



NATIONAL DEFENSE RESEARCH INSTITUTE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Purchase this document](#)

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore the [RAND National Defense
Research Institute](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

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

Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation

Eric Landree, Daniel Gonzales, Chad Ohlandt, Carolyn Wong

Prepared for the United States Navy

Approved for public release; distribution unlimited



NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was sponsored by the United States Navy. The research was conducted in the 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

Implications of aggregated DoD information systems for information assurance certification and accreditation / Eric Landree ... [et al.].

p. cm.

Includes bibliographical references.

ISBN 978-0-8330-4948-3 (pbk. : alk. paper)

1. United States. Dept. of Defense--Information resources management. 2. United States. Dept. of Defense--Information technology. 3. Computer security--United States--Management. 4. Cyberinfrastructure--United States. 5. Computer networks--Security measures--United States. 6. Computer networks--Certification--United States. 7. Computer networks--Accreditation--United States. 8. Information technology--Security measures--United States. 9. Information technology--Certification--United States. 10. Information technology--Accreditation--United States. I. Landree, Eric.

UA23.3.I47 2010

355.6'88011--dc22

2010004574

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Cover photos: (top) U.S. Navy photo by Mass Communication Specialist 3rd Class Joshua Scott; (bottom) iStockphoto.

© Copyright 2010 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND Web site is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (<http://www.rand.org/publications/permissions.html>).

Published 2010 by the RAND Corporation

1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

1200 South Hayes Street, Arlington, VA 22202-5050

4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665

RAND URL: <http://www.rand.org>

To order RAND documents or to obtain additional information, contact

Distribution Services: Telephone: (310) 451-7002;

Fax: (310) 451-6915; Email: order@rand.org

Preface

This monograph presents observations from an ongoing research project cosponsored by the Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition, Chief Systems Engineer (ASN RDA CHSENG). It discusses existing policies that prevent or inhibit military services from conducting information assurance certification and accreditation for a collection of systems that are colocated or operate on a common platform.

This research was conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on RAND's Acquisition and Technology Policy Center, contact the Director, Philip Antón. He can be reached by email at atpc-director@rand.org; by phone at 310-393-0411, extension 7798; or by mail at the RAND Corporation, 1776 Main Street, P.O. Box 2138, Santa Monica, California 90407-2138. More information about RAND is available at www.rand.org.

Contents

Preface	iii
Figures	vii
Tables	ix
Summary	xi
Acknowledgments	xvii
Abbreviations	xix
 CHAPTER ONE	
Background and Objective	1
Background	1
Objective	4
Organization of This Monograph	5
 CHAPTER TWO	
Growing Challenges for the Information Assurance Certification and Accreditation of DoD Information Systems	7
Software Complexity	7
Increasing Software Vulnerabilities and Malware Population	9
Limitations of Automated Software Review Tools	11
Challenge of Incremental Program Development	11
Increasing Scrutiny of Programs	12
System Interdependence and Interconnectedness	12
Configuration Management and System Administration	13

CHAPTER THREE

Overview of the Current DoD Information Assurance

Certification and Accreditation Process..... 15
DIACAP Activities and Scope..... 15
Definition of a DoD Information System..... 16
DIACAP Validation Activities and Results..... 17

CHAPTER FOUR

Aggregation Approach to DoD Information Assurance

Certification and Accreditation 19
Degrees of Aggregation..... 19
Potential DIACAP Policy Issues 23
 Initiate and Plan Information Assurance Certification and
 Accreditation 23
 Implement and Validate Information Assurance Controls..... 24
 Decommission 27
Potential DIACAP Implementation Difficulties for Aggregate
 Information Systems..... 28
 Initiate and Plan Information Assurance Certification and
 Accreditation 28
 Implement and Validate Information Assurance Controls..... 28
 Make Certification Determination and Accreditation Decisions..... 29
 Maintain Authorization to Operate and Conduct Reviews 36
Balancing Transparency and Reporting Requirements..... 36
Information System Information Assurance Pedigree 37

CHAPTER FIVE

Observations and Recommended Changes to DoD and

Federal Policy..... 41
Policy Recommendations 42
Implementation Recommendations..... 44
A Suggested Partial IA Aggregation Approach..... 45

APPENDIXES

A. DIACAP System Identification Profile 47
B. Definitions of MAC, CL, and MC..... 53

References 57

Figures

2.1.	Source Lines of Code for the Windows and Debian Linux Operating Systems.....	8
2.2.	Executable Source Lines of Code for Selected Weapon Systems.....	9
3.1.	DIACAP Activities.....	16
4.1.	Hypothetical Categories for Aggregating DoD Information Systems.....	20
4.2.	Schematic Diagram for Platform Accreditation Determination for Example in Table 4.4.....	35

Tables

S.1.	Assessment of Policy Issues Related to IS Aggregation.....	xiii
4.1.	Assessment of Policy Issues Related to IS Aggregation.....	22
4.2.	Potential DIACAP Accreditation Determination.....	31
4.3.	Example Aggregate DoD IS Interdependency Matrix	32
4.4.	Example Aggregate DoD IS Interdependency Matrix with Interdependent Accreditation Determination.....	34
A.1.	SIP Data Elements from DoDI 8510.01, Enclosure 3.....	48

Summary

The challenges associated with securing U.S. Department of Defense (DoD) information systems (ISs) have grown as the department's information infrastructure has become more complex and interconnected. At the same time, the potential negative consequences associated with cyber intrusions have become more severe, as demonstrated by the recently publicized breach of computer networks at defense contractors involved in the development of the F-35 aircraft (Gorman, Cole, and Dreazen, 2009). An important question to consider is whether current information assurance (IA) policies and procedures are sufficient to address this growing threat and well suited to address vulnerability issues associated with highly networked ISs.

Presently, all DoD ISs must individually satisfy the certification and accreditation (C&A) requirements outlined in DoD Instruction (DoDI) 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)" (2007), prior to receiving authorization to operate (ATO). As written, the DIACAP is focused on conducting C&A for a single system.

As the number of individual DoD ISs continues to grow, and as they become more interdependent and are integrated in more complex ways (for example, using service-oriented architectures, or SOAs), the time and resources required to complete the C&A process will also increase. Similarly, the current C&A process, which focuses on the individual, discrete IS, may overlook potential vulnerabilities introduced at the interface between an ever-increasing number of ISs and by increasingly complex network connections. Therefore, DoD might

find it necessary to consider new policies and procedures for assessing IA C&A for heterogeneous and variable collections of networked systems and components. The objective of this study was to determine whether there were any existing DoD or other federal policies that could prevent or inhibit the U.S. Department of the Navy from applying the DIACAP to an aggregate of ISs or systems of systems (SoSs) that are colocated or operate on a common platform (e.g., Navy vessel or aircraft). A revised C&A process that focuses on aggregates of ISs or SoSs should ideally provide the transparency and situational awareness sought by the current process, require fewer resources to conduct, and identify potential vulnerabilities that exist at the interface between ISs.

We considered three levels of aggregation. The first was the full aggregation approach (option 1), in which every DoD IS on the platform or at the location is aggregated into a single DoD IS. The second was the partial aggregation approach (option 2), in which systems are logically aggregated such that the final number of aggregate DoD ISs is less than the original number of ISs. For the purposes of this policy analysis, we aggregated DoD ISs by mission assurance category (MAC), confidentiality level (CL), and mission criticality (MC).¹ We used these categories because of their relationship to the required IA controls and the final accreditation determination. Further investigation would be needed to determine the optimal set of categories for aggregating DoD IS. The final case that we investigated involved no aggregation (option 3), or what is essentially the current status quo defined in federal policy documents, in which each system is assessed and certified individually. The final analysis for each of the three types of aggregation is shown in Table S.1.

The partial aggregation approach (option 2) identified fewer potential policy issues and fewer implementation difficulties compared to the full aggregation approach. Many of the issues associated with implementing a partial aggregation approach could be addressed with minor changes to the current DIACAP System Identification

¹ See Appendix B for definitions of these three characteristics and their levels.

Table S.1
Assessment of Policy Issues Related to IS Aggregation

Degree of Aggregation	Full Aggregation	Partial Aggregation	No Aggregation
	<i>Option 1</i>	<i>Option 2</i>	<i>Option 3</i>
1. Initiate and plan IA C&A			
–Register system with DoD component IA program	Red	Yellow	Green
–Assign IA controls	Yellow	Green	Green
–Assemble DIACAP team	Green	Green	Green
–Initiate DIACAP implementation plan	Green	Green	Green
2. Implement and validate assigned IA controls			
–Execute DIACAP implementation plan	Green	Green	Green
–Conduct validation activities	Yellow	Yellow	Green
–Prepare POA&M	Red	Yellow	Green
–Compile validation results and DIACAP Scorecard	Yellow	Yellow	Green
3. Make certification determination and accreditation decisions			
–Make certification determination	Yellow	Green	Green
–Issue accreditation decision	Yellow	Green	Green
4. Maintain authorization to operate and conduct reviews			
–Maintain situational awareness	Yellow	Yellow	Yellow
–Maintain IA posture	Yellow	Yellow	Yellow
–Conduct review (at least annually)	Yellow	Yellow	Green
–Initiate reaccreditation	Green	Green	Green
5. Decommission			
–Retire system	Red	Red	Green

■ No policy issues identified
■ No policy issues identified; potential difficulties with implementation identified
■ Potential policy issue(s) identified

Profile (SIP) and the DIACAP Scorecard. It would also be necessary to work with the White House's Office of Management and Budget (OMB) to determine the appropriate level of aggregation to meet OMB's Plan of Action and Milestones (POA&M) reporting requirements.

Under the current DoDI 8510.01, IA managers encounter difficult obstacles associated with monitoring IA situational awareness, conducting IA control validation activities, summarizing validation results, and attempting to preserve the IA posture of their systems individually and collectively as part of a larger SoS. The difficulty associated with these activities would likely persist even if an aggregate DoD IS approach were implemented unless new standards for measuring IS security are developed, along with new techniques for monitoring, tracking, and validating IA controls. These techniques should leverage methods derived from systems engineering.

We identified one potential policy issue for this approach that would require significant modification to DoD policy. Specifically, DoD policy does not currently allow for the decommissioning or the modification of a portion of a DoD IS. It would be necessary to alter existing policy to allow a component DoD IS that is part of a larger aggregate DoD IS to be decommissioned or modified without the need to also decommission or modify the larger aggregate DoD IS. Similarly, there is no method to verify the validity or accuracy of the C&A assessment for a DoD IS with a component DoD IS that has been decommissioned, modified, or removed. Currently, the only option is to recertify the entire IS.

In the Navy, identical or nearly identical individual ISs are implemented across different platforms. According to current IA policy, each instantiation of an IS should be certified and accredited independently. The current approach is possibly justified by the fact that the configuration of individual ISs may vary across platforms. It should be noted, however, that this heterogeneity potentially introduces IA vulnerabilities and complexity. Furthermore, the current approach may cause the Navy to incur greater costs for the many individual IA certifications required than if a common configuration of individual ISs were defined and maintained across the Navy fleet and other platforms. Analysts in the Navy and in DoD have started to develop concepts and approaches

for defining common secure or trusted configurations for individual ISs. Such a configuration can generally be characterized as the IA pedigree of an IS. Several definitions of IA pedigree have been proposed. However, in order for the concept of IA pedigree to be applied effectively to IA C&A aggregation efforts, a precise definition is needed.

