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

NATIONAL DEFENSE RESEARCH INSTITUTE

RAPID ACQUISITION AND FIELDING FOR INFORMATION ASSURANCE AND CYBER SECURITY IN THE NAVY

Isaac R. Porche III | Shawn McKay | Megan McKernan
Robert W. Button | Bob Murphy | Kate Giglio | Elliot Axelband

Prepared for the United States Navy

The research described in this report was prepared for the United States Navy. The research was conducted within 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 under Contract W74V8H-06-C-0002.

Library of Congress Cataloging-in-Publication Data

Porche, Isaac, 1968–
Rapid acquisition and fielding for information assurance and cyber security in the Navy / Isaac R. Porche III, Shawn McKay, Megan McKernan, Robert W. Button, Bob Murphy, Kate Giglio, Elliot Axelband.
pages cm
Includes bibliographical references.
ISBN 978-0-8330-7855-1 (pbk. : alk. paper)
1. United States. Navy—Computer networks. 2. United States. Navy—Procurement. 3. Computer networks—Security measures—United States—Planning. 4. Computer networks—Access control—United States. I. Rand Corporation. II. Title.

VB212.P67 2012
359.6'212—dc23

2012048798

Published 2012 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

In July 2010, the U.S. Navy's Program Manager, Warfare (PMW) 130, Information Assurance and Cyber Security Program Office, was established under the Program Executive Office for Command, Control, Communications, Computers, and Intelligence (PEO C4I). PMW 130's primary mission is to maintain cyber security, and one of its challenges is the need to rapidly acquire and field materiel that provides cyber security. The reason for this challenge is that today's acquisition approach is not geared toward cyber security. Like the other services, the Navy requires a cyber acquisition process that can react much faster than formal U.S. Department of Defense acquisition channels. The primary reason for this need is that many cyber technologies and products have fast development and deployment cycles that must be matched with rapid acquisition processes to avoid obsolescence when deployed. This report recommends a streamlined acquisition process that supports PMW 130's goals to rapidly and proactively field innovative capabilities that will keep the Navy ahead of the cyber threat. It specifically focuses on testing, certification and accreditation, ship modernization, budgeting and funding, contracting, governance, and integration and training.

This report should be of interest to the acquisition community in the Navy and the other military services, the Office of the Secretary of Defense, the defense agencies, Congress, and the defense industry.

This research was sponsored by PMW 130 in PEO C4I, U.S. Department of the Navy, and 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. Questions and comments about this research are welcome and should be directed to the project leader, Isaac Porche, at Isaac_Porche@rand.org.

For more information on the RAND Acquisition and Technology Policy Center, see http://www.rand.org/nsrd/ndri/centers/atp.html or contact the director (contact information is provided on the web page).

Contents

Figures

Tables

Summary

This report focuses on a single analytical question: How can the information technology (IT) acquisition process best support the mission of the U.S. Navy's Program Executive Office for Command, Control, Communications, Computers, and Intelligence (PEO C4I) with regard to computer network defense (CND) programs of record?

Identifying an agile and adaptable acquisition process that can field new IT capabilities and services in relatively short and responsive time frames "to provide capabilities to secure the cyber domain, assure end-to-end information and enable decision superiority" is a pressing issue for the Navy. Cyber threats, such as viruses and worms, can wreak havoc on computer networks, swiftly mutating on a daily basis. A quick response to these threats is not just desirable—it is critical. The Navy's Program Manager, Warfare (PMW) 130, an office within PEO C4I that is focused on rapidly and proactively fielding innovative capabilities to stay ahead of cyber threats, anticipates needing an acquisition and fielding cycle that can deliver hardware security products within 12–18 months, software security products within six to 12 months, and incremental development for both hardware and software every three months. These time frames are very expeditious when compared with the Navy's traditional acquisition cycle time, which can take 36 months from concept approval to initial operational capability (IOC) or eight to ten years for full operational capability (FOC). The traditional acquisition process, as it now exists, needs to be accelerated in response to the unique demands of IT and especially in addressing emerging cyber threats.

