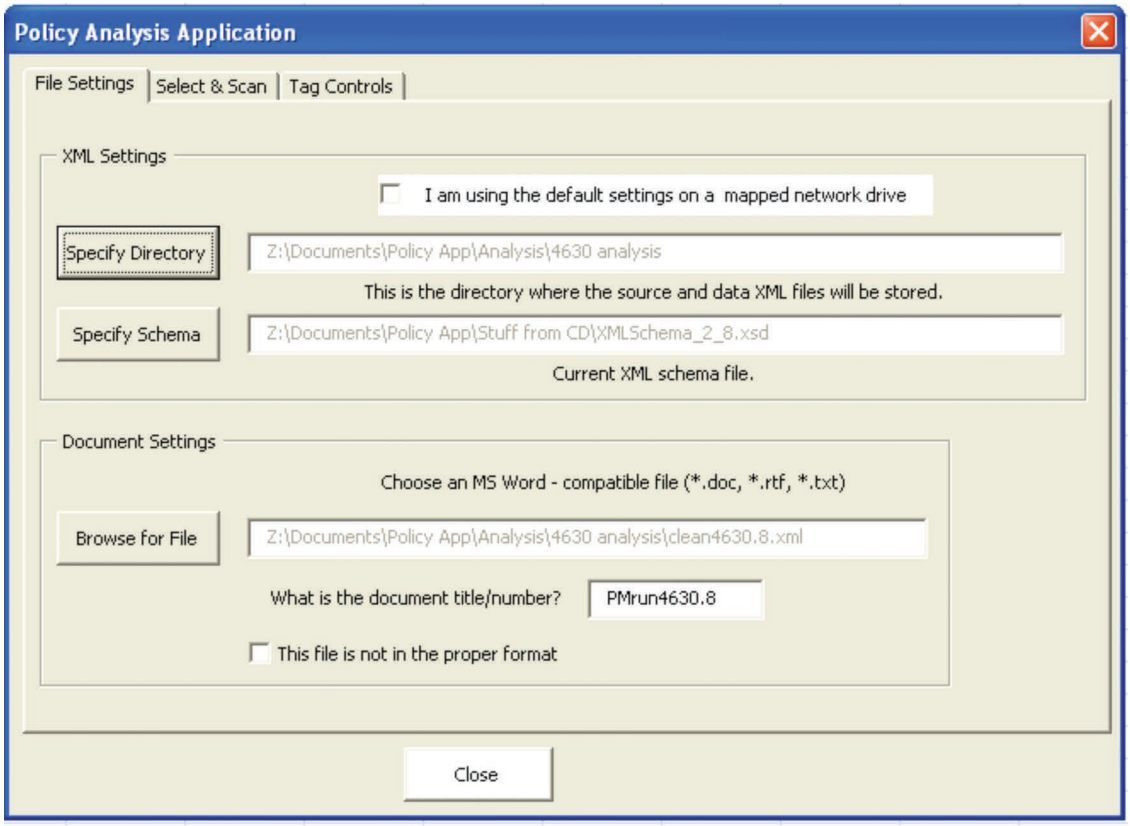
The *File Settings* tab has five key fields that define the input and output files for the scan. EPIC remembers the input and output file settings from the previous time it was run. The user

Figure A.2
The *Launch Policy Analysis Tool* Button



RAND *TR1277-A.2*

Figure A.3
Choosing Output Directory, XML Schema, Input File, and Output Filename



RAND *TR1277-A.3*

can select the directory where EPIC will place the output files from the scan. To do this, the user clicks the *Specify Directory* button and navigates to the desired folder.

The user may also choose the XML schema used by EPIC by clicking the *Specify Schema* button and navigating to the schema file. EPIC uses only one schema at this time, so in the current version of EPIC, the schema needs to be selected only when EPIC is being set up the first time. For this version of EPIC, the schema is the marked XML output file.

In the bottom half of the *File Settings* tab, the user may click the *Browse for File* button and navigate to the RTF file containing the policy document to be scanned. By default, EPIC keeps the input file the same as for the previous run.

Below the input file selection, the user must choose a unique name for the output files for the scan. This name will also become the name of the tab in the EPIC workbook where the results are displayed.

Finally, if the input file has not been preprocessed, the user must click the checkbox at the bottom of the *File Settings* tab before moving on to the *Select and Scan* tab. Clicking on this box labeled "This file is not in the proper format" will activate the EPIC preprocessor routine before beginning the EPIC search. The EPIC preprocessor routine is described below. The user will usually check this box the first time the document is being subject to a search by EPIC.

The *Select and Scan* Tab

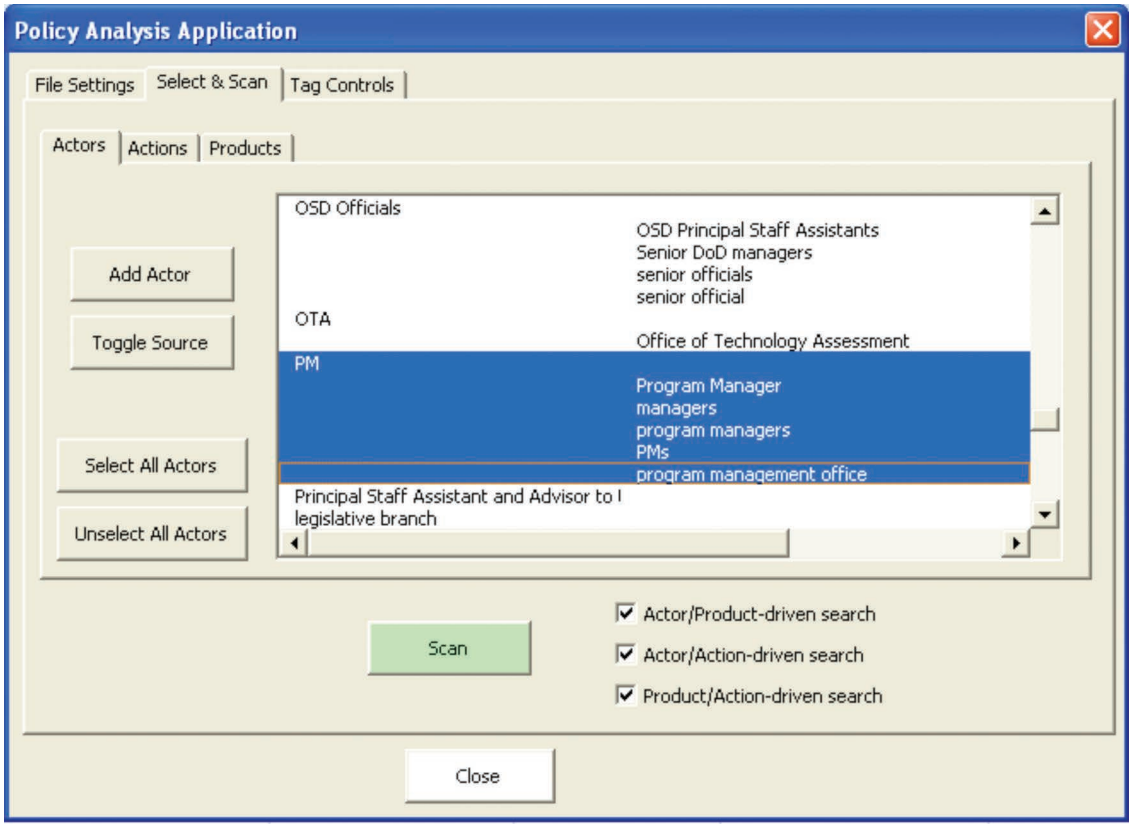
Once the appropriate input and output file settings have been chosen, the user should click on the *Select and Scan* tab. Figure A.4 shows a screenshot of this tab. This tab has three subtabs: one for actor keywords, one for action keywords, and one for product keywords. Each keyword subtab has a similar format.