Based on our analysis of existing policies, we make the following recommendations to enable an SoS approach to conducting IA C&A:

- Policy recommendations:
 - Restructure the SIP and the DIACAP Scorecard described in DoDI 8510.01 to allow them to track both component DoD ISs and aggregate DoD ISs.
 - In consultation with OMB, develop an acceptable level of DoD IS aggregation, and develop a strategy for tracking information security performance between the POA&M and DoD budget documentation.
 - Develop or adopt a common set of IS security metrics that can be used to aggregate information assurance control validation results across the full range of ISs.
 - Develop specific guidance and policy for modifying or decommissioning components or subsystems of an aggregated DoD IS.
- Implementation recommendations:
 - Conduct a pilot project to investigate alternative approaches to and categories for partial aggregation and to assess the potential benefits of IA controls and C&A procedures for an aggregated DoD IS or DoD SoS.
 - Develop and refine a definition of IS IA pedigree that can be used in the IA aggregation C&A process.

In this monograph, we define an IS IA *pedigree* as including an IS configuration management plan and an IS IA control profile, as well as other IA metrics. (For a detailed definition of an IS IA pedigree, see Chapter Four of this monograph.)

Drawing from experience in other areas of systems engineering, it is possible that an SoS approach to IA may improve overall IA per-

formance and enhance overall information security situational awareness, IA posture, and overall performance. However, this has yet to be proven. Based on our initial analysis, a partial aggregation strategy that used MAC, CL, and MC as the principal categories for aggregation appears to present a reasonable first approach for achieving an aggregated C&A process and would require relatively few changes to the current process outlined in DoDI 8510.01.

The current DIACAP process has been characterized as a significant improvement over its predecessor. However, it is not without its own limitations. As DoD and the rest of the federal government move toward a more decentralized, service-oriented architecture, the process of conducting IA C&A will become more daunting, and an ever-increasing number of potentially critical IA vulnerabilities will likely go unidentified until it is too late. Therefore, it is important for DoD to investigate systems engineering methods and techniques to help ensure the protection and availability of the nation's critical communication and information networks.

Acknowledgments

This monograph would not have been possible without the support of our sponsor, Carl Siel, chief systems engineer for ASN RDA CHSENG, and Cheryl Walton, director of ASN RDA CHSENG's Standards, Policy, and Guidance Directorate. We also wish to specifically thank Michael Harper and Scott Bell, who were detailed to ASN RDA CHSENG's Standards, Policy, and Guidance Directorate to investigate IA aggregation, for their feedback and input regarding the initial presentation that eventually led to this monograph.

We thank Philip Antón and Mark Arena for their careful reviews of initial drafts. And we thank RAND colleagues Robert Anderson and LCDR David Levy, 2009–2010 U.S. Navy research fellow, for their thorough reviews of the final draft. Their comments and insights significantly improved the logic, clarity, and accuracy of the final document.

Abbreviations

AIS	automated information system
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ASN RDA CHSENG	Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition, Chief Systems Engineer
ATO	authorization to operate
C&A	certification and accreditation
CL	confidentiality level
COTS	commercial, off the shelf
DATO	denied authorization to operate
DIACAP	U.S. Department of Defense Information Assurance Certification and Accreditation Process
DoD	U.S. Department of Defense
DoDD	U.S. Department of Defense Directive
DoDI	U.S. Department of Defense Instruction
DoD CIO	U.S. Department of Defense Chief Information Officer

ESLOC	executable source lines of code
GIG	Global Information Grid
IA	information assurance
IAC	information assurance control
IATO	interim authorization to operate
IATT	interim authorization to test
IS	information system
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JTRS	Joint Tactical Radio System
MAC	mission assurance category
MC	mission criticality
OMB	Office of Management and Budget
OS	operating system
POA&M	Plan of Action and Milestones
SIP	System Identification Profile
SOA	service-oriented architecture
SoS	system of systems

Background and Objective

Background

The purpose of information assurance (IA) is to protect information systems (ISs) from serious and frivolous attacks and to ensure the integrity, availability, confidentiality, authentication, and nonrepudiation of the information contained therein. Over time, there has been a steady increase in the number of attacks against federal agencies' computer systems, including those of the U.S. Department of Defense (DoD) (Nakashima, 2008). DoD has disclosed to Congress that it detected 360 million attempts to penetrate its networks in 2008—up from 6 million in 2006—and that it had spent \$100 million in the previous six months repairing damage from cyberattacks (Gorman, Cole, and Dreazen, 2009).

The challenges associated with securing DoD ISs have grown as the department's information infrastructure has become more extensive, complex, and interconnected. At the same time, the potential negative consequences associated with cyber intrusions have also become more severe, as demonstrated by the recently publicized breach of computer networks at defense contractors involved in the development of the F-35 aircraft (Gorman, Cole, and Dreazen, 2009). While contradictory statements have been issued regarding the intrusion into the F-35 program and whether the unclassified networks of primary U.S. defense contractors were compromised (Nakashima, 2009; Fulghum and Warwick, 2009), it is clear that the U.S. government has made significant changes in response to this and related intrusions.

In early 2007, the Air Force launched a partnership with about a dozen contractors working on the F-35 and F-22 programs. In August of that year, then–Deputy Secretary of Defense Gordon England gathered the top executives of major contractors for a classified briefing on cyber threats to their companies:

“We shared with them the fact that we’ve got a very, very aggressive cyber threat,” said Robert Lentz, a Pentagon official who heads the partnership. The Pentagon soon will seek to amend defense acquisition rules to require cybersecurity standards for firms seeking contracts. (Nakashima, 2009)

Other changes to DoD IA policy are also under consideration, including revisiting the DoD certification and accreditation (C&A) framework. This framework is critical for ensuring that IA controls and procedures for securing DoD ISs are in compliance with DoD and federal policies.

An important question to consider is whether current IA policies and procedures are sufficient to address the threat. Most current IA policies and procedures are focused on protecting and securing individual ISs and the networks that connect them. However, they do not identify or address vulnerabilities that can emerge when ISs and networks that are certified and accredited individually are interconnected in more complex configurations.

Although small portions of the overall DoD network (e.g., enclaves and local area networks) have been certified using the DIACAP process, DoD has not attempted to apply this C&A process collectively to all system types or all systems in the entire Global Information Grid (GIG). This is probably not technically feasible for a number of reasons, in particular because the GIG is a constantly changing and growing network of networks.¹ In addition, the advent of Web ser-

¹ While much greater configuration control is maintained over the GIG than over the Internet, the two collections of networks have many similarities, especially in terms of configuration-control challenges, because of the many hosts and interconnections that characterize both networks, the many heterogeneous IT standards in use, and the many generations of technologies employed. This lack of homogeneity presents significant IA challenges.

vices and service-oriented architectures (SOAs) has further increased the interconnectivity of DoD and federal ISs. SOAs are becoming the standard design paradigm for new and emerging DoD ISs. The rapid evolution of interconnected ISs and new SOA technologies suggest that a larger collection of ISs should undergo IA C&A as a configuration-controlled collection of systems.

Another important question is whether the IA C&A framework can accommodate the growing number and complexity of ISs being installed on military platforms and at fixed locations. In addition, there is the question of whether the time necessary to execute the C&A process makes it less effective—both operationally and from a security perspective.

In a recent speech, General Peter Chiarelli, the U.S. Army Vice Chief of Staff, touted the rapid development and deployment of two new ISs that have provided U.S. forces with important new capabilities during recent operations in Iraq (Chiarelli, 2009). He had a major hand in bringing these systems to the field without going through the traditional IA certification process.² Both were developed by the Defense Advanced Research Projects Agency outside of the DoDI 5000 acquisition process (see DoDI 5000.02, 2008). In justifying the reasons for this, General Chiarelli characterized the IA certification process as broken and stated that, if the Army had had to put these systems through the traditional IA certification process, Command Post of the Future would only now be reaching troops in the field, in 2009. And, even though the Tactical Ground Reporting System completed initial development in 2008, by the end of 2009, more than 19 brigade combat teams will be equipped with this new IS (Chiarelli 2009).

The Navy faces similar challenges. It takes on average 18 months to complete an IA C&A for a typical IS on a Navy ship (Newborn, 2009). Navy cruisers have upwards of 27 separate networks onboard, and carriers have up to 44 separate networks (Kiriakou, 2009). In addi-

² The systems are Command Post of the Future and the Tactical Ground Reporting System. The first was fielded in 2005, less than a year after its initial development. The latter was fielded in 2008 after a similarly compressed development schedule.

tion, each ship has hundreds of individual ISs, each requiring IA C&A. These IA C&A processes are conducted in parallel, frequently using independent test regimes or different IS vulnerability and exposure enumerations, even though the ISs will be operated simultaneously in a mutually interdependent way during actual operations. Increasingly, in the Navy and at the joint program level, a system of systems (SoS) approach is being used to manage the development of large system clusters. Therefore, it is useful to consider whether an SoS approach can improve effectiveness and reduce the time required for IA DoD C&A processes.

Objective

Presently, all DoD ISs must satisfy the C&A requirements outlined in DoD Instruction (DoDI) 8510.01 “DoD Information Assurance Certification and Accreditation Process (DIACAP)” (2007) prior to receiving authorization to operate (ATO).³ Current DoD and federal policies are defined for individual, homogeneous systems or components. However, as the number of individual DoD ISs continues to grow, and as these systems become more interdependent and are integrated in more complex ways (for example, using SOAs), the time and resources required to complete the C&A process will also increase. Similarly, the current C&A framework, which focuses on the individual, discrete IS, may overlook potential vulnerabilities introduced at the interface between an ever-increasing number of ISs and by increasingly complex network connections. Therefore, DoD might find it necessary to consider new policies and procedures to assess IA C&A for heterogeneous collections of networked systems and components that vary across multiple dimensions (e.g., mission assurance category [MAC],

³ DoD IS is defined in DoDI 8500.2 (2003) as the “[s]et of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS [automated information system] applications, enclaves, outsourced IT-based processes, and platform IT interconnections” (para. E2.1.17). It includes within its definition hardware, software, and networks.

confidentiality level [CL], mission criticality [MC], function, life-cycle phase).

The objective of this study was to determine whether there are any existing DoD or other federal policies that would prevent or inhibit the U.S. Department of the Navy from applying the DIACAP to an aggregate of ISs or SoS that are colocated or operate on a common platform (e.g., Navy vessel or aircraft). We also examined whether the current single-system C&A approach can be extended with minimal changes to DoD or U.S. government policy to address IA vulnerabilities that are evident only in the SoS context. Ideally, a revised C&A framework should provide all the benefits sought by the current process but consume fewer resources, not impair the operational readiness of the vessel, and identify vulnerabilities that can arise from the integration of individual systems.

Organization of This Monograph

This monograph is organized as follows. Chapter One has briefly explored the issues concerning the need for IA C&A and the motivation for this study. Chapter Two discusses some of the challenges associated with the current framework as applied to DoD information infrastructure. Chapter Three provides a brief introduction to the DIACAP process and a description of its primary activities.

Chapter Four introduces the concept of degrees of aggregation of DoD ISs for the purposes of C&A and provides an assessment of specific DIACAP activities that either inhibit or preclude aggregated C&A because of current DoD or federal policies. That chapter also includes a discussion of some of the potential security trade-offs and offers a definition of IS IA pedigree for use in the IA aggregation C&A process.

Chapter Five concludes the monograph with preliminary recommendations for changes to DoD and federal policies to enable the current DIACAP to be applied to C&A of an aggregation of DoD ISs in a logically defined SoS. It also proposes some additional considerations

and strategies as the Department of the Navy moves forward with SoS C&A aggregation.

Finally, two appendixes provide background on the DIACAP System Identification Profile (SIP) and some of the terminology used in this monograph.

Growing Challenges for the Information Assurance Certification and Accreditation of DoD Information Systems

DoD acquisition programs that produce ISs face growing challenges in obtaining IA C&A. In this chapter, we review some of the factors that appear to influence these trends and that are increasing the time required to obtain IA C&A.