The RAND National Defense Research Institute was asked to recommend a streamlined acquisition process that supports PMW 130 goals to field innovative capabilities in a way that is sufficiently rapid and proactive to ensure that the Navy stays ahead of the cyber threat.[1] The resulting analysis took into account requirements management, integration and experimentation, testing, certification and accreditation, ship modernization, budgeting, and fielding, and this report offers a number of options for structuring the organizations and processes that support or will support PMW 130's acquisition goals. As with all change, success in the cyber acquisition arena will require a good deal of planning, strong governance, and openness to stepping beyond the familiar.

It should be emphasized that future planning for PMW 130's main acquisition program, Computer Network Defense, was part of the motivation for this study. PMW 130 quickly realized the challenges involved in fulfilling time-critical operational requirements when the office started planning for Increment 2 of the CND program, which relies on the traditional

[1] We define *streamlined* as the absence of many of the bottlenecks in the current acquisition process, which would allow PMW 130 to acquire and field capabilities within an expedited timeline.

acquisition process rather than the less formal measures used for Increment 1 of the program. The program office wants to follow the Defense Science Board (DSB) model described in the "804 Report" issued by the Office of the Secretary of Defense, which provides for the iterative and incremental development of IT programs.[2] This is a challenge. To stay ahead of cyber threats, PMW 130 anticipates needing software updates every six months with CND's Increment 2. Formulating an acquisition strategy with updates every six months is challenging in an acquisition system in which information assurance, testing, and installation typically take a significant amount of time. Thus, we provide recommendations for PEO C4I, and PMW 130 in particular, to navigate these processes and fulfill their cyber missions and goals.

Approach

To develop a streamlined approach to cyber acquisition for PMW 130 and the CND acquisition program, we first explored the current literature on rapid and IT acquisition. We also conducted interviews with Navy PEO C4I personnel and examined case studies of successfully streamlined cyber acquisition programs. From studies, interviews, and case studies, the research team was able to garner a host of potential best practices that might be applied here.

Interviews with key personnel and offices revealed the specific hurdles that PMW 130 is encountering in trying to secure a suitable acquisition schedule. To supplement the insight gained from these discussions, we also reviewed current DoD and Navy policy, guidance, and memos related to PMW 130's cyber acquisition processes. Supplemented by interviews, this review of policy allowed us to identify the specific acquisition processes that the CND program will require to meet PMW 130's needs. It also provided valuable insight into how PMW 130 and CND might overcome policy and process hurdles.

Defining PMW 130's Acquisition Challenges

In general, today's acquisition system is designed for large-scale, hardware-based weapon systems. It is marked by a high level of oversight and a deliberate, serial approach to development and testing. As a result, the current DoD 5000-series process—from requirements definition to initial operational test and evaluation (OT&E)—typically takes years to complete. Such a process is particularly unsuited for dynamically changing IT systems.[3] DSB studied the issue and found that only 16 percent of all IT systems were on budget and on time, while 53 percent were both late and over budget, typically by more than 89 percent (DSB, 2000, p. 11).

In PEO C4I, acquisition programs average 36 months from concept approval to IOC and eight to ten years to FOC. Table S.1 compares the average timelines for traditional major defense acquisition programs (MDAPs), IT programs, and Navy rapid acquisition programs.

PEO C4I recognizes that these processes are not responsive enough for Navy warfighters operating in the cyber domain. Cyber assets are needed with greater immediacy than assets that fulfill needs in other, more traditional domains; cyber threats surface frequently–even

[2] The report, *A New Approach to Delivering Information Technology Capabilities in the Department of Defense*, was issued in response to Section 804 of the fiscal year 2010 National Defense Authorization Act. Section 804 directs the U.S. Department of Defense (DoD) to develop and implement a new acquisition process for IT systems based on the recommendations of a March 2009 DSB report.

[3] The DoD 5000 series is a set of DoD instructions that govern the defense acquisition process.

Table S.1
Estimated Average Duration of Steps in the Acquisition Process, Traditional, IT, and Navy Rapid Acquisition Programs

	Program Type			
Process Step	**20 Navy Rapid Acquisition Programs**	**PEO C4I Rapid Deployment Capability Programs (AIS, CBSP, SNR/HFIP, WRBS)**	**IT MAIS Acquisition Programs**	**DoD MDAPs**
Validate requirements	185 days	376 days to IOC	14 months (AoA approved)	10 months
Develop and submit PPBE/budget request	206 days to IOC		77 months to IOC (5 months of OT&E)	2 years
Acquisition				2 years to decades
System engineering/ testing and C&A				
Contract/product/ procurement				
NMP and installation		18 months		
Logistics and Training				

NOTE: AIS = Automatic Identification System. C&A = certification and accreditation. CBSP = Commercial Broadband Satellite Program. MAIS = major automated information system. PPBE = planning, programming, budgeting, and execution. SNR/HFIP = Subnet Relay and High-Frequency Internet Protocol. WRBS = Wireless Reachback System. NMP = Navy Modernization Process.

daily—and can morph according to how cyber specialists choose to defend networks. As the DSB concluded, what is needed is a unique, incremental acquisition model for IT capabilities.