Actors Subtab. Figure A.4 shows a screenshot of the *Actor* keyword subtab. To the right, a scrollable list of keywords appears. Keywords to the left side of the box are categories of keywords that include the words in the category to the right and below them. Thus, in Figure A.4, "PM" is a keyword category that includes the terms "program manager," "managers," "program managers," "PMs," and "program management office." When the user selects a subordinate keyword, EPIC automatically selects the parent category.

Four buttons appear on the left of the interface. The upper buttons shown in Figure A.4 are labeled *Add Actor* and *Toggle Source*. These buttons allow the user to bring up interfaces to edit the corresponding list of keywords.

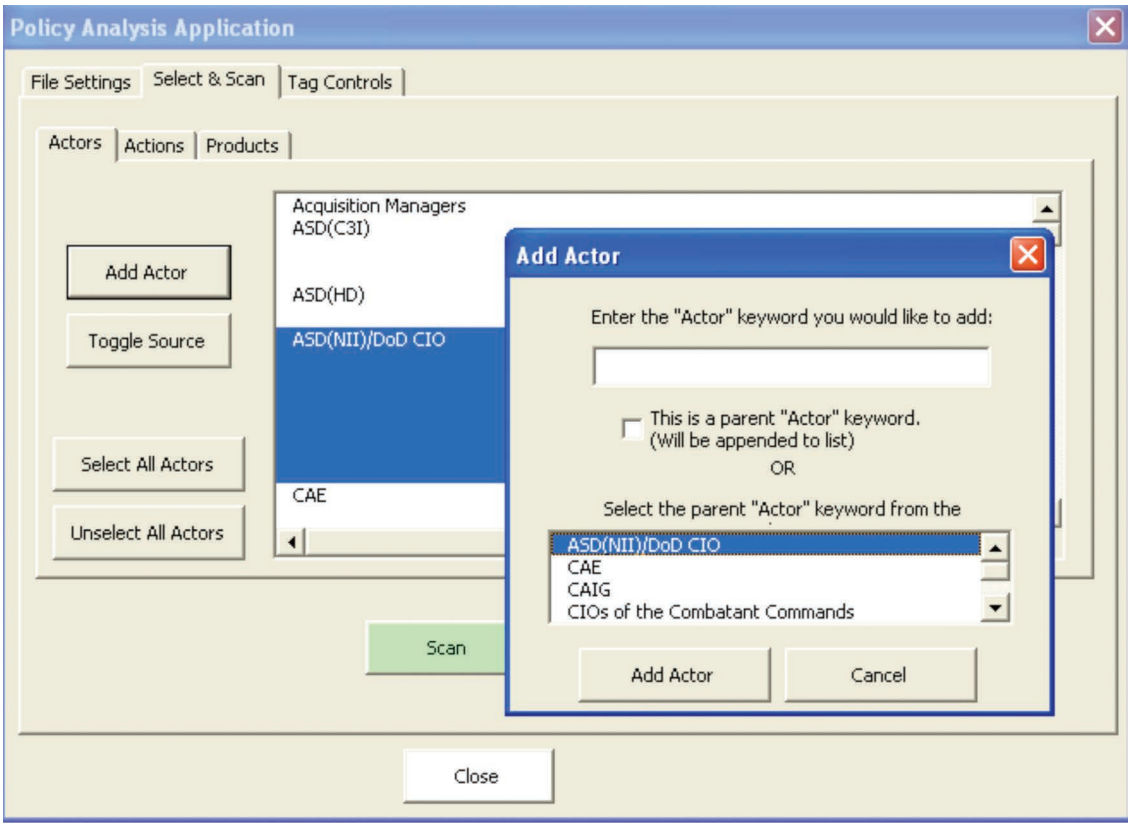
Clicking on the *Add Actor* button would allow the user to add actors such as the ones discovered during the user's initial examination of the document. To add an actor to the EPIC list, the user clicks the *Add Actor* button, which brings up a small interface for the user to type the new keyword and indicate whether this new keyword is another name for an actor already in the list or a new actor altogether. For instance, Figure A.5 shows a screenshot that allows

Figure A.4
Selecting Actor Keywords for Program Manager



RAND *TR1277-A.4*

Figure A.5
Adding an Additional Keyword to Describe the ASD(NII)/DoD CIO



RAND *TR1277-A.5*

the user to add a term for the actor ASD(NII)/DoD CIO. The "This is a parent "Actor/Action" keyword. (Will be appended to list)" checkbox should be checked when the new keyword being added belongs in its own category and is not subordinate to any of the previous categories of actors or actions.

The lower buttons in the *Select and Scan* tab, labeled *Select All Actors* and *Unselect All Actors,* allow the user to quickly select and unselect lists of keywords. These buttons allow the user to avoid the need to individually click on each line of the keyword list if all keywords on particular list are of interest.

The user selects the types of searches that will be run at the bottom of the *Select and Scan* tab. Using the selected keywords from the three categories, EPIC can perform up to three kinds of searches on a document: Actor and Action, Action and Product, and Actor and Product. In an Actor and Action search, EPIC identifies only sentences that contain at least one Actor and at least one Action. If only an Actor and Action search is selected, sentences with one or more Action keywords, but no Actor keywords, would not be selected. The user selects an Actor and Action search by checking the box labeled *Actor/Action-driven search*.