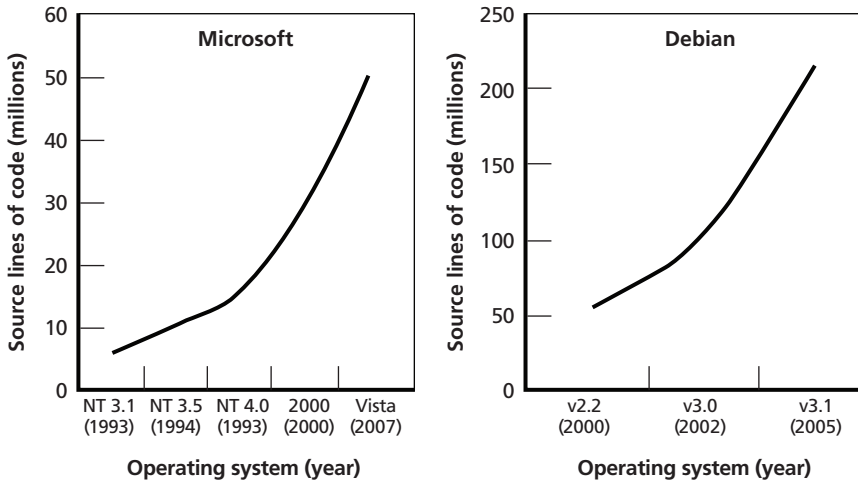
Software Complexity

The first of these factors is the growing software complexity of DoD ISs. The number of software lines of code in commercial, off the shelf (COTS) systems is growing significantly. Figure 2.1 shows the growth in the size of two important elements of the COTS software infrastructure, the Microsoft® Windows® and Debian Linux operating systems (OSs).

The Microsoft Windows OS has grown exponentially in the past decade and now contains more than 50 million lines of code. What is even more surprising is the large size of Debian Linux, one particular variant of the open-source Linux OS. This software code base now comprises more than 200 million lines of code. As the functionality of these two OSs has grown over the past decade, their complexity has also increased significantly.

Of course, DoD is not immune to these trends. DoD ISs, including weapon systems, are increasing in their software complexity as well.

Figure 2.1
Source Lines of Code for the Windows and Debian Linux Operating Systems



SOURCE: Defense Science Board (2009, p. 13, Figure 5).

RAND MG951-2.1

As the Defense Science Board noted in its recent report on information technology (IT) acquisition issues,

Software has spread well beyond defense infrastructure into the very heart of weapon systems. For example, thousands of microprocessors, linear electric drive controllers, dynamic sensors, and millions of lines of sophisticated code enable the startling capabilities of the F-22 and Joint Strike Fighter, as well as quantum increases in the sensitivity achieved using pre-existing sensors. Several years ago a handheld grenade launcher was created with smart projectiles guided by 2,000 lines of code. Moreover, the software code base within mission systems is growing rapidly from generation to generation. (Defense Science Board, 2009, p. 14)

In DoD systems, executable source lines of code (ESLOC) are one metric for measuring the size and complexity of a piece of software. This metric is independent of the source code associated with

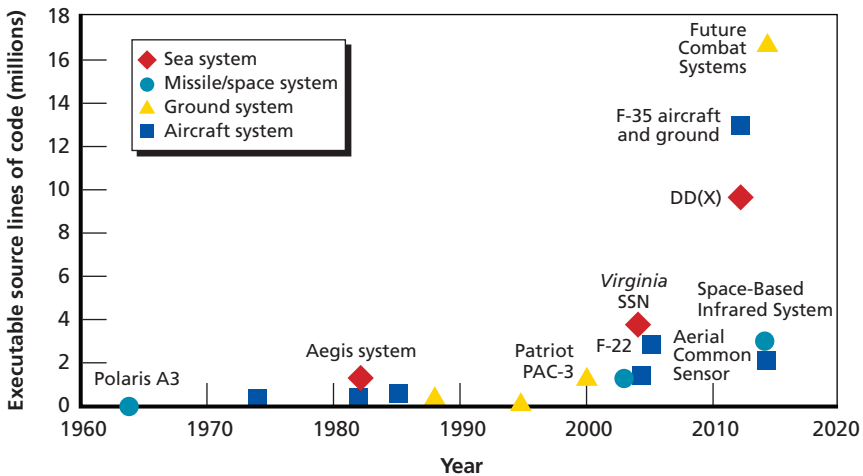
the COTS base or platform on which a particular system may be built. Figure 2.2 illustrates ESLOC growth over time for a selection of weapon systems and how it is expected to dramatically increase out to the year 2020.

The IS component of the U.S. Navy DDG-1000 program contains almost 10 million ESLOC, more than a 50-percent increase from the *Virginia* SSN program and an even larger increase from the Aegis 7.1R baseline.

Increasing Software Vulnerabilities and Malware Population

Growing software complexity and size increases the possibility for intentionally hidden functions to go unnoticed (Baker, 2007). Perhaps more importantly, unintentional errors could remain undetected in the code (Lyons, 2007). It is difficult to produce flawless code with no errors. Software defects can reduce the effectiveness of security features

Figure 2.2
Executable Source Lines of Code for Selected Weapon Systems



SOURCE: Defense Science Board (2009, p. 15, Figure 6).

and can be exploited by an adversary to gain root-level access to an IS. Studies of software defects in large code bases indicate that a defect rate of one per thousand lines of code is typical (Marchenko and Abrahamsson, 2007). This implies that there may have been approximately 50,000 defects in the Microsoft Windows Vista OS at its initial release, and more 200,000 defects in the initial release of Debian Linux. It also implies that there may be 10,000 defects in the Navy's DD(X) software code base. These are IA vulnerabilities that state-sponsored adversaries or hackers could potentially take advantage of.

In addition, a greater amount of software is being produced overseas in countries with lower software engineering costs. These countries may also harbor organizations and individuals with ulterior motives for producing software with flaws of one sort or another. Recent data indicate that more than 70 percent of firms in the U.S. software industry are now offshoring, or producing major software components overseas (Defense Science Board, 2009). These trends raise concerns about the level of trust that can be placed in a software supply chain that now extends, in most cases, beyond the United States, increasing the need for rigorous and comprehensive analysis of software code bases used in DoD ISs.

Another important factor that influences system complexity and the need for comprehensive IA C&A processes is the growing threat that DoD systems face from malware. Earlier in this monograph, we described some of the most visible and publicly discussed threats that have affected DoD programs. Another measure of the threat is the number of viruses or distinct malware programs being released over the Internet that affect both commercial and DoD systems. The number of viruses has increased exponentially over time and is doubling on a year-to-year basis. In 2007, roughly half a million viruses were released over the Internet, requiring antivirus programmers to produce a large number of signatures and countermeasures. In 2008, the number of viruses released into the "wild" reached about a million and 2009 numbers appear to be on track to reach 2 million (Viega, 2009). What are the implications for IA C&A? The C&A process must demonstrate that the IS in question is not vulnerable to all known viruses, for example. With the virus population increasing so rapidly,

test scripts are also growing in size, and tests must be run repeatedly to keep up with the number of viruses, resulting in an increase in the size and complexity of IA tools and tests.

Limitations of Automated Software Review Tools

While automated tools exist to examine the integrity of software code, these tools are far from perfect and, in many cases, can be used only to examine code written in specific software languages. This implies that highly trained individuals are needed to examine software code for flaws and to ensure its integrity. The time needed to review large software programs is one significant factor in determining the overall amount of time required for a program to obtain IA C&A. For example, when the initial version of the Joint Tactical Radio System (JTRS) wideband networking waveform was completed, it was submitted to the National Security Agency for IA C&A. In late 2006, it was determined that this software code contained 2.4 million lines. Initially, the JTRS program office had hoped that this software review could be completed within three months. Experts at the National Security Agency were able to determine very early on that three months would be an insufficient amount of time to review software of this complexity.¹

Challenge of Incremental Program Development

A third factor that makes it difficult to obtain clear-cut IA C&A decisions is that IS programs are increasingly utilizing an incremental development or spiral development approach. The JTRS program again provides a good example. The wideband networking waveform development effort has proceeded over a number of years. Roughly every six months, a new version of the waveform has been developed to try to meet the operational needs of the program. In other words,

¹ Personal communication from Jarrat Mowery, deputy technical director of the JTRS Joint Program Executive Office.

the code base for this IS has changed significantly over time. However, a program code base must be frozen before it can undergo a definitive IA certification. This means that IA certification of software code has to be done serially, after the program has completed development of a major software version, or more than once in incrementally developed programs. Incremental development of IS programs has become the norm rather than the exception in DoD in recent years.

Increasing Scrutiny of Programs

A fourth reason that IA certification has become more difficult is that the level of scrutiny of programs has increased significantly. This was as a result, at least in part, of a retrospective review that determined that a number of older, legacy programs have serious IA vulnerability flaws that were not detected during program development. A thorough evaluation of this problem is beyond the scope of this monograph, however.

System Interdependence and Interconnectedness

Other reasons for the growing difficulty associated with IA C&A have to do with the growing interdependence and interconnectedness of ISs, both in the open commercial market and in DoD. Indeed, the entire concept of the GIG is based on the ability of ISs to be interconnected regardless of their function or organizational lineage. It should also be remembered that the GIG vision includes not just the ability of communication systems to be linked together, but also that computing resources should be shared and made available dynamically to users regardless of their physical location. The growing interoperability afforded by the GIG also introduces potential vulnerabilities that, in the past, may have affected only one small component of the GIG but may now lead to increased vulnerability across the entire network.

Configuration Management and System Administration

Configuration management is, itself, a growing challenge as systems become more complex. It is often possible to secure a system by carefully managing its configuration and ensuring that all ports and protocols are set to a specific set of conditions or options that eliminate vulnerabilities. However, as the complexity of systems grows, so do the number of options or settings that must be managed in these systems. To ensure the security and integrity of the system, highly trained operators may be needed to prevent the settings from being changed inadvertently or, if they are changed, to ensure that they do not introduce potential vulnerabilities.

A related challenge is the administration of systems of greater capability and functionality. Even a desktop computer today has much greater functionality and associated management complexity at the enterprise level than a desktop computer from several IT generations ago. While automated tools have been introduced to help system administrators manage networks of PCs, other computing devices, and networks, it is still a challenge to understand the implications of anomalous behavior that may be detected by intrusion detection systems, network management systems, or other IA tools. In some cases, only highly trained operators can safely ignore or quickly act on an anomalous reading.

Overview of the Current DoD Information Assurance Certification and Accreditation Process

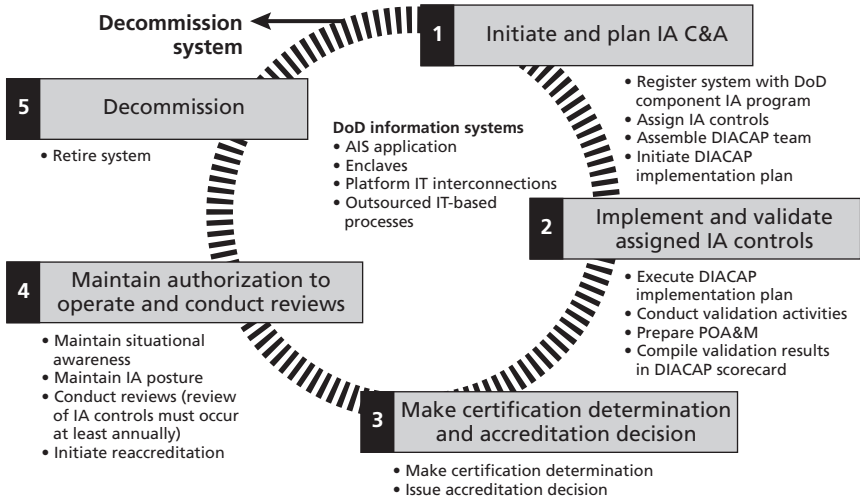
In July 2006, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD[NII]/DoD CIO) signed a memorandum establishing an interim policy for conducting C&A on DoD ISs (Grimes, 2006). The memo was accompanied by a guidance document that outlined the specific procedure to be used for conducting the C&A process for all DoD systems.