Within PEO C4I, PMW 130 is focused on rapidly and proactively fielding innovative capabilities to stay ahead of cyber threats. Due to technology refresh rates and quickly evolving threats from worms and other forms of malware, an acquisition speed of mere months (certainly not years) is required for effective cyber defense. PMW 130's goals include achieving acquisition and fielding cycle times that are sufficient to deliver (1) hardware cyber security products within 12–18 months to IOC; (2) incremental software cyber security products within six to 12 months to IOC; and (3) software patches in response to vulnerabilities within days or weeks.

PEO C4I and PMW 130 offices and personnel recognize that there are a number of challenges that hinder the responsive and rapid acquisition of cyber assets:

- timeliness of requirement approval
- excessive documentation requirements
- time-consuming contracting processes
- unstable funding and program objective memorandum planning
- lengthy testing, C&A, and installation processes.

Moreover, officials recognize that the afloat environment offers its own unique set of challenges, including ship availability scheduling. There are also the challenge of configuration management, change control, and the need for constant patching.

To remedy these challenges, authoritative entities, such as the National Research Council (NRC, 2010a, pp. 73–74) and the DSB (2009a, p. xi) have suggested more iterative and incremental acquisition. Others have suggested that traditional acquisition processes be sped up through a modified Joint Capabilities Integration Development System (the "IT Box") used specifically to meet the needs of IT programs that do not require hardware development. The process is currently in use in such Navy programs as the Distributed Common Ground/Surface System–Navy (DCGS-N) and Consolidated Afloat Networks and Enterprise Services (CANES).

Key Findings and Recommendations from the Analysis

The following is a summary of the primary key findings from our analysis. First, we focus on the major institutional and cultural changes that would contribute to the missions and goals of PMW 130, which, as discussed, is within PEO C4I and therefore any changes may affect the entire U.S. naval enterprise. We then present findings and recommendations specific to PMW 130.

In our view, PEO C4I and PMW 130 need at least two distinct acquisition processes that allow multiple processing speeds for C&A packages to meet cyber acquisition needs. A revised version of the current acquisition process would not be enough to create the highly responsive cyber procurement timeline that PEO C4I and PMW 130 need now. DoD acquisition processes are too lengthy and complicated, they can be streamlined only to a certain extent, and the current procedures in place for urgent procurement are limited.

New authorities at the PEO and PM levels are needed to address the assessment, validation, sourcing, resourcing, and fielding of operationally driven urgent requests. We found that iterative and incremental development for a program of record is conceivable on a six-month cycle but likely requires new PEO- and PM-level authorities to test and field requests on a preliminary basis. We propose a reimbursable funding mechanism that can handle uncertain but urgent cyber needs (as opposed to relying on a fixed budget that would be difficult to calculate several years out).

The Navy should segment processes according to time constraints. Acquisition processes may be divided into three groups according to their time requirements:

- acquisitions that must be complete in less than 30 days, such as virus definition updates, IAVAs, simple patches
- acquisitions that cannot exceed six months, such as productivity suite applications or operating system service packs or replacements
- acquisitions requiring longer than six months (and often much longer).

Fortunately, there is a strong correlation between the complexity of an action and the desired time to completion: Those needed soonest are often simplest.

Key Findings and Recommendations Specific to PMW 130

We found that iterative and incremental (or agile) development will be a challenge for PMW 130's CND program. The main issue is that current processes available to PMW 130 are not sufficient to keep ahead of the cyber threat. For less urgent, iterative acquisition, changes in

current acquisition processes (especially for C&A and installation) are necessary and sufficient. In addition, there are general design guidelines that will ease the acquisition burden for iterative development.

