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

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.

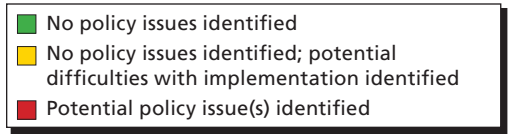
We considered three levels of aggregation. The first was the full aggregation approach (option 1), in which every DoD IS on the platform or at the location is aggregated into a single DoD IS. The second was the partial aggregation approach (option 2), in which systems are logically aggregated such that 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 *Option 1*	Partial Aggregation *Option 2*	No Aggregation *Option 3*
1. Initiate and plan IA C&A			
–Register system with DoD component IA program			
–Assign IA controls			
–Assemble DIACAP team			
–Initiate DIACAP implementation plan			
2. Implement and validate assigned IA controls			
–Execute DIACAP implementation plan			
–Conduct validation activities			
–Prepare POA&M			
–Compile validation results and DIACAP Scorecard			
3. Make certification determination and accreditation decisions			
–Make certification determination			
–Issue accreditation decision			
4. Maintain authorization to operate and conduct reviews			
–Maintain situational awareness			
–Maintain IA posture			
–Conduct review (at least annually)			
–Initiate reaccreditation			
5. Decommission			
–Retire system			



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.