DIACAP Activities and Scope

In November 2007, DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” established as DoD policy the guidance included in the 2006 memorandum. The instruction outlines a series of individual activities or tasks that are to be executed during DoD IS C&A, shown in Figure 3.1. The purpose of the DIACAP is to provide a framework for implementing required or necessary IA capabilities and services and an auditable and transparent process for assessing compliance.

Each of the steps and information requirements are supported by DoD or other federal policies and are intended to parallel various steps in the life cycle of a particular system, beginning with initial conception and design and continuing through decommissioning.

Figure 3.1
DIACAP Activities



SOURCE: DoDI 8510.01 (2007, p. 13, Figure F.2).

NOTE: POA&M = Plan of Action and Milestones.

RAND MG951-3.1

The scope of DoDI 8510.01 includes all DoD-owned and -controlled ISs that are operated by a contractor or other entity on behalf of DoD, regardless of sensitivity or classification.¹

Definition of a DoD Information System

A DoD IS is defined in Department of Defense Directive (DoDD) 8500.01E (2007, para. E2.1.16) as the

[s]et of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

¹ DoDI 8510.01 does not alter or supersede existing policies or authorities associated with sensitive compartmentalized information or special-access programs.

Importantly, Enclosure E of DoDD 8500.01E does not preclude this definition from being applied to an aggregation of multiple ISs or an SoS. In other words, the definition of DoD IS does not assert that the information resources specified are tied to a particular function or mission, but rather to the handling and manipulation of information. Thus, this definition does not restrict the number or types of IT resources that can be included in a DoD IS and evaluated as part of a single C&A assessment.

However, as we discuss in Chapter Four, specific steps associated with particular DIACAP activities do inhibit or prevent a single C&A assessment for an aggregation of multiple ISs or an SoS.

DIACAP Validation Activities and Results

In the interest of brevity, we do not describe in detail the steps of the DIACAP process in this monograph. However, in this section, we highlight a few important points regarding DIACAP validation activities. A key part of the validation process is the verification that the proper information assurance controls (IACs) that are needed to maintain the IS's assigned MAC, CL, and MC levels are in place, properly designed, and work effectively. In some cases, a particular system's IACs are inherited from other ISs using the concept of inheritance described in DIACAP policy and in the DIACAP handbook (U.S. Department of the Navy, 2008).

The DIACAP implements the IACs identified in DoDI 8500.2, which include a mandatory set of controls based on an individual system's MAC and CL. The MAC and CL are independent of each other, so there are a total of nine possible combinations. The MAC IA controls address integrity and availability, while the CL IA controls primarily address confidentiality.

The results are compiled into the DIACAP Scorecard, which summarizes the IA posture of an individual IS, documents the accreditation decision, and contains a listing of all IACs and their status. The status of each IAC is determined by one or more validation procedures. Some of these procedures may include tests against known vulnerabili-

ties (for example, computer viruses). The status of each IAC is indicated on the scorecard as follows:

Compliant (C). IACs for which expected results for all associated validation procedures have been achieved.

Non-Compliant (NC). IACs for which one or more expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.

Not Applicable (NA). IACs that do not impact the security posture of the IS as determined by the [designated accrediting authority]. (U.S. Department of the Navy, 2009, para. 4.4.2.7)

Validation tests for each IAC are typically conducted using test scripts that cover a wide range of potential vulnerabilities and have been developed in prior test plans. Test results are compiled and categorized using vulnerability, weakness, and exposure criteria for that particular IS. Later in this monograph, we examine how well such test plans, reports, and results can be aggregated across separate and possibly dissimilar ISs.

Aggregation Approach to DoD Information Assurance Certification and Accreditation

Degrees of Aggregation

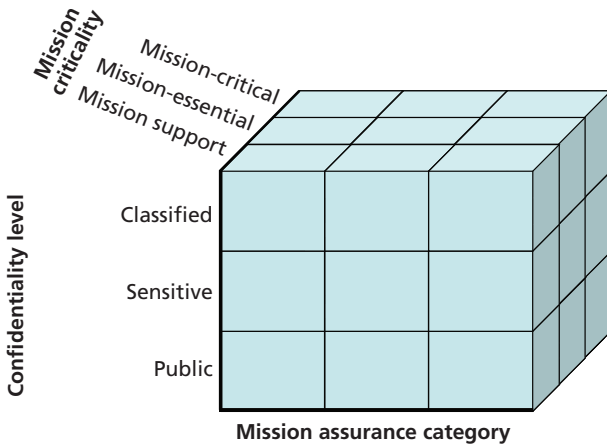
The degree to which one could aggregate DoD ISs for the purposes of conducting C&A is marked by two endpoints. At one end, there is no aggregation of independently developed DoD ISs. This endpoint most closely approximates the current situation, in which each individual IS is documented, reviewed, and assessed independently of all other DoD ISs with which it may interact.

At the other extreme is the notion of aggregating all DoD ISs associated with a particular site or platform, which we refer to as “full aggregation.” While it is conceptually possible to aggregate all DoD ISs across a department or service, for the purposes of this monograph, complete or full aggregation is limited to DoD systems that are collocated or operate on a common platform.

Between these extremes is the notion of partial aggregation of DoD ISs. There are multiple categorizations that could be used for aggregating “similar” or compatible DoD ISs. It may be possible to combine DoD ISs that are related to the same function or based on specific characteristics, such as CL or MAC.¹ We evaluated the partial aggregation scheme that assumed that DoD ISs would be aggregated based on three separate categories, MAC, CL, and MC, as shown in Figure 4.1. Each category contained three values. In other words, a particular platform or location would have, at most, 27 DoD ISs after aggregation was applied. These three categories were selected to

¹ See Appendix B for definitions of these three characteristics and their levels.

Figure 4.1
Hypothetical Categories for Aggregating DoD Information Systems



NOTE: “Public” confidentiality levels refer to systems whose purpose is to provide publicly released information to the public (DoDI 8500.2, 2003).

RAND MG951-4.1

illustrate the concept of partial aggregation because both CL and MAC define the set of IS IA controls that must be implemented, and MC relates to the role of the aggregate DoD IS relative to the platform’s or installation’s mission or function.

Once the systems are aggregated or combined for IA C&A, the number of systems requiring individual C&A will typically be lower than the total number of systems on the platform. This form of aggregation has the potential to produce significant efficiencies (because the number of individual IA tests and analyses can be reduced to correspond to the number of aggregated ISs), and the probability of detecting and resolving cross-IS or networked IS vulnerabilities can be increased (presumably because a comprehensive set of network vulnerability tests can be run against all ISs at once in each aggregation).

In the partial aggregation scheme suggested here, the final number of aggregated DoD ISs that require individual IA C&A will depend on the number of categories, the degree to which individual systems can be combined, and the specific details of the platform or location. Some platforms may possess few distinct types of DoD ISs, resulting

in relatively few aggregate systems (each aggregate may contain a large number of individual ISs). Alternatively, a fixed site or carrier that contains multiple networks and supports a broad range of missions and functions could have all 27 separate aggregate DoD ISs. However, in practice, it would be uncommon for a DoD IS to have a MAC level of 1 (i.e., a system that is vital for operational readiness or mission effectiveness) and also have a CL of “public” and an MC category of “mission support.” Therefore, for most platforms and locations, there would be fewer than 27 separate aggregated DoD ISs.

Using partial aggregation, as opposed to full aggregation, will require a systems engineering approach for defining the boundaries of the aggregated DoD IS, identifying the interdependencies between the various aggregates, and appropriately applying the C&A framework.

We reviewed each of the individual DIACAP activities to determine whether any current DoD or federal policies inhibited conducting the C&A process for DoD ISs that are fully aggregated (option 1) or partially aggregated (option 2). A summary of those findings is shown in Table 4.1. Option 3 is intended to reflect the current status quo, in which no aggregation is implemented and each individual DoD IS is assessed and certified separately. Green cells in the table identify DIACAP activities for which no policy issues were identified.

Yellow indicates DIACAP activities that do not have any specific DoD or federal policy issues but could be difficult to implement or accomplish as currently described in DoDI 8510.01. In the cases of full (option 1) and partial (option 2) aggregation of DoD ISs, the difficulties are generally related to the added complexity incurred as a result of the aggregation.

Cells that are shaded red indicate DIACAP activities for which clear policy issues exist that would inhibit or prevent the C&A process as written from being applied to an aggregated DoD IS.

For the purposes of this monograph, we discuss only those DIACAP activities for which specific policy issues or implementation challenges were identified.

Table 4.1
Assessment of Policy Issues Related to IS Aggregation

Degree of Aggregation	Full Aggregation	Partial Aggregation	No Aggregation
	Option 1	Option 2	Option 3
1. Initiate and plan IA C&A			
-Register system with DoD component IA program	Red	Yellow	Green
-Assign IA controls	Yellow	Green	Green
-Assemble DIACAP team	Green	Green	Green
-Initiate DIACAP implementation plan	Green	Green	Green
2. Implement and validate assigned IA controls			
-Execute DIACAP implementation plan	Green	Green	Green
-Conduct validation activities	Yellow	Yellow	Green
-Prepare POA&M	Red	Yellow	Green
-Compile validation results and DIACAP Scorecard	Yellow	Yellow	Green
3. Make certification determination and accreditation decisions			
-Make certification determination	Yellow	Green	Green
-Issue accreditation decision	Yellow	Green	Green
4. Maintain authorization to operate and conduct reviews			
-Maintain situational awareness	Yellow	Yellow	Yellow
-Maintain IA posture	Yellow	Yellow	Yellow
-Conduct review (at least annually)	Yellow	Yellow	Green
-Initiate reaccreditation	Green	Green	Green
5. Decommission			
-Retire system	Red	Red	Green

■ No policy issues identified
■ No policy issues identified; potential difficulties with implementation identified
■ Potential policy issue(s) identified

Potential DIACAP Policy Issues

Initiate and Plan Information Assurance Certification and Accreditation

As part of the step to register the system with the DoD component IA program under “Initiate and plan IA C&A” (see Table 4.1), the DIACAP requires that each DoD IS being reviewed have a SIP. According to DoDI 8510.01 (2007), the SIP, which contains 32 unique data elements, is used throughout the DIACAP. Attachment 1, Enclosure E of DoDI 8510.01 includes specific instructions along with the minimum data requirements for identifying a particular system. The SIP’s current structure prevents option 1, or full SoS aggregation of DoD ISs. Specific data elements of the SIP require that a program have a unique system type (e.g., AIS, enclaves, platform IT interconnection, outsourced IT-based processes), that it be associated with a single governing mission area (e.g., enterprise information environment, business, warfighting, defense intelligence), and that it also have a single acquisition phase (i.e., pre-A, A, B, C, or post-full-rate production). The current SIP record format also requires that each DoD IS have a single, unique MC, MAC, or CL. In addition, only a single accreditation status (i.e., ATO, interim ATO [IATO], interim authorization to test [IATT], or denied ATO [DATO]) can be issued to a system. The complete list of the SIP data elements identified in DoDI 8510.01 are presented in Appendix A.

The requirement that these SIP data elements have unique entries (i.e., only a single response per data element, not multiple entries per element) would prevent the DIACAP from being applied to a DoD IS that was aggregated at the site or platform level. Most platforms (e.g., Navy vessels) have many DoD ISs at different MACs, at different CLs, and of different types. A single aggregated IS that included all the DoD ISs contained therein would then be composed of multiple MACs, multiple CLs, multiple MC levels, and perhaps even ISs at different phases of acquisition. Such a system could not be registered to perform C&A aggregation using the SIP structure specified in current DoD policy.