There is a need for a distinct process for emerging needs. Emerging needs should be handled through a separate process and budget.[4] We found that emerging needs generated from immediate threats, such as a new network virus, lie outside of the CND program of record and present a host of challenges, including those regarding resource availability. The 2009 Secretary of the Navy Notice (SECNAVNOTE) 5000 outlines one alternative mechanism for the Navy, but a U.S. Department of Defense Inspector General assessment of the process (2009, p. 18) found unnecessary confusion and delays due to incomplete guidance and procedures. A new acquisition process needs to be institutionalized to provide PMW 130 with the necessary authorities to urgently address emerging needs.

The C&A process needs attention. Changes to the current DoD 5000 acquisition process are required for iterative CND acquisition. Out of all the Navy acquisition processes we examined, we found that the C&A process is the most rigid long pole in the tent, and "information assurance certifications are consuming 30 percent to 50 percent of the IT development time" (Simpson and Langston, 2010, p. 74). Notably, CND can turn in perfect C&A packages, but there are still administrative roadblocks in the process, and, thus far, streamlining the C&A process has not been successful in reducing major wait times. The opportunity for improvement remains.

As shown in Table S.2, the C&A process includes multiple steps that vary from a few days to nearly a month for the programs we reviewed.

One of our specific recommendation regarding the C&A process is that PMW 130 should obtain dedicated test facilities and ensure that their dedicated personnel (i.e., the validator) are properly trained and adequately experienced. We found that programs that invested in well-trained, dedicated personnel (and test facilities) to push through certifications and accreditations were able to shorten their C&A timelines. Although these best practices help, more needs to be done to reduce the C&A process time. We recommended that the PMW 130 PM engage Space and Naval Warfare Systems Command (SPAWAR) and operational decision accreditation authority (ODAA) to change current business rules and create a new C&A tempo for CND and similar programs. According to our assessment, it is possible for a CND C&A package to go through all the required process steps within two months if the business rules governing the C&A package processing are altered. Finally, given how tight resources are in the C&A environment, we concluded that any further decrease in Navy C&A resources will further burden processing cycle time for CND.

In addition, we found that the Navy Ship Change and Installation process, or the NMP, is not set up to accommodate rapid technology change. Wait times are measured in months, and there is considerable variance throughout the process, as shown in Table S.3. The table shows the experiences of selected PEO C4I programs. While the sample size is small, it highlights the fact that actual installation times are minor compared to processing and wait times. Again, this demonstrates that there is room for improvement.

We were able to identify instances in which NMP was expedited; however, expedited cases require dedicated manpower that cannot be scaled to a broader level. We recommend

[4] An emerging cyber need requires a solution immediately (i.e., within hours or days).

Table S.2
Average Duration of Steps in the C&A Process

	IA Process Step				
Process Characteristic	**IA Testing**	**CA/ODAA C&A Package Review**	**E-Vote**	**CA Letter**	**ODAA Authority to Operate**
Participants	Information system security engineer or validator	CA liaison, ODAA	CA liaison, ODAA OA, Echelon II representative, program	CA	ODAA
Minimum time (days)	7	15[a]		1	2
Mean time (days)	20			10	8
Maximum time (days)	28		1	26	28

SOURCES: Interviews conducted with program and process personnel; data from the IATS database.

NOTE: Days are regular working calendar days. Information assurance (IA) testing provides data on potential vulnerabilities of the system's IA controls. The certifying authority/operational decision accreditation authority (CA/ODAA) review is used to determine whether the testing was sufficient and results were accurately captured. The e-vote is a short, formal meeting to review the test results before formal CA and ODAA review. The CA letter certifies that the risk statement resulting from the test results is accurate. The ODAA assesses whether the risks associated with the new information system are acceptable for operation in the network. .

[a] Current business rules affecting the PMW 130 C&A package review are set up to allow package processing in no more than 15 days. This may take more than 15 days only if there are resource constraints. We were unable to find empirical data on resource constraints that cause review times to exceed 15 days, however.