Selecting the Action and Product search will return sentences and phrases that specify an Action and a Product but not necessarily an Actor. The user selects an Action and Product search by checking the box labeled *Action/Product-driven search*.

Similarly, the actor and product search looks for sentences with both an actor and a product. The user selects an actor and product search by checking the box labeled *Actor/Product-driven search*.

The user can select one, two, or all three searches to identify all sentences with any combination of actor, action, and product keywords.

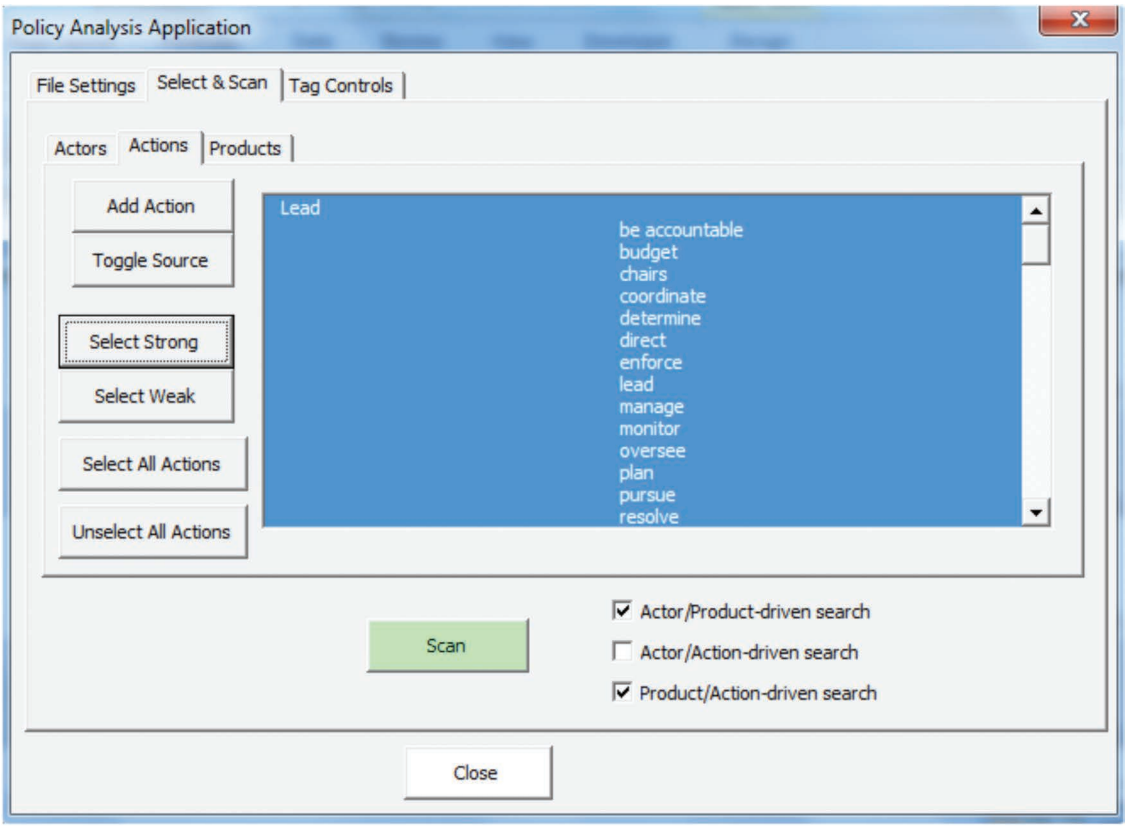
Finally, when the user has finished selecting all actor, action, and product keywords as well as the search types, clicking the *Scan* button will launch the EPIC scan and generate the output.

If the user clicks on the button labeled *Close* at the bottom of the screen, EPIC will exit the interface without any further action. Any EPIC scan that has already been performed will be unaffected, but no additional changes will occur.

Actions Subtab. Figure A.6 shows a screenshot of the *Actions* keyword subtab. This subtab contains two buttons that do not appear on the actor keyword subtab. These two buttons are on the left-hand side of the screen and are labeled *Select Strong* and *Select Weak*. The *Select Strong* button allows the user to select all strong action verbs. The *Select Weak* button allows the user to select all advisory action verbs. All of the other buttons on the *Actions* keyword subtab function as described above for the *Actor* keyword subtab.

Products Subtab. The buttons in the *Products* subtab work the same way the buttons on the *Actors* subtabs work. If new top-level product keyword categories are needed, they must be

Figure A.6
***Actions* Keyword Subtab**



RAND *TR1277-A.6*

added manually to the worksheet of keywords; this worksheet can be revealed by clicking the *Toggle Source* button of the *Products* subtab. This option is also useful for removing unneeded keywords or making extensive changes to the organization of the keyword list.

The *Tag Controls* Tab

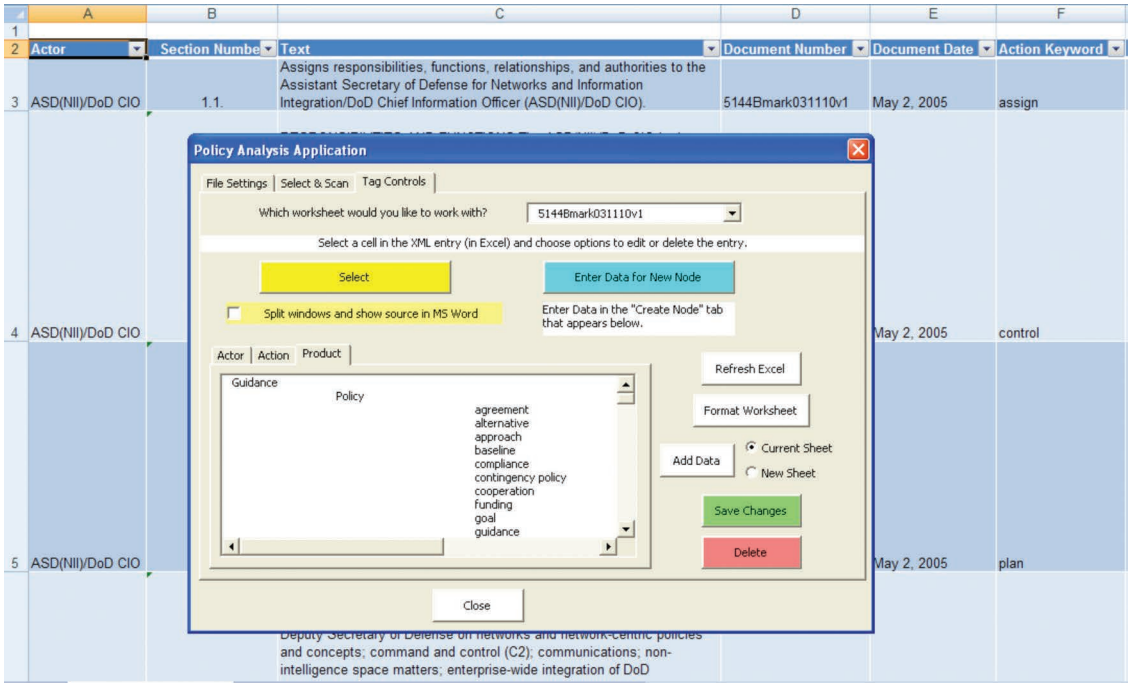
The *Tag Controls* tab (Figure A.4) allows the user to select a previously scanned document and simultaneously examine the Excel and Word version of search results. The user will be able to use the *Tag Controls* tab to "manually" add new search hits to both output files. *Tag Controls* keeps both versions of the results consistent with one another. Figure A.7 shows the *Tag Controls* interface.