For some of the SIP data elements, it may be possible to set the value for the aggregated IS default to the highest or most restrictive level contained within the aggregate. In other words, if an aggregated DoD IS contained public, unclassified, and classified ISs, the aggregate would need to meet all the assigned IA controls corresponding to the highest CL present. However, in practice, this would entail having low-priority, nonessential ISs held to the same standards as high-value, mission-essential ISs. This would not only impose restrictive IA controls on ISs that were never intended to operate under those conditions, potentially causing them to cease to function, but it would also eliminate the justification for assigning separate IA controls based on MAC and CL.

Another drawback to full aggregation, as mentioned earlier, is the assignment of a single accreditation status. Full aggregation would imply that if a single nonessential, non-mission-critical system on a platform or at a common location were issued DATO, the entire aggregate DoD IS would default to the same status.

Implement and Validate Information Assurance Controls

One of the steps under “Implement and validate IA controls” (see Table 4.1) requires that each DoD IS be included in the department’s POA&M. According to the Federal Information Security Management Act (44 U.S.C. 3541 et seq.) and Office of Management and Budget (OMB) policy, agencies are required to report quarterly on IT security performance measures and progress toward addressing or resolving known IT security issues through the POA&M (Bolten, 2004). The policy also explicitly states that it includes both non-national security programs and national security systems and programs. According to OMB Memorandum M-04-25 (Bolten, 2004, p. 14), an agency’s POA&M must “[b]e tied to the agency’s budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.” In other words, the purpose of this requirement is to enable the monitoring and assessment of the relationship between the cost of information security and IA controls for a particular system and that system’s IA performance.

If DoD ISs are aggregated fully to the site or platform level, the aggregate DoD IS would not match the corresponding budget submissions provided to OMB, unless the budget for all the ISs at a single site or platform were similarly aggregated and reported to OMB as such. Assuming that the purpose of linking information security spending with security performance is to improve transparency and accountability, aggregating all DoD ISs to the platform or site level may also be at odds with this POA&M reporting requirement.

In addition, the POA&M does not contain detailed descriptions of specific weaknesses, but it does provide sufficient data to permit oversight and tracking. Aggregation to the site or platform level for all information security weaknesses will likely make tracking and providing oversight more complex and opaque.

Another important step under the “Implement and validate IA controls” area of the DIACAP is to conduct validation activities. These validation activities may include the review of design information for the IS and particular IACs, as well as actual IA vulnerability tests using carefully documented test scripts that cover the full range of vulnerabilities to which a system may be subject. The results of these tests are used to evaluate whether a particular IAC meets the DIACAP criteria discussed in Chapter Three. If these IAC test results are to be combined to produce an aggregated test score for an aggregated or combined set of ISs, these results would have to be summed or combined according to some sort of quantitative combinatorial criteria. This implies that the test results for different ISs must be comparable and, ideally, represent the same security assessment factors. In other words, a common set of security metrics is needed to assess risk for a combined set of ISs.

Security metrics that are measurable and that can be combined for multiple ISs have turned out to be a nontrivial technical challenge for the IT community. A number of initiatives have been created to address shortcomings in IS security metrics, including the following:²

Common Vulnerabilities and Exposures (CVE®)—common vulnerability identifiers

² For detailed descriptions of these initiatives, see *Making Security Measurable* (2009).

Common Weakness Enumeration (CWE™)—list of software weakness types

Common Attack Pattern Enumeration and Classification (CAPEC™)—list of common attack patterns

Common Configuration Enumeration (CCE™)—common security configuration identifiers

Common Platform Enumeration (CPE™)—common platform identifiers

Center for Internet Security (CIS) Consensus Security Metrics Definitions—set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes

Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous [Federal Information Security Management Act] Compliance—twenty key actions or security “controls” that organizations must take to block or mitigate known and reasonably expected attacks

SANS [Institute] Top Twenty—SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses [common vulnerability and exposure identifiers] to identify the issues

OWASP Top Ten—ten most critical Web application security flaws

[Web Application Security Consortium] Web Security Threat Classification—list of Web security threats

Open Vulnerability and Assessment Language (OVAL®)—standard for determining vulnerability and configuration issues

Common Result Format (CRF™)—standardized assessment result format for conveying findings based on common names and naming schemes

Common Event Expression (CEE™)—standardizes the way computer events are described, logged, and exchanged

Open Checklist Reporting Language (OCRL™)—standard for creating reports used in compliance evaluation. (Making Security Measurable, 2009)

The significant number of these initiatives indicates the complexity and the scale of the need for IS vulnerability testing and IS design vulnerability assessments. A potentially even greater challenge will be to develop a methodology to aggregate the results that complies with emerging common IS security metrics across the full spectrum of metrics that are now under development. For these reasons, we assessed the “Conduct validation activities” step of the DIACAP to have implementation challenges, as shown in Table 4.1.

Decommission

Current guidance in DoDI 8510.01 (2007, p. 22) describes the various steps involved in decommissioning a DoD IS. These steps include removing the DIACAP Scorecard and the POA&Ms from all tracking systems. However, DoDI 8510.01 does not provide any guidance or options for decommissioning or modifying only portions of a system. In other words, for a DoD IS that is aggregated to include all DoD ISs located at a given site or on a particular platform (i.e., option 1), or that is aggregated to include even *some* of the DoD ISs (i.e., option 2), if any IS in that aggregation needs to be decommissioned or significantly modified, then the entire aggregated system must either be decommissioned or lose its accreditation.

In the DIACAP, a DoD IS is treated as a single entity and characterized by the various attributes defined in the SIP. Just as DoDI 8510.01 does not allow a DoD IS to have more than one IA record type (e.g., AIS application, enclave, outsourced IT-based process, platform IT interconnection) or more than one MAC level, each DoD IS is allowed to have only a single system life-cycle phase (i.e., concept refinement, technology development, system development and demonstration, production and deployment, operations and support, disposal or decommission).

Potential DIACAP Implementation Difficulties for Aggregate Information Systems

Initiate and Plan Information Assurance Certification and Accreditation

While potentially difficult, a partial aggregation approach (option 2) could be applied for the “Register system with DoD component IA program” activity without the need to change the structure of the current SIP record. The difficulty would depend on which categories were used for the aggregation and the variation of the DoD IS preset. Nonetheless, a partial aggregation strategy would still require careful thought when identifying which DoD IS to aggregate, as well as consideration of the interdependencies and information exchange between individual systems and between aggregates of DoD ISs.

A full aggregation (option 1) approach would also be difficult to implement for the “Assign IA controls” activity and would depend on the variation in MAC and CL on the platform or location. Based on current practices, IS IA controls would default to the highest MAC and CL in the aggregate. For the partial aggregation strategy illustrated in Table 4.1, this would not be an issue because all the systems with similar, MACs, CLs, and MCs would be combined in the same aggregation. However, for the full aggregation approach, public, non-mission-essential ISs would potentially have to meet the same standards as classified, mission-critical systems. While it is conceivably doable, the process of assigning IA controls would be more difficult if aggregated to the entire platform or location.

Implement and Validate Information Assurance Controls

Under the “Prepare POA&M” activity, a partial aggregation approach (option 2) could potentially achieve the appropriate balance between aggregation and traceability of the program’s IA compliance. Achieving both aggregation and traceability would require modification to OMB policy and, possibly, to DoD policy. While the task of rewriting OMB and DoD policy is not insurmountable, OMB policy regarding POA&M reporting applies to all federal departments and agencies. Consequently, changes to federal policy would have to be evaluated to

determine how they may affect other departments or agencies. Therefore, changing OMB policy to suit the needs of a single department, such as DoD, can be difficult, particularly if the same need is not perceived across the rest of the federal government. Even if the changes can be made to OMB policy, it will likely still be necessary to modify DoD policies for IA C&A, which can also be challenging, particularly when the policy changes have the potential to affect large portions of the DoD program baseline.

The “Compile validation results and DIACAP Scorecard” activity is an impediment for both full aggregation (option 1) and partial aggregation (option 2) approaches. This step involves assessing and compiling compliance data for each assigned IA control. Each IA control associated with a particular system is assigned one of three options: compliant, noncompliant, or not applicable. Under the current scorecard method, an IA control is attributed to the entire system, and it can have only a single status (i.e., compliant, noncompliant, or not applicable). However, under an aggregation approach, the same IA control may have a different status in different constituent DoD ISs (i.e., one constituent DoD IS may be “compliant” while another is “noncompliant”). While it may be possible for every IA control to have the same status across the aggregate DoD IS, maintaining the visibility and coherence of each IA control across an entire SoS will be difficult. One solution would be to monitor and track each component IA control separately. A partial aggregation approach in which systems are aggregated by MAC, CL, and MC (Figure 3.1) would make this activity less difficult compared to aggregating DoD ISs of different MACs, CLs, and MCs because all the DoD ISs in the aggregate would have to meet the same IA controls and have approximately the same level of impact on the mission.

Make Certification Determination and Accreditation Decisions

The “Make certification determination” activity requires the certifying authority to assess the performance of the IA mechanisms and the system behavior in the greater information environment. As part of this activity, the certifying authority assigns severity categories for each particular weakness or shortcoming associated with a given DoD IS.

The final DoD IS certification determination involves consideration of the impact codes for the system, which is in indication of the negative consequences associated with failure of the system, and the severity categories, which relate to the level of risk with an identified weakness or shortcoming (e.g., a specific IA control that is noncompliant). According to DoDI 8510.01, severity codes in one part of the system may be offset by security measures in place in a separate system component. However, the process of accounting for any offset that one IA mechanism provides for another is difficult under the best of circumstances. The process of making an informed certification determination will only become more challenging as the degree to which DoD ISs are aggregated increases and systems become both larger and more interconnected.

Once the certification determination is complete, the designated accrediting authority issues the accreditation decision. According to DoDI 8510.01, only a single accreditation status (i.e., ATO, IATO, IATT, DATO) is assigned for the entire system. A description of each accreditation determination and its relative ranking is shown in Table 4.2. There is currently no process or method for documenting accreditations at the component level, nor are there any methods for combining the component accreditations to determine a final aggregate accreditation status.

The full aggregation (option 1) approach would require the constituent DoD ISs to meet IA controls associated with a higher CL or MAC level than those for which they were initially intended or designed, thus making the process of achieving an ATO for the aggregate IS more difficult. However, a partial aggregation approach (option 2) in which all the DoD ISs were aggregated by MAC, CL, and MC would provide a more manageable solution for making a certification determination and issuing an aggregate accreditation decision based on the fact that all the components of the aggregated system would be designed for, and have to be in compliance with, the same set of IA controls.

Once the accreditation decision has been issued for each of the aggregated DoD ISs in a particular platform or location, there then must be a specific logic or clearly defined method for combining the

Table 4.2
Potential DIACAP Accreditation Determination

Accreditation Determination	Description	Relative Ranking
ATO	The DoD IS is authorized to process, store, or transmit information, granted by the designated accrediting authority. Authorization is based on an acceptable IA design and implementation of assigned IA controls.	Highest
IATO	The DoD IS has temporary approval to operate, granted by the designated accrediting authority, based on an assessment of the implementation status of the assigned IA controls.	Medium-high
IATT	The DoD IS is granted temporary approval to conduct system testing by the designated accrediting authority based on an assessment of the implementation status of the assigned IA controls.	Medium-low
DATO	The DoD IS is denied authorization to operate if it is determined by the designated accrediting authority that the system has an inadequate IA design or has failed to implement assigned IA controls.	Lowest

SOURCE: Bendel (2006).

individual accreditation decisions into a single accreditation decision for the SoS. Next, we present a potential method for combining the constituent accreditation decisions to achieve a platform accreditation decision.