Table S.3
Average NMP Installation, Processing, and Wait Times for Five PEO C4I Programs

	PEO C4I Program				
Process Characteristic	**WRBS**	**AIS**	**CND**	**CBSP**	**SNR/HFIP**
Minimum time (months)	3.3	14.3	7	12.6	30.8
Maximum time (months)	8.7	21.5	28.1	47.3	40
Mean time (months)	5.1	16.8	17.6	30.3	35.4
Installation time (months)	0.6	0.4	1.9	4.4	4.0
Processing time (months)	3.8	8	10.1	18	14.5
Wait time (months)	0.7	8.3	5.7	8.1	16.8
Number of data points	5	6	15	4	2

NOTE: Installation time is the documented time from the beginning to the end of the system's physical installation on a ship. The processing time is the time from the beginning to the end of the approval process. Wait time is the time during approval processing in which nothing is happening, meaning that no one is actively working on that case. The three variables together constitute the total NMP time.

that programs submit a ship change document immediately when an installation is required. Programs should also utilize the NMP expedited process, which should take under 30 days. Stipulations for use include the need for a safety-related item, a mission-critical capability, or a solution to address critical software, firmware, or other deficiencies (i.e., Strike Force Interoperability Category 1 or 2). One barrier to the use of the NMP expedited process is that all required documentation should be completed before starting. This requirement is prohibitive to CND iterative cycle times. We recommend that PMW 130 work with the NMP to identify and make the necessary changes to the expedited process to meet required CND cycle times. Finally, program offices should work closely with all NMP approving authorities when an expedited need arises.

Iterative acquisition is in need of general design guidelines. To further alleviate some of the iterative acquisition challenges for CND, an initial "future-proof" design should be pursued to the greatest extent practical. However, it should be noted that generous design margins still will not alleviate issues of hardware obsolescence.

Ideally, changes to a system should be made through software upgrade "patches." To the greatest extent possible, programs should seek initial system designs that enable such software (and configuration) changes. These changes should be targeted at the operations and maintenance, Navy, phase. The advantage is in avoiding reaccreditation for NMP and C&A and thus expediting these processes. The CND capabilities production document allows enough flexibility in the technology insertion cycles between increments for PMW 130 to carry out these recommendations.

Acknowledgments

First, we thank the sponsors of this study, acquisition manager Christopher Newborn, deputy program manager CAPT Don Harder, and program manager Kevin McNally at PMW 130 for their guidance and for providing the means for us to undertake this research.

We received helpful input throughout this study from several DoD personnel and others. Specifically, we benefited from discussions with government personnel and contractors working for the Navy, including Gleason Snashall, IA manager, SPAWAR Systems Center Pacific; Penny Matter, director of configuration management and ship maintenance, PEO Integrated Warfare Systems; Patricia K. Mausert, assistant program manager, Deployable Joint Command and Control (DJC2); Norman Beebe, IA contractor handling C&A for DJC2; Leo Martinez, Booz Allen Hamilton, PEO C4I and Space Support; Marianne Chalut, Navy ODAA; Ann Hess, test and evaluation manager, PMW 130; Paul Hilton, SPAWAR; Bill Helmick, Navy/Marine Corps Internet; Scott Hetkey, PEO C4I, 67610, NMP Coordination; Christina LaRussa-Martin, acting afloat networks and data centers integrated product team lead and SPAWAR Systems Center, Atlantic, PMW 160 BAM (acting); Chuck Waterman, certifying authority liaison, Sentek Consulting; and Brent Hipps, PMW 130 validator, Booz Allen Hamilton. The contributions of these interviewees were important for our understanding of the many complicated parts of the traditional acquisition process. Josh Caplan, cyber portfolio business manager, SSC Pacific, also provided valuable advice and suggestions.

We would also like to thank Grant Wagner, technical director at the National Information Assurance Research Laboratory, and Charles Campbell, co-lead on the Acquisition Task Force in the Office of the Secretary of Defense, who provided us with their perspectives on issues outside the Navy. Larry Coe from Air Force Materiel Command's Electronic Systems Center at Hanscom Air Force Base also generously shared his ideas. We also extend gratitude to our reviewers for their insightful comments and suggestions. The manuscript benefited from the expertise of CAPT (ret.) Steven Sudkamp, U.S. Navy, and RAND colleague Bill Shelton.

At RAND, this research effort benefited from debate and discussions with a number of research colleagues, including Jeffrey Drezner, Charles Nemfakos, Christopher Pernin, Mark Arena, John Schank, Irv Blickstein, and John Birkler. We thank Cynthia Cook and Paul DeLuca for their guidance. We are particularly grateful for the support efforts provided by Michelle McMullen and Maria Falvo. Finally, we thank Lauren Skrabala for her careful editing of this document.