When the user selects a previous scan from the dropdown menu, EPIC switches to the corresponding worksheet in Excel and loads the Word version of the results in the background. By selecting the *Split windows and show source in MS Word* checkbox, the user can also view the results worksheet and the Word document results side by side. Figure A.8 shows an example of the side-by-side display.

With the two results sets open, the *Tag Controls* tab then allows the user to perform three types of functions: First, the user can create new XML nodes to flag policy statements that the search did not find. These results might have been missed because they do not actually contain any search terms, for example. The new search result will appear in both the Word and Excel results when this document is accessed in the future.

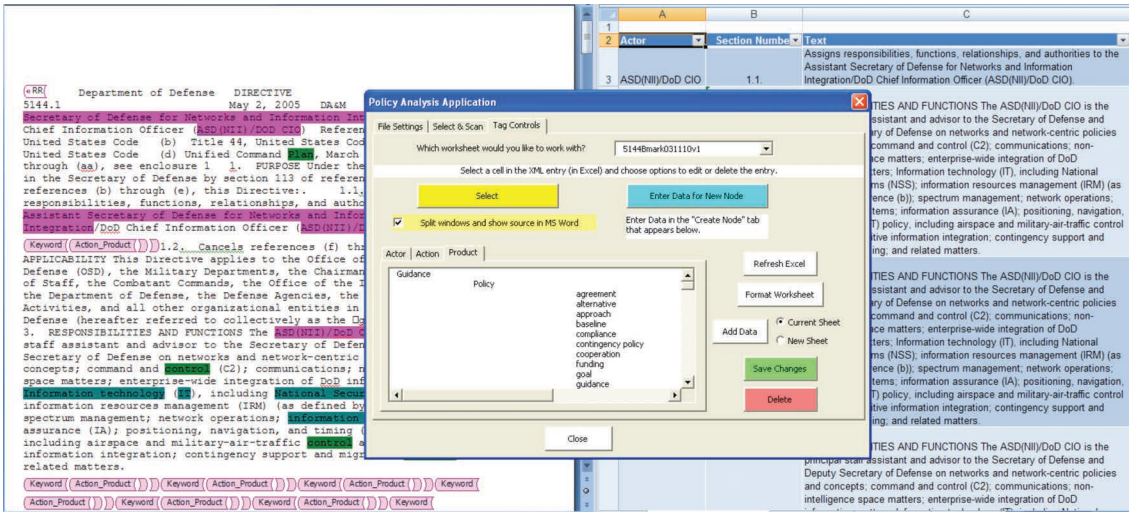
A new XLM node is the medium an analyst uses to modify the results of a previous scan. To create a new node, the user should select the *Split windows and show source in MS Word* checkbox to make the Word results visible. The user then clicks the *Enter Data for New Node*

Figure A.7
***Tag Controls* Interface**



RAND *TR1277-A.7*

Figure A.8
Example *Tag Controls* Side-by-Side Display



RAND *TR1277-A.8*

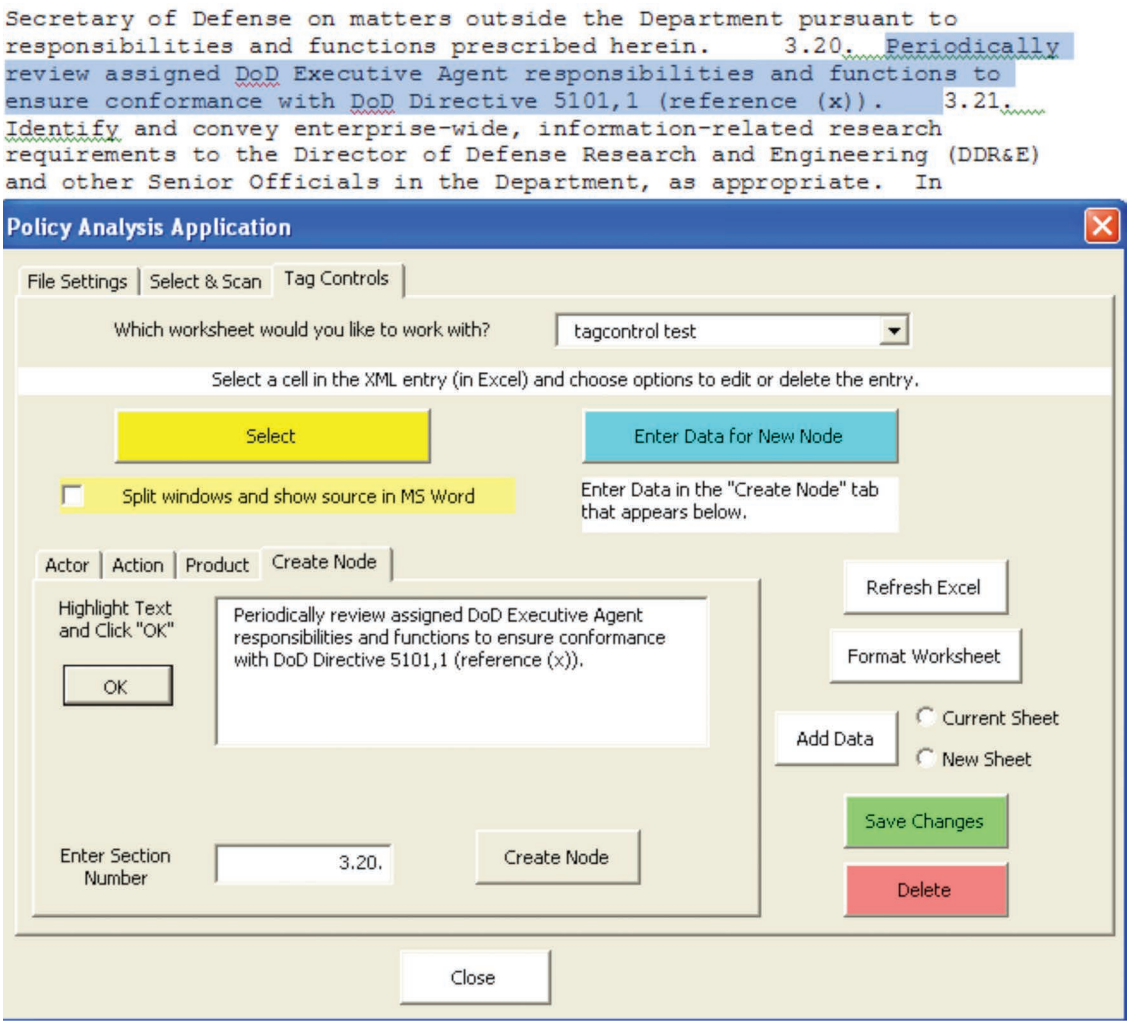
button to make a new subtab visible in the EPIC interface. This subtab is called *Create Node*. In the Word document, the user selects the text of the policy statement, being sure not to include the policy statement's section number in the selection. Then, the user clicks the *OK* button of the *Create Node* subtab. This will automatically move the selected text into the *Create Node* subtab. The user can then edit the text of the policy statement in the subtab and change the section number.