C&A Process for a Notional SoS. The example is intended to illustrate a method for determining the accreditation determination for a platform that contains only a limited number of specialized DoD ISs. In our example, the platform contains only the following types of systems, identified by MAC, CL, and MC:

- MAC: level 1
- CL: classified, or sensitive
- MC: mission-critical, or mission-essential.

Aggregating all of the ISs by these three categories would produce four aggregate DoD ISs. For clarity, the four aggregate DoD ISs have been labeled “Weapons,” “ISR” (intelligence, surveillance, and recon-

naissance), “Nav” (navigation), and “Comm” (communication) and are shown in Table 4.3.

The first step involves assessing the accreditation determination for each aggregate DoD IS independently. This could be done using a modified DIACAP C&A procedure that incorporates the recommendations presented in this monograph.

Table 4.3
Example Aggregate DoD IS Interdependency Matrix

Column		A	B	C	D	E				
Row	Aggregate name	Aggregate name				Weapons	ISR	Nav	Comm	Interdependent accreditation determination
		MAC				1	1	1	1	
		CL				Classified	Classified	Sensitive	Sensitive	
		MC				Mission-critical	Mission-critical	Mission-essential	Mission-essential	
		Independently assesses accreditation determination				ATO	IATO	DATO	ATO	
1	Weapons	1	Classified	Mission-critical	ATO					
2	ISR	1	Classified	Mission-essential	IATO					
3	Nav	1	Sensitive	Mission-critical	DATO					
4	Comm	1	Sensitive	Mission-essential	ATO					

After the accreditation determination has been established for each of the aggregate DoD ISs, the next step involves assessing the interdependency of each aggregate DoD IS relative to every other aggregate DoD IS on the platform or those to which it connects. The four aggregate DoD ISs are used to populate the sample dependency matrix shown in Table 4.3.

For this particular example, as shown in Table 4.4, we assigned three levels of interdependency: strong (S), weak (W), and none (blank). The degree of interdependency within the aggregate will be unique for each platform or location and will depend on the specific component DoD ISs present.

In the table, the aggregate for “Weapons” (row 1) is strongly dependent on “ISR” (column B) and weakly dependent on “Nav” (column C). The relationship between aggregate DoD ISs does not necessarily need to be reciprocal. The DoD IS aggregate “Weapons” is strongly dependent on “ISR” (i.e., row 1 is strongly dependent on column B), but the reverse relationship has only a weak dependency (i.e., “ISR” is only weakly dependent on “Weapons”). The term *dependent* means that one system depends on the output or data of another system to operate. A system that is strongly dependent may lose complete functionality if the system on which it depends ceases to function, whereas a system that is weakly dependent would lose only some functionality.

Once the relative interdependencies are determined and the cells in Table 4.4 are filled in, the aggregate DoD ISs are assessed to determine how their relative interdependencies influence their overall accreditation determination. For the purposes of this example, two simple logical operations are constructed to illustrate the process:

- First, if one aggregate DoD IS is strongly dependent on a second aggregate DoD IS that has a lower accreditation determination, then the inferior accreditation (based on the relative rankings shown in Table 4.2) of the second DoD IS is assigned to the first DoD IS.
- Second, if one aggregate DoD IS is only weakly dependent on a second aggregate DoD IS, then the accreditation of the second aggregate has no effect on the first unless it is DATO, in which

case the first aggregate inherits the DATO accreditation from the second aggregate.

We used these two rules to complete the overall accreditation determination for each aggregate DoD IS, based on the separate accreditation determinations and the relative interdependencies, as shown in column E in Table 4.4.

Table 4.4
Example Aggregate DoD IS Interdependency Matrix with Interdependent Accreditation Determination

Column		A	B	C	D	E				
Row	Aggregate name	Aggregate name				Weapons	Interdependent accreditation determination			
		MAC				1		1	1	1
		CL				Classified		Classified	Sensitive	Sensitive
		MC				Mission-critical		Mission-critical	Mission-essential	Mission-essential
		Independently assesses accreditation determination				ATO		IATO	DATO	ATO
1	Weapons	1	Classified	Mission-critical	ATO	S	W	DATO		
2	ISR	1	Classified	Mission-essential	IATO	W		IATO		
3	Nav	1	Sensitive	Mission-critical	DATO			DATO		
4	Comm	1	Sensitive	Mission-essential	ATO		S	DATO		

The application of this method to an actual program or platform would require a more robust set of interdependency rules. They could potentially be designed to be applicable across all platforms and locations. Alternatively, rules could be developed that have the same general structure but could also be tailored to suit the particular mission or function for the platform or location being assessed.

The final step involves using the interdependent aggregate DoD IS accreditation determinations to determine a final platform accreditation. The process described in our example is illustrated in Figure 4.2.

A process for combining the interdependent, aggregate DoD IS accreditation determinations shown at step 3 in Figure 4.2 would need to be developed. Like the rules established for step 2, they could be modified or tailored to the particular platform or mission.

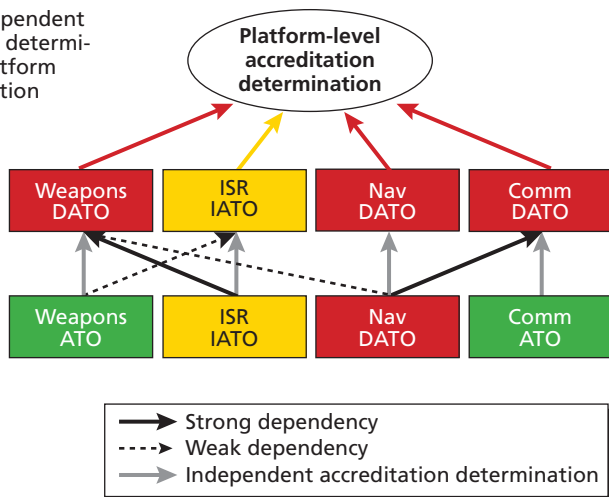
If a particular platform or location had a larger number of aggregate DoD ISs, the matrix shown in Tables 4.3 and 4.4 would have to be scaled up to include rows and columns for each aggregate DoD IS.

Figure 4.2
Schematic Diagram for Platform Accreditation Determination for
Example in Table 4.4

Step 3: Combine interdependent aggregate accreditation determinations to assess the platform accreditation determination

Step 2: Modify accreditation determination based on interdependencies

Step 1: Make accreditation determination for each aggregate DoD IS



This also opens the possibility for more degrees of interdependency as well as the need for more complex rules for combining the various accreditation determinations. Nonetheless, this matrix and much of the process could be automated to the point that the platform program manager inserts the separate accreditation determinations for each aggregate DoD IS and the relative interdependencies into a spreadsheet or tool. The rules for combining could then be either user-defined or predetermined to allow the user see an overall accreditation determination for the platform or location, similar to how the current DIACAP Scorecard operates. As mentioned earlier, this method would also allow changes in the mission or accreditation status of an aggregate DoD IS to be incorporated in real time to inform the platform managers of the impact on mission readiness or capability.

Maintain Authorization to Operate and Conduct Reviews

The “Maintain situational awareness” and the “Maintain IA posture” steps represent a difficult task not only in the context of the full aggregation and partial aggregation approaches, but also for the current status quo. In all three cases, the highly complex interdependency of DoD ISs means that integrating new systems, updating or modifying existing systems, or removing or decommissioning antiquated systems makes maintaining situational awareness and IA posture a daunting task, even under the best of circumstances.

Similarly, the process of “Conducting an annual review” becomes more difficult as the level of aggregation is increased. Conducting a full review of C&A of either the fully aggregated DoD IS (option 1) or the partially aggregated DoD IS (option 2) will require more time, involve greater interdependency, and potentially have a greater impact on the platform’s readiness to operate.

Balancing Transparency and Reporting Requirements

Establishing an IA aggregation approach that balances the need for transparency and reporting requirements is a difficult task. DoDI 8510.01 requires that C&A be conducted at the individual DoD IS

level. However, what is not fully accounted for in the instruction is the validity or fragility of that accreditation once it is introduced into an SoS. The current systems-only approach may lead to IA vulnerabilities that, while not present when the system is assessed independently, emerge once the system is interconnected with other DoD ISs. A potential benefit of an aggregated IA C&A approach is that it may, through an SoS approach, explicitly identify interdependencies between aggregations (in the case of a partial aggregation strategy) while at the same time reducing the total number of individual C&As that need to be performed.

Another important reason for achieving the correct balance is the ability to associate an organization's budget for a specific set of IA capabilities and the performance of those capabilities. However, the current POA&M approach required by OMB associates IA cost and performance with a system-specific view. It assumes that if the IA posture for a given system is low, the program may not be provided sufficient funds for IA capabilities. However, recall that the process of integrating (or removing) a single DoD IS into (or from) a larger DoD SoS can be a source of IA vulnerability. Thus, it is not evident that the sum of funds spent on IA capabilities for individual ISs on a given platform or at a given location is an accurate representation of the overall IA in the aggregate system.

Information System Information Assurance Pedigree

A question related to IA C&A aggregation is how program managers should handle IA certification of individual systems that are identical or nearly identical *internally* across platforms—for example, across ships of the same ship class or across multiple SoSs or network implementations. Should the individual IS be certified for each instantiation of the system, regardless of the similarity or difference among the systems' operating environments? Repeating IA tests, assessments, and risk estimates for the same IS for many similar platforms and SoSs or network implementations may increase certification cost, perhaps substantially.

In this section, we discuss the concept of an IS IA pedigree and investigate whether it can provide a way to manage and control the configuration of individual systems that are part of an IA aggregation and that may enable program managers and platform managers to reduce the cost of IA certifications, especially for identical systems that are implemented across ship, aircraft, or other platform classes.

The Office of the Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance has issued a DoD strategy that provides general guidelines for building trusted platforms and systems that can be used to develop a definition of IA pedigree:

“Pedigree” of a piece of equipment—who designed it, where was it built, and how it was obtained

“Pedigree” of a system’s life cycle – who installed it and maintains it and how is its security parameters configured (e.g., best commercial practices, DoD configuration guide, federal configuration guide)

Trust level of the entity that maintains the configuration (e.g., industry or cleared contractor/government personnel)

How well the system ensures that its configuration is correct, e.g., are software downloads limited to authorized sources and are integrity mechanisms applied, is the configuration frequently checked and refreshed from known good source, are physical security audits performed, and are inventory controls utilized? (ASD[NII]/DoD CIO, 2009)

These guidelines imply that an IS IA pedigree for an individual IS should contain an IS IA posture assessment. Such a posture assessment can be designed so that it can be used in an aggregated IA C&A process for an SoS or platform. For this definition, we borrow heavily from the IS IA pedigree concept under development by Scott Bell in his work for the Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition, Chief Systems Engineer. However, our definition differs in some significant ways. We define the IS IA pedigree as containing the following elements:

- trusted and signed IS design metadata for all IS hardware and software components
- IS IA control profiles
- IA test scripts and plans
- IA test results
- external interface specifications, including DoDI 8510.01 (2007) compliance verification statements
- vulnerability management plan
- IS configuration management plan.

All of these individual items are specified in current DoD IA policy. The one additional item that is of special interest and importance in this investigation is the system configuration management plan. This plan would assure IS IA managers and platform and SoS managers that the configuration of the IS in question had not changed over time in an uncontrolled way and that the latest version of the IS with specified IA control profiles, configuration changes, or system modifications had been retested and recertified.

It is important to point out that the definition of IS IA pedigree does not require that two ISs with the same pedigree have exactly the same physical configuration. For example, the first IS could have two PCs connected to a network with two identical Ethernet ports, while the second could have six PCs connected to a network with six identical Ethernet ports. These two ISs could be determined to have the same pedigree if the Ethernet port interface specifications were identical.