Abbreviations

ACAT	Acquisition Category
AFOM	alteration figure of merit
AIS	Automatic Identification System
A-RCI	Submarine Acoustic-Rapid Commercial-Off-the-Shelf Insertion System
ASN(RDA)	Assistant Secretary of the Navy for Research, Development, and Acquisition
BCL	Business Capability Lifecycle
C&A	certification and accreditation
CA	certifying authority
CBSP	Commercial Broadband Satellite Program
CND	computer network defense
COMPOSE	Common PC Operating Environment
COTS	commercial, off the shelf
DIACAP	U.S. Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DJC2	Deployable Joint Command and Control
DoD	U.S. Department of Defense
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
DSB	Defense Science Board
DT&E	developmental testing and evaluation
E2	Echelon II
EMD	engineering and manufacturing development

FIFO	first in, first out
FOC	full operational capability
GAO	U.S. Government Accountability Office
GCCS-M	Global Command and Control System–Maritime
GOTS	government, off the shelf
HBSS	Host-Based Security System
IA	information assurance
IATS	Information Assurance Tracking System
IAVA	Information Assurance Vulnerability Alert
IDIQ	indefinite delivery/indefinite quantity
IOC	initial operational capability
ISPAN	Integrated Strategic Planning and Analysis Network
IT	information technology
ITT	integrated test team
JCIDS	Joint Capabilities Integration Development System
MAIS	major automated information system
MDA	milestone decision authority
MDAP	major defense acquisition program
NaIL	Naval Innovation Laboratory
NMCI	Navy/Marine Corps Intranet
NMP	Navy Modernization Process
NRC	National Research Council
ODAA	operational decision accreditation authority
O&M	operations and maintenance
ONR	Office of Naval Research
OPTEMPO	operational tempo
OSD	Office of the Secretary of Defense
OT&E	operational test and evaluation
PEO	program executive office
PEO C4I	Program Executive Office for Command, Control, Communications, Computers, and Intelligence

PEO IWS	Program Executive Office Integrated Warfare Systems
PM	program manager
PMW	Program Manager, Warfare
PPBE	planning, programming, budgeting, and execution
RDC	rapid deployment capability
RDD	rapid development and deployment
RDDC	Rapid Development and Deployment Committee
RDT&E	research, development, test, and evaluation
REF	Rapid Equipping Force
RTT	Rapid Technology Transition program
S&T	science and technology
SCD	ship change document
SECNAVINST	Secretary of the Navy Instruction
SECNAVNOTE	Secretary of the Navy Notice
SNR/HFIP	Subnet Relay and High-Frequency Internet Protocol
SPAWAR	Space and Naval Warfare Systems Command
SPIDER	Program Executive Office for Command, Control, Communications, Computers, and Intelligence Space and Naval Warfare Systems Center/Program Executive Office Integrated Data Environment and Repository
TIPS	Technology Insertion Program for Savings
TRL	technology readiness level
UON	urgent operational need
USSOCOM	U.S. Special Operations Command
WRBS	Wireless Reachback System
WSARA	Weapon Systems Acquisition Reform Act of 2009

CHAPTER ONE

Introduction

In general, today's acquisition and testing system is designed for large-scale, hardware-based weapon systems. It is marked by high-level oversight and a deliberate, serial approach to development and testing. As a result, this current process (based on the U.S. Department of Defense [DoD] 5000-series regulations)—from requirements definition to initial operational test and evaluation (OT&E)—typically takes years to complete. Such a process is particularly unsuited for dynamically changing information technology (IT) systems. A Defense Science Board (DSB) study found that only 16 percent of all IT systems were on budget and on time, while 53 percent were both late and over budget, typically by more than 89 percent (DSB, 2000, p. 11).

Across the Program Executive Office for Command, Control, Communications, Computers, and Intelligence (PEO C4I), acquisition programs average 36 months from concept approval to initial operational capability (IOC) and eight to ten years to full operational capability (FOC). Within PEO C4I, the Navy's Program Manager, Warfare (PMW) 130, Information Assurance and Cyber Security Program Office, recognizes that this is not responsive enough for its customers in the cyber domain to adequately defend networks.[1] Threats and technologies evolve very rapidly, and policies are not yet agile enough to foster prompt and efficient responses. As the DSB review concluded, what is needed is a unique, incremental acquisition model for IT capabilities in which schedule is