When the user is satisfied with the text, he or she should go to the *Actor, Action,* and *Product* subtabs and select the keywords for this policy. Only one keyword from each category can be used in a single entry, but the same text can be added multiple times if there are multiple keywords of the same type in the same policy statement. Once the appropriate actor, action, and product keywords have been chosen for the policy statement, the user should click *Save Changes* to save the new entry to both the Word and Excel results. Figure A.9 shows an example of highlighted text that can be used to create a new node.

Using the *Tag Controls* tab, the user is also able to delete search results from both the Excel and Word files that do not represent actual policy statements. To delete a result, the user should select a cell in the Excel line for that result, then click *Delete*. EPIC will prompt the user to confirm the deletion. Clicking *OK* will delete the result from both the Word and Excel results. Figure A.10 shows a screen shot of the deletion confirmation interface.

The user can also edit the attributes of search results to capture the best representation of the actual policy statement. To make a change in both the Word and Excel versions of the search results, the user should click on a cell in the Excel line for the particular result to be edited and then click the *Select* button. EPIC will automatically highlight the keywords for the result in the *Actor, Action,* and *Product* subtabs of the *Tag Controls* tab. The user can select different keywords to better reflect the content of the actual policy statement. When the desired keywords have been selected, the user should click *Save Changes* to update both the Excel and Word results. Figure A.11 shows an example of using *Tag Controls* to edit attributes of search results.

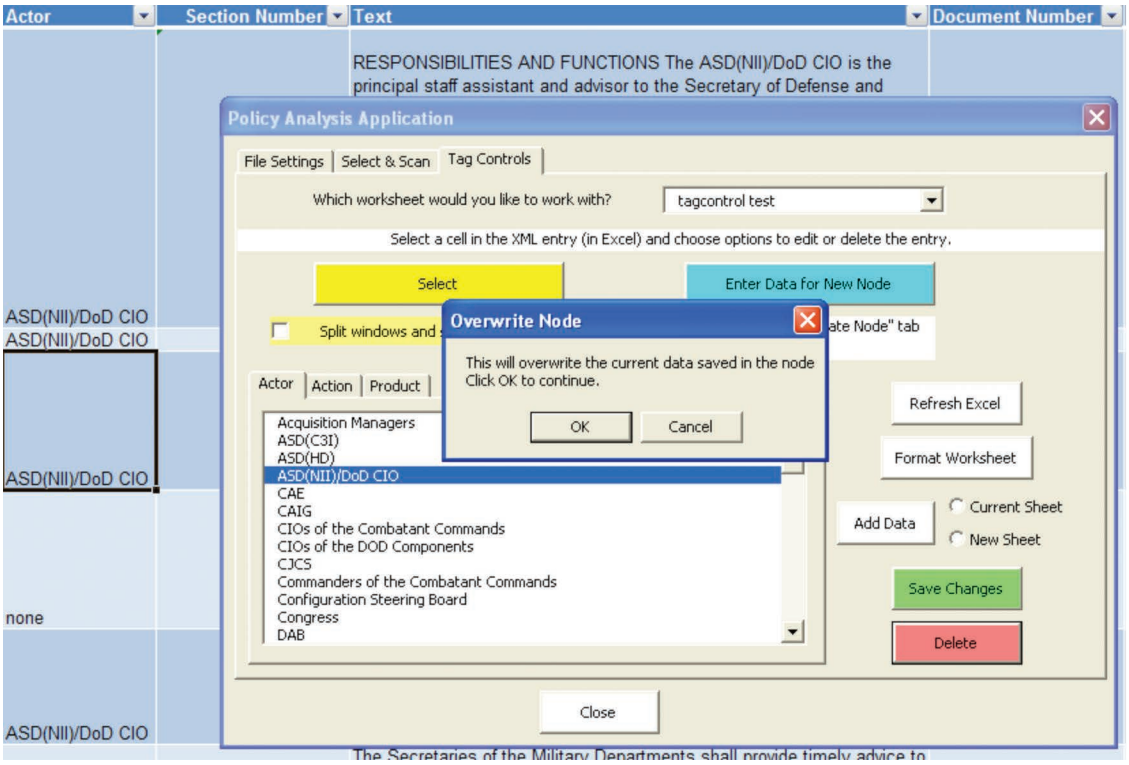
Figure A.9
Example of Highlighted Text to Create Node



RAND *TR1277-A.9*

Finally, the white buttons on the right-hand side of the *Tag Controls* tab provide additional capability for users to share results and keep the Word and Excel versions of the results consistent with each other. The *Add Data* button allows the user to import a set of Word results into Excel as part of the *Current Results* tab or as a new sheet. Importing data this way, rather than copying and pasting a whole worksheet out of another copy of EPIC, maintains the XML settings that allow EPIC to keep the Word and Excel versions of the results in sync. However, if the user does not need to maintain consistency between Word and Excel, copy and paste will suffice. The radio buttons for *Current Sheet* and *New Sheet* control whether the *Add Data* button imports results into a new worksheet or the current worksheet. The *Refresh Excel* button saves the Word and Excel versions of the results and refreshes the screen. If the user has manually deleted any XML result nodes in the Word results, the Excel results must be updated using the *Refresh Excel* button. The *Format Worksheet* button reformats the Excel results to the default EPIC settings.