What would be the benefit of establishing an IS IA pedigree for an individual IS and for an aggregated approach to IA certification? Underlying our analysis of IA aggregation is the assumption that individual ISs would have to undergo IA certification at some point in their development cycle, as is required by current DoD IA policy. However, once an individual IS has been certified and given ATO on a particular platform or in a particular SoS, this IA certification could be applied to the same type of IS that is to be implemented on other platforms or in other SoSs. The IS IA pedigree would allow this implementation to occur *without* a second recertification of the individual IS. (An aggre-

gated IS IA certification would still be required at the platform or SoS level.)

The pedigree of the IS could be maintained only if the program manager could demonstrate that the configuration of the system—all elements of the IA pedigree—were unchanged or, if changed, had been tested and recertified. If this is the case, then the system would be given an ATO for the same type of platform or SoS.

For example, assume that a particular IS is certified to operate on a new class of destroyer, the DDG-1000. If the IA pedigree of the IS remained unchanged, then it could be implemented on later ships of the same ship class without having to undergo a second individual IA certification. However the second implementation of the IS on the second destroyer of the same ship class would still have to undergo an aggregated IA certification (either at the platform level or at a lower partial aggregation level for a particular SoS or network).³

³ Further research is required to determine whether the concept of IS IA pedigree as defined in this monograph can enable an effective IA C&A aggregation scheme at the platform level.

Observations and Recommended Changes to DoD and Federal Policy

In the current DIACAP framework, DoD ISs are handled and assessed individually. There is justification for this approach, particularly in light of the POA&M and OMB's desire to be able to link IS security performance with IS security funding. However, the current C&A process does not address the increasing interdependency of these systems and the potential vulnerabilities that may result from an IS-centric assessment. Currently, the C&A process focuses primarily on the system with only limited attention given to the connections and interdependencies between the various systems, which can be a source of vulnerability. Similarly, it is unclear whether the DIACAP can be applied with confidence to an increasingly decentralized or SOA SoS. Services that are developed for use in SOAs typically do not have clear, well-defined boundaries that comply with DoD program deliverables. In particular, DoD is attempting to maximize reuse of data and software services by encouraging the development of SOA services that can be employed across system boundaries and by multiple DoD components and agencies. These services are being designed so they can be orchestrated with other services and applications to provide highly decentralized capabilities for use across DoD. What does it mean to perform C&A on a DoD IS or capability that is composed of multiple services that are distributed across the GIG and that are separately owned, controlled, certified, and accredited? What will be the impact on DoD ISs that are dependent on services whose underlying IA controls or operations have changed? It is not clear that the DIACAP would identify or provide adequate guidance for addressing these issues.

In addition, it is known from systems engineering that gaps in desired capabilities or functions can be introduced when systems are not integrated effectively. This has led to an increasing emphasis on SoS integration and engineering. An idea to consider is whether a similar SoS approach needs to be applied to IA controls and the C&A process. In the same way that adoption of systems engineering approaches has led to improvements in the overall performance and function of systems, a similar emphasis in IA may lead to an improved level of IA and protection for complex SoS.

The appropriate degree of aggregation will be strongly dependent on the platform or site, as well as its function or mission. If the scope of aggregation is too small, it will resemble the current state of affairs and potentially ignore the individual connections to other systems that may introduce vulnerabilities. However, if the degree of aggregation is too large (e.g., all of the Internet), the aggregate DoD IS will be too complex to assign, certify, and accredit reasonable IA controls.

Our preliminary recommendations focus on enabling the first steps toward aggregated C&A of logical collections of IT and national security systems.

Policy Recommendations

Restructure the SIP and the DIACAP Scorecard to enable it to track component and aggregate DoD ISs. Current policy set forth in DoDI 8510.01 (2007) requires DoD ISs to be defined by single attributes (e.g., a single MAC level, a single CL, a single life-cycle phase). The structure and organization of the SIP would need to be modified to allow collections of systems that could potentially accommodate multiple DoD ISs in an aggregated DoD IS. It would also need to be modified to allow the nesting of SIP attributes that relate to either individual component DoD ISs or higher-level aggregated DoD ISs.

Develop an acceptable level of DoD IS aggregation and a strategy for tracking IS security performance between POA&M and budget documentation. One of OMB's primary purposes for requiring departments, services, and agencies to report on information security weak-

nesses and progress toward resolving them is to monitor the balance of the IA and information security budget with IA performance. It is unlikely that this requirement will change in the near future. However, it may be possible to work with OMB to understand what level of granularity is needed and how best to provide information that is both accurate and appropriate. As mentioned earlier, monitoring individual IA spending and capabilities at the system level may not represent the most accurate assessment of the aggregate IA posture at the platform (or location) level. Intelligent aggregation of DoD IS may enable more of a systems engineering approach to designing and implementing IA controls, which could potentially lead to improved IA and information security performance for the aggregate DoD IS.

Develop or adopt a common set of IS security metrics that can be used to aggregate IAC validation results across the full range of systems. Common validation result reporting mechanisms that can be measured using existing or emerging standards are needed to facilitate the aggregation of test and design-review assessment results. These metrics will need to be applicable across the spectrum of different information systems found on board Navy ships and platforms.

Develop specific guidance and policy for modifying or decommissioning a component or subsystem of an aggregated DoD IS. Current policy in DoDI 8510.01 does not provide any information or guidance for decommissioning or modifying only a component of a DoD IS. Irrespective of developing new policies for C&A of aggregated DoD ISs, guidance should be developed and promulgated for decommissioning components or portions of existing DoD ISs. As mentioned in Chapter One, a DoD IS is composed of multiple, individual IT resources—both hardware and software. In most cases, the component IT resources could be defined as their own DoD IS. If an existing piece of hardware or software that is integral to a particular DoD IS is removed, replaced, or modified in a significant way, there is presently no guidance for recertifying or reaccrediting the DoD IS. Therefore, developing new policy for C&A of DoD ISs in which components or subsystems are decommissioned or modified will not only benefit current DoD systems; it will also be useful for informing program manag-

ers of the appropriate methods for decommissioning DoD ISs that are part of a larger, aggregated DoD IS.

Implementation Recommendations

Conduct a pilot project to investigate alternative approaches to and categories for partial aggregation, and to assess the potential benefits of IA controls and C&A procedures for an aggregated DoD IS or DoD SoS. The correct balance of partial aggregation for a DoD IS is still unknown. Drawing from experience in other areas of systems engineering, it is possible that an SoS approach to IA may improve the overall IA posture of an SoS and enhance overall information security situational awareness, IA posture, and overall performance of major DoD platforms, such as Navy ships. However, this has yet to be proven. The current model for IA C&A has numerous reporting requirements (i.e., one DIACAP for each system), even for systems that are relatively simple.

In addition, the current IS IA C&A framework can be slow and cumbersome for larger, more complex ISs. The length of time required to certify ISs has become a major concern and a “road block” that some senior military commanders have chosen to bypass entirely to meet urgent operational requirements (Chiarelli, 2009). Focusing the IA C&A framework at an appropriate SoS or networking level—as opposed to the individual system level—could eventually benefit the IA certification of all ISs for a series of large platforms, such as a Navy ship class.

An approach for further investigating this topic would be to attempt to model the individual DoD systems and their interactions as part of an aggregated DoD IS. Potentially, each DoD IS could be modeled as an independent agent with inherent attributes (e.g., MAC, CL, MC, IA controls) and an explicitly defined interdependency with every other system on the platform. It may be possible through modeling and simulation to determine the optimal parameters along which to aggregate separate DoD ISs. It may also provide useful information about how the SoS may react to changes in individual component DoD ISs due to modification, decommission, or failure.

Another approach could be to develop a pilot project whose purpose is to develop modifications to the current C&A procedures and then apply them to aggregated DoD ISs to assess information security performance compared to other similar systems that are reviewed and assessed independently.

Develop a definition of IS IA pedigree. To achieve the promise of IA C&A aggregation suggested by Navy officials and still comply with existing DoD IA policy, such a policy may need to be supplemented by the concept of an IS IA pedigree, perhaps as defined in this monograph.

An important related question is whether it is possible to reduce IS IA testing, risk analysis, and reporting requirements (i.e., reduce the time and manpower spent conducting C&A) while maintaining the same level of security or improving it. If an IA aggregation pilot study were conducted, it could be used to refine the concept of IS IA pedigree. However, such a pilot study should examine how the concept of IS IA pedigree can be applied to a second SoS or platform, after an initial IS IA pedigree is established. The second case in the pilot study could be used to determine whether planned IA testing, risk analysis, and reporting requirements are reduced and by how much.

A Suggested Partial IA Aggregation Approach

Based on the initial policy analysis presented here, one approach for aggregating DoD ISs would be to use MAC, CL, and MC as the principal categories for aggregation. The central role that MAC, CL, and MC play in assigning specific IA controls, assessing system risk to the mission, and identifying potential IA weaknesses or gaps suggests that they would be the reasonable candidates for an initial IA aggregation approach. Furthermore, they would likely require relatively few modifications to the current process outlined in DoDI 8510.01. Systems with specific MAC, CL, and MC categories can then be defined using criteria that will satisfy C&A requirements. Systems that transcend across categories must be held to a higher standard to meet the same criteria.

The current DIACAP process has been characterized as a significant improvement over its predecessor by some of its authors in the IA community. However, it is not without its own limitations, and some program managers reportedly do not share the same view of the new process. IA managers tasked with maintaining IA situational awareness and preserving the current IA posture struggle at times to fully comprehend and account for potential IA vulnerabilities because they are limited to a system-centric perspective. As DoD and the rest of the federal government move toward a more decentralized and service-oriented architecture, these tasks will only become more daunting, and an ever-increasing number of potentially critical IA vulnerabilities will likely go unidentified until it is too late. Methods for conducting C&A and applying IA controls will need to be reevaluated and updated to provide users and managers with the appropriate methods for ensuring maximum protection and assurance of their information, for their platform or location, and across the GIG.

DIACAP System Identification Profile

Table A.1 presents the 32 SIP data elements included in Enclosure 3 of DoDI 8510.01 (2007). In July 2008, the U.S. Department of the Navy's DIACAP working group released its DIACAP handbook (U.S. Department of the Navy, 2008), which included a table describing the various elements of the SIP. While the SIPs presented in both documents are similar, there are notable discrepancies. For instance, the SIP provided in the Navy's DIACAP handbook contains a total of 48 data elements, compared to the 32 data elements described in DoDI 8510.01 and shown in Table A.1. Most of the additional data elements in the Navy's DIACAP handbook request additional details about the project or are Navy-centric. However, a direct comparison between the two documents also reveals that there is not a one-to-one match between all the data elements in the DoDI 8510.01 SIP and in the Navy's DIACAP handbook. Twenty-eight of the 32 SIP data elements included in DoDI 8510.01 are reflected in the handbook SIP data elements, although in some cases, there are slight differences in the description or text.

Two of the data elements in DoDI 8510.01 have slightly different interpretations in the Navy's DIACAP handbook. Specifically, "Governing mission area" (ID 16 in Table A.1) is not directly present in the SIP included the handbook. The closest matching data element is "Type of IT investment" (U.S. Department of the Navy, 2008, Enclosure 5, Field ID 33). Similarly, "Accreditation status" (ID 20 in Table A.1), which seems to imply the current accreditation status of the DoD IS, is not present in the SIP in the Navy's DIACAP handbook. The closest matching data element appears to be "Accreditation request

type” (U.S. Department of the Navy, 2008, Enclosure 5, Field ID 28). However, in the former case, the data element indicates the current status of the DoD IS being assessed (i.e., unaccredited, ATO, IATO, IATT, or DATO), while in the latter it is an indication of the desired final disposition of the assessment (i.e., ATO, IATO, interim authority to build, interim authority to connect, or IATT).