Figure A.10
Example Use of *Tag Controls* to Confirm a Deletion



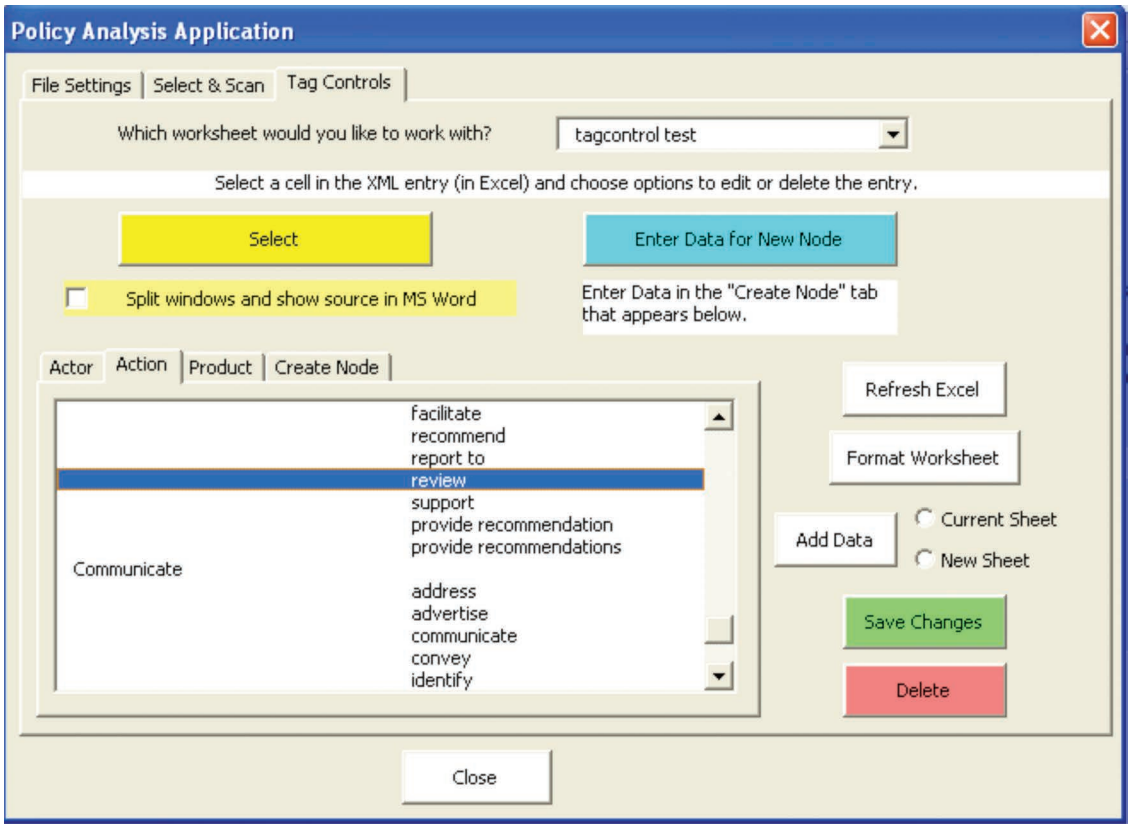
RAND *TR1277-A.10*

The EPIC Preprocessor

The first time EPIC is used to parse a document, the EPIC preprocessor must remove any formatting in the document that might prevent EPIC from properly associating a policy statement with the associated section number. EPIC will run the preprocessor on the input document if the user selected the "This file is not in the proper format" box at the bottom of the *File Settings* tab. The preprocessor edits excess carriage returns, abbreviations, document number references, and colon marks that otherwise break up the structure of the document. When the preprocessor finishes editing the document, it asks the user to inspect the changes and make some manual edits that cannot be done by the program. The user must delete all page headers manually because they interrupt the structure of the text and vary in content from one policy document to another. To assist the user in finding headers, EPIC highlights likely header text. EPIC also reminds the user to remove any unneeded sections of the document before proceeding. Figure A.12 shows a screenshot of the reminders that appear on the screen when the preprocessor has finished its routine. After the user has reviewed the file and made any necessary adjustments, the user clicks *OK*, which causes EPIC to immediately begin the main scan of the document with the user-specified search terms.

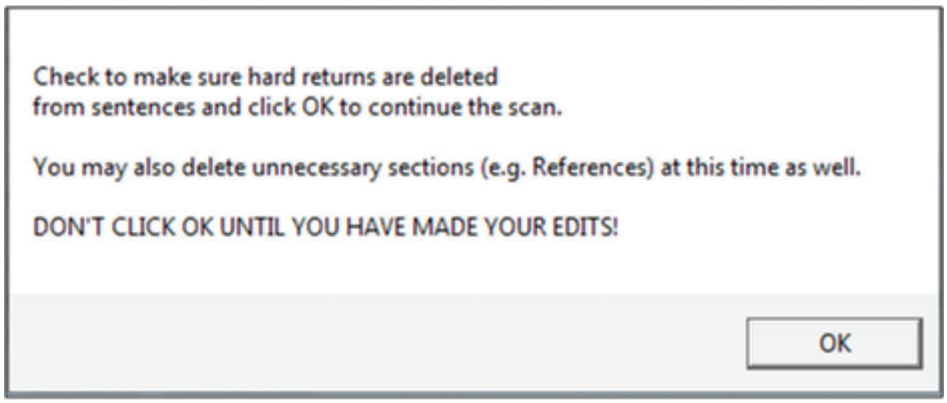
Once the document has been preprocessed, EPIC saves a clean version of the file for future scans. For ease of use, these cleaned files can also be shared with other users through websites, libraries, or shared directories.

Figure A.11
Example Use of *Tag Controls* to Edit Attributes of Search Results



RAND *TR1277-A.11*

Figure A.12
Preprocessor Reminders



RAND *TR1277-A.12*

If the document has previously been scanned by EPIC, then the user will not have checked the "This file is not in proper format" box and the preprocessor step is skipped. In this case, the tool automatically proceeds to scan the document for R&R and creates a searchable file in the form of an Excel spreadsheet that shows the actor, action, and product components of the R&R found based on the input supplied by the user.

The EPIC Scan

During a scan of the cleaned file, EPIC identifies every sentence[4] of the document that contains a selected keyword or a variation of a selected keyword. These keywords are highlighted in a color according to whether the word is an actor, action, or product. If a sentence contains keywords from different categories, EPIC underlines the sentence in the document, attaches an XML tag describing what was found, and adds entries for the sentence to a new Excel worksheet for these results. A given sentence might be cataloged in the results worksheet multiple times, if it has many keywords in it. Each occurrence of the extracted text is called an extraction. Since the same sentence can be listed multiple times in the Excel worksheet with each occurrence associated with a different set of parameters, the analyst may choose to filter the extracted text to nonredundant extractions if that is consistent with the type of R&R analysis being conducted.

EPIC relies on document formatting to correctly identify the section number and other metadata in policy documents. EPIC can identify section numbers up to 15 characters long made up of a series of one- or two-digit numbers separated by periods. For example, "1.3.4.", "12.3.1.1.", and "2." are all valid section numbers to EPIC, but "3.3.a." is not. Some DoD instructions mix Roman numerals, letters, or parentheses in their section numbers; currently, EPIC cannot read section numbers in that format. Other policy documents, such as DTMs, do not typically include section numbers at all. If need be, the user can manually edit documents to include properly formatted section numbers.

The EPIC Output

When the scan is complete, EPIC produces two forms of output. First, EPIC saves the marked-up copy of the document in XML. This document allows the user to quickly glance through the text for other occurrences of highlighted keywords that might be of interest. Second, EPIC saves the catalog of results in an Excel worksheet. This worksheet lists each combination of keywords identified and the text of the entire sentence. To make analysis and organization easier, the section number, the date the search was conducted, and XML filename are all provided.

[4] We are using the term "sentence" loosely to include sentence fragments and other word groupings that may not constitute grammatically correct English sentences. For example, some policies contain lists of R&R written in bulleted format with each bullet being a different R&R, but the bulleted text may not constitute a grammatically correct English sentence. EPIC will extract the text in each bullet as a separate R&R.

Figure A.13 shows an example of an XLM ouput file from an EPIC scan of DoDI 4630.8.[5] In this example, the verbs or actions are highlighted in green and the actors are highlighted in magenta.

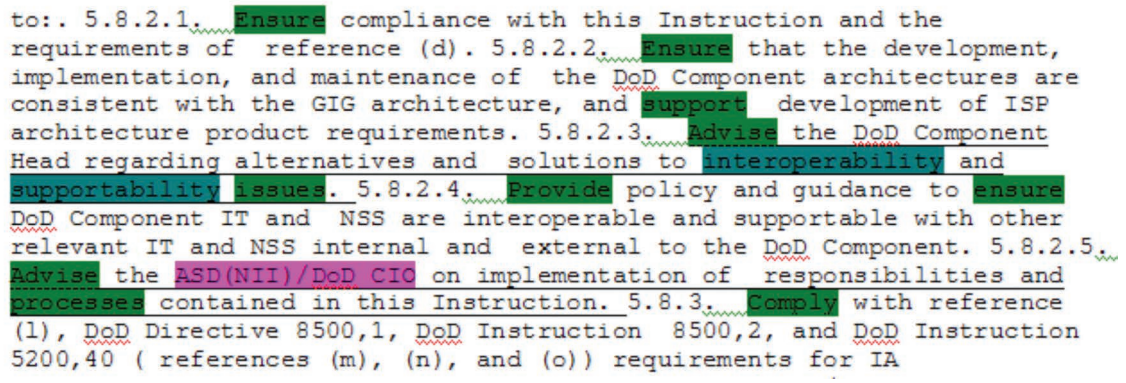
Table A.1 shows an example of the EPIC spreadsheet output from a scan of DoDD 5144.1. The first column shows the actor—in this case, ASD(NII)/DoD CIO is listed as the actor in the extraction. The second column shows the section number where the extracted text appears in DoDD 5144.1. In this case, the extracted text can be found in section 3.26. The third column shows the extracted text. The fourth and fifth columns show document attributes: The fourth column shows the document number, namely, DoDD 5144.1 in this case. The fifth column shows the date that DoDD 5144.1 was issued, namely, "2 May 05."

The sixth and seventh columns show action attributes. The sixth column shows the keyword "ensure" for the first extraction and the keyword "manage" for the extraction in the second row.

The seventh column shows the category of the keyword, which happens to be "Ensure" for the extraction in the first row. The action keyword "manage" in the extraction in the second row is from the action category named "Lead" as shown in the cell in second row and seventh column.

The eighth, ninth, and tenth columns show the product attributes. The eighth column shows the product keyword from the extracted text. For the extraction in the first row, the product keyword is "policy." For the extraction in the second row, the product keyword is also "policy." The ninth column shows the product category of the product keywords. For both extractions, the product category of the product keyword "policy" is "Guidance." The tenth column shows the product keyword subcategory. For both extractions, the product keyword subcategory is "Policy."

Figure A.13
Example of the Word Markup of a Policy Document



RAND *TR1277-A.13*

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

Table A.1
Example of EPIC Output

Actor	Section Number	Text of Policy Statement	Document Attributes		Action Attributes		Product Attributes		
			Number	Date	Keyword	Category	Keyword	Category	Subcategory
ASD(NII)/DoD CIO	3.26	Ensure that NII and CIO policies and programs are designed and managed in ways that improve standards of performance, economy, and efficiency and that all Defense Agencies and DoD Field Activities under the authority, direction, and control of the ASD(NII)/DoD CIO are attentive and responsive to the requirements of their organizational customers, internal and external to the Department.	DoDD 5144.1	May 2, 2005	Ensure	Ensure	Policy	Guidance	Policy
ASD(NII)/DoD CIO	3.26	Ensure that NII and CIO policies and programs are designed and managed in ways that improve standards of performance, economy, and efficiency and that all Defense Agencies and DoD Field Activities under the authority, direction, and control of the ASD(NII)/DoD CIO are attentive and responsive to the requirements of their organizational customers, internal and external to the Department.	DoDD 5144.1	May 2, 2005	Manage	Lead	Policy	Guidance	Policy

Bibliography

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

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

Chairman of the Joint Chiefs of Staff Instruction 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems,* December 15, 2008.

Chairman of the Joint Chiefs of Staff Instruction 3170.01G, *Joint Capabilities Integration and Development System (JCIDS),* March 1, 2009.

Chen, Peter, "The Entity-Relationship Model—Toward a Unified View of Data," *ACM Transactions on Database Systems,* Vol. 1, 1976.

———, "Entity-Relationship Modeling: Historical Events, Future Trends, and Lessons Learned," in Manfred Broy and Ernst Denert, eds., *Software Pioneers: Contributions to Software Engineering,* Berlin and Heidelberg: Springer-Verlag, 2002.

Department of Defense Directive 3020.49, *Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,* Under Secretary of Defense for Acquisition, Technology, and Logistics, June 4, 2007.

Department of Defense Directive 3200.12, *DoD Scientific and Technical Information (STI) Program (STIP),* Under Secretary of Defense for Acquisition, Technology, and Logistics, February 11, 1998.

Department of Defense Directive 3222.4, *Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures,* July 31, 1992, Change 1, October 22, 1993; Change 2, Under Secretary of Defense for Acquisition, Technology, and Logistics, January 28, 1994.

Department of Defense Directive 3600.1, *Information Operations (IO),* Under Secretary of Defense for Policy, August 14, 2008.

Department of Defense Directive 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* Department of Defense Chief Information Officer, May 5, 2004.

Department of Defense Directive 4650.05, *Positioning, Navigation, and Timing (PNT),* Department of Defense Chief Information Officer, February 19, 2008.

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 5000.59, *DoD Modeling and Simulation Management,* Under Secretary of Defense for Acquisition, Technology, and Logistics, August 8, 2007.

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 5134.01, *Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))*, Director of Administration and Management, December 9, 2005.

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 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),* Department of Defense Chief Information Officer, April 14, 2004.

Department of Defense Directive 8115.01, *Information Technology Portfolio Management,* Department of Defense Chief Information Officer, October 10, 2005.

Department of Defense Directive 8320.03, *Unique Identification (UID) Standards for a Net-Centric Department of Defense,* Director of Administration and Management, March 23, 2007.

Department of Defense Directive 8500.01E, *Information Assurance (IA),* Department of Defense Chief Information Officer, October 24, 2002.

Department of Defense Directive 8521.01E, *Department of Defense Biometrics,* Under Secretary of Defense for Acquisition, Technology, and Logistics, February 21, 2008.

Department of Defense Directive 8570.01, *Information Assurance (IA) Training, Certification, and Workforce Management,* Department of Defense Chief Information Officer, August 15, 2004.

"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),* Department of Defense Chief Information Officer, June 30, 2004.

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 Defense Instruction 5000.35, *Defense Acquisition Regulations (DAR) System,* Under Secretary of Defense for Acquisition, Technology, and Logistics, October 21, 2008.

Department of Defense Instruction 5000.61, *DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A),* Under Secretary of Defense for Acquisition, Technology, and Logistics, December 9, 2009.

Department of Defense Instruction 8410.02, *NetOps for the Global Information Grid (GIG),* Department of Defense Chief Information Officer, December 19, 2008.

Department of Defense Instruction 8430.02, *NetOps for the Global Information Grid (GIG),* November 3, 2008.

Department of Defense Instruction 8410.02, *NetOps for the Global Information Grid (GIG),* Department of Defense Chief Information Officer, December 19, 2008

Department of Defense Instruction 8500.2, *Information Assurance (IA) Implementation,* Department of Defense Chief Information Officer, February 6, 2003.

Department of Defense Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP),* Department of Defense Chief Information Officer, November 28, 2007.

Department of Defense Instruction 8520.2, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE),* Department of Defense Chief Information Officer, April 1, 2004.

Department of Defense Instruction 8523.01, *Communications Security (COMSEC),* Department of Defense Chief Information Officer, April 22, 2008.

Department of Defense Instruction 8551.01, *Ports, Protocols and Services Management (PPSM),* Department of Defense Chief Information Officer, August 13, 2004.

Department of Defense Instruction 8552.01, *Use of Mobile Code Technologies in DoD Information Systems,* Department of Defense Chief Information Officer, October 23, 2006.

Department of Defense Instruction 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing,* Department of Defense Chief Information Officer, October 9, 2007.

Department of Defense Instruction 8580.01, *Information Assurance (IA) in the Defense Acquisition System,* Department of Defense Chief Information Officer, July 9, 2004.

Department of Defense Instruction 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense,* Department of Defense Chief Information Officer, June 2005.

Department of Defense Instruction 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense,* Department of Defense Chief Information Officer, June 8, 2010.

Department of Defense, "DoD Issuances," website. As of July 7, 2012:
http://www.dtic.mil/whs/directives

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

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

Feinerer, Ingo, *A Formal Treatment of UML Class Diagrams as an Efficient Method for Configuration Management*, Vienna, Austria: Vienna University of Technology, 2007.

Gonzales, Daniel, Carolyn Wong, Eric Landree, and Leland Joe, *Are Law and Policy Clear and Consistent? Roles and Responsibilities of the Defense Acquisition Executive and the Chief Information Officer*, Santa Monica, Calif.: RAND Corporation, MG-958-NAVY, 2010. As of July 7, 2012:
http://www.rand.org/pubs/monographs/MG958.html

Public Law 107-347, *E-Government Act of 2002,* December 17, 2002.

Some PDF to Word Converter freeware. As of July 7, 2012:
http://www.somepdf.com/

U.S. Code Title 10—Armed Forces. [This report refers to the 2006 version of Title 10, with Supplement II, dated October 5, 2009. This was the version available on the House of Representatives website on December 21, 2009.]

U.S. Code Title 40—Public Buildings, Property, and Works. [This report refers to the 2007 version of Title 40 dated June 18, 2009. This was the version available on the House of Representatives website on December 21, 2009.]

U.S. Code Title 44—Public Printing and Documents. [This report refers to the 2007 version of Title 44 dated July 20, 2009. This was the version available on the House of Representatives website on December 21, 2009.]

U.S. 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.

U.S. Department of Defense, *DoD Architecture Framework Version 2.0,* DoD Deputy Chief Information Officer, May 28, 2009.

U.S. Department of Defense, *Department of Defense (DoD) Efficiency Initiatives,* Secretary of Defense Memorandum, August 16, 2010.

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

RAND

HEADQUARTERS CAMPUS
1776 MAIN STREET, P.O. BOX 2138
SANTA MONICA, CA 90407-2138

OFFICES
SANTA MONICA, CA
WASHINGTON, DC
PITTSBURGH, PA
NEW ORLEANS, LA/JACKSON, MS
BOSTON, MA

ABU DHABI, AE

CAMBRIDGE, UK
BRUSSELS, BE

www.rand.org

OBJECTIVE ANALYSIS.
EFFECTIVE SOLUTIONS.

RAND publications are available at www.rand.org

$32.95

TR-1277-NAVY