Finally, two of the SIP data elements in the DoDI 8510.01 SIP do not appear to be represented in the Navy’s DIACAP handbook SIP. The first is “Accreditation documentation” (ID 22 in Table A.1), which asks whether there is documentation to support the current accreditation. The second is “Privacy Act system of records notice required” (ID 26 in Table A.1), which asks whether a Privacy Act system or record notice is required per DoD Regulation 5400.11-R, “Department of Defense Privacy Program,” (2007).

Table A.1
SIP Data Elements from DoDI 8510.01, Enclosure 3

ID	Data Element Descriptor	Example, Acceptable Values, or Comment	Required or Conditional ^a
1	System identification	Provide the system identification number or code used by the DoD component to uniquely identify the system.	Required/ system generated
2	System owner	List the element or organization in the DoD component that owns, controls, or manages the IS.	Required
3	Governing DoD component IA program	List the DoD component that owns the IS.	Required
4	System name	Provide the full descriptive name (e.g., Agency Billing System).	Required
5	Acronym	Provide a shortened or commonly used name or abbreviation (upper case, e.g., ABS).	Required
6	System version or release number	List the version or release number for the IS (e.g., 1.0).	Required
7	System description	Provide a narrative description of the system, its function, and uses. Indicate whether it is a stand-alone system.	Required

Table A.1—Continued

ID	Data Element Descriptor	Example, Acceptable Values, or Comment	Required or Conditional ^a
8	DIACAP activity	Identify the current DIACAP activity: 1. Initiate and plan IA C&A 2. Implement and validate assigned IA controls 3. Make certification determination and accreditation decision 4. Maintain ATO and conduct reviews 5. Decommission.	Required
9	System life-cycle phase	Identify the current life-cycle phase of the IS: 1. Concept refinement 2. Technology development 3. System development and demonstration 4. Production and deployment 5. Operations and support 6. Disposal or decommissioning.	Required
10	System acquisition phase	For programs of record, identify the current system acquisition phase: 1. Pre-Milestone A (concept refinement) 2. Post-Milestone A (technology development) 3. Post-Milestone B (system development and demonstration) 4. Post-Milestone C (production and deployment) 5. Post-full-rate production/deployment decision.	Conditional
11	IA record type	Identify the type of DoD IS: 1. AIS application 2. Enclave (indicate whether stand-alone or network demilitarized zone) 3. Outsourced IT-based process (indicate whether DoD-controlled or whether control is shared with service provider) 4. Platform IT interconnection.	Required
12	Mission criticality	Identify the mission criticality (i.e., mission-critical, mission-essential, or mission support).	Required
13	Accreditation vehicle	Identify the C&A process that was or is being used for C&A of the IS (e.g., DIACAP; Director of Central Intelligence Directive 6/3, 1999; NIST 800-37, 2004).	Required

Table A.1—Continued

ID	Data Element Descriptor	Example, Acceptable Values, or Comment	Required or Conditional ^a
14	Additional accreditation requirements	Identify any additional accreditation requirements beyond the IA C&A process (e.g., privacy, special access requirements, cross-security domain solutions, Nonsecure Internet Protocol Router Network, Secret Internet Protocol Router Network, ports, protocols, and services management).	Conditional
15	Acquisition category	Identify the acquisition category, if applicable (e.g., Acquisition Category I).	Conditional
16	Governing mission area	Identify the mission area: enterprise information, environment, business, warfighting, or defense intelligence.	Required
17	Software category	Identify whether the system software is COTS or government, off the shelf.	Required
18	MAC level	List the IS's MAC level (i.e., MAC I, MAC II, or MAC III).	Required
19	Confidentiality level	List the IS's CL (i.e., public, sensitive, or classified).	Required
20	Accreditation status	Identify the accreditation status of the IS (i.e., unaccredited, ATO, IATO, IATT, or DATO).	Required (default is unaccredited)
21	Certification date	List the date the IS was certified by the certifying authority.	Conditional
22	Accreditation documentation	Are there documentation and artifacts that support the accreditation status?	Conditional
23	Accreditation date	List the date of the current accreditation decision (ATO, IATO, IATT, or DATO). If the IS has no accreditation determination, enter "NONE" and the projected accreditation date.	Required
24	Authorization termination date	List the date that the current accreditation (ATO, IATO, or IATT) is set to expire.	Conditional

Table A.1—Continued

ID	Data Element Descriptor	Example, Acceptable Values, or Comment	Required or Conditional ^a
25	DIACAP team roles, member names, and contact information	Identify the DIACAP team (e.g., designated accrediting authority, certifying authority, the DoD IS program manager or system manager, the DoD IS IA manager, information assurance officer, user representative.	Required
26	Privacy impact assessment required	Indicate whether a privacy impact assessment is required for a new or previously existing IT system.	Required
27	Privacy Act system of records notice required	Indicate whether a Privacy Act system of record notice is required.	Required
28	E-authentication risk assessment required	Indicate whether an e-authentication risk assessment has been performed according to OMB M-04-04 (Bolten, 2003).	Required
29	Date of annual security review	List the date of the last annual security review for systems with an ATO. Required for ISs with an ATO in effect for more than one year.	Required
30	System operation	Identify whether the system operation is 1. Government (DoD)–owned, government-operated 2. Government (DoD)–owned, contractor-operated 3. Contractor-owned, contractor-operated (including outsourced IT services) 4. Contractor-owned, government (DoD)–operated 5. Non-DoD (including federal, state, and local governments; grantees, industry partners, etc.).	Required
31	Contingency plan required	Indicate whether a contingency plan addressing disruptions in operations of the IS is in place.	Required
32	Contingency plan tested	Indicate whether the contingency plan that is in place has been tested.	Required

SOURCE: DoDI 8510.01 (2007, Enclosure 3).

^a Required entries are mandatory for completing the SIP. Conditional entries must be completed if they apply to the system being profiled. If the entry does not apply, it should be left blank.

Definitions of MAC, CL, and MC

Unless otherwise indicated, the following definitions are reprinted verbatim from their respective source documents.

Mission Assurance Category. “Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters’ combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories” (DoDI 8500.2, 2003, Enclosure 2, p. 22).

- **Mission Assurance Category I (MAC I).** “Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures” (DoDI 8500.2, 2003, Enclosure 2, p. 22).
- **Mission Assurance Category II (MAC II).** “Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or com-

modities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance” (DoDI 8500.2, 2003, Enclosure 2, p. 22).

- **Mission Assurance Category III (MAC III).** “Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices” (DoDI 8500.2, 2003, Enclosure 2, pp. 22–23).

Confidentiality Level. “Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: classified, sensitive, and public” (DoDI 8500.2, 2003, Enclosure 2, p. 16).

Mission Criticality, Mission-Critical Information System. “A system that meets the definitions of ‘information system’ and ‘national security system’ in the [Clinger-Cohen Act], the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense [Comptroller].) A ‘Mission-Critical Information Technology System’ has the same meaning as a ‘Mission-Critical Information System’” (DoDI 5000.02, p. 48, Table 8).

Mission-Essential Information System. “A system that meets the definition of ‘information system’ in Reference (v), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the [Under Secretary of Defense (Comptroller)].) A ‘Mission-Essential Information Technology System’ has the same meaning as a ‘Mission-Essential Information System’” (DoDI 5000.02, 2008, Table 8, p. 48.).

Mission-Support Information System. If the information system is neither mission-critical nor mission-essential, it is labeled *mission support* (based on DoDI 8510.01, 2007, p. 37, Table E3.A1.T1).

References

ASD(NII)/DoD CIO—*see* Assistant Secretary of Defense for Networks and Information Integration/U.S. Department of Defense Chief Information Officer.

Assistant Secretary of Defense for Networks and Information Integration/U.S. Department of Defense Chief Information Officer, “DoD Information Assurance Certification and Accreditation Process,” memorandum, July 6, 2006.

———, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, Washington, D.C., August 2009. As of January 12, 2010: http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf

Baker, Jordan, “Cyber Crime Will Spread: Study,” *Sydney Morning Herald*, September 6, 2007, p. 2.

Bendel, Mike, *An Introduction to Department of Defense IA Certification and Accreditation Process (DIACAP)*, Washington, D.C.: Lunarline, Inc., March 1, 2006. As of November 30, 2009: http://www.lunarline.com/docs/Lunarline_DIACAP_Process.pdf

Bolten, Joshua B., Director, Office of Management and Budget, “E-Authentication Guidance for Federal Agencies,” Memorandum M-04-04, December 16, 2003.

———, Director, Office of Management and Budget, “FY 2004 Reporting Instructions for the Federal Information Security Management Act,” Memorandum M-04-25, August 23, 2004. As of November 30, 2009: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf>

Chiarelli, Peter W., keynote address, “Communications and Networking Workshop,” Lincoln Laboratory, Massachusetts Institute of Technology, July 7–9, 2009.

Director of Central Intelligence Directive 6/3, “Protecting Sensitive Compartmented Information Within Information Systems,” June 5, 1999.

Defense Science Board, *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2009.

DoDD—see U.S. Department of Defense Directive.

DoDI—see U.S. Department of Defense Instruction.

Fulghum, David A., and Graham Warwick, “Report of F-35 Data Theft Spotlights Flaws,” *Aviation Week*, April 21, 2009. As of November 30, 2009: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&cid=news/THEFT042109.xml

Gorman, Siobhan, August Cole, and Yochi Dreazen, “Computer Spies Breach Fighter-Jet Project,” *Wall Street Journal*, April 21, 2009, p. A1. As of November 30, 2009: <http://online.wsj.com/article/SB124027491029837401.html>

Grimes, John G., Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, “Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance,” memorandum, July 6, 2006.

Kiriakou, Charlie, “Operation Cyber Asset Reduction and Security (CARS),” July 16, 2009. Not available to the general public.

Lyons, James A., “Asymmetric Cyber Threat,” *Washington Times*, November 13, 2007, p. 21.

Making Security Measurable, homepage, last updated September 10, 2009. As of November 30, 2009: <http://measurablesecurity.mitre.org/>

Marchenko, Artem, and Pekka Abrahamsson, “Predicting Software Defect Density: A Case Study on Automated Static Code Analysis,” in Giulio Concas, Ernesto Damiani, Marco Scotto, and Giancarlo Succi, eds., *Agile Processes in Software Engineering and Extreme Programming*, Berlin: Springer, 2007, pp. 137–140.

Nakashima, Ellen, “Bush Order Expands Network Monitoring; Intelligence Agencies to Track Intrusions,” *Washington Post*, January 26, 2008, p. A3.

———, “Defense Dept., Industry Join to Protect Data,” *Washington Post*, May 25, 2009, p. A19.

Newborn, Chris, “Consolidated Afloat Networks and Enterprise Services (CANES)—The Vision,” briefing, “Communications and Networking Workshop,” Lincoln Laboratory, Massachusetts Institute of Technology, July 7–9, 2009.

National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems: Information Security*, Gaithersburg, Md., Special Publication 800-37, May 2004. As of November 30, 2009: <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

NIST—see National Institute of Standards and Technology.

U.S. Code, Title 44, Section 3541 et seq., Federal Information Security Act of 2002.

U.S. Department of Defense Directive 8500.01E, "Information Assurance," current as of April 23, 2007.

U.S. Department of Defense Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008.

U.S. Department of Defense Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

U.S. Department of Defense Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007.

U.S. Department of Defense Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

U.S. Department of the Navy, *DOD Information Assurance Certification and Accreditation Process (DIACAP) Handbook*, version 1.0, July 15, 2008. As of November 30, 2009:
<http://www.doncio.navy.mil/PolicyView.aspx?ID=730>

Viega, John, McAfee, Inc., "The Future of Anti-Virus," briefing, "Communications and Networking Workshop," Lincoln Laboratory, Massachusetts Institute of Technology, July 7–9, 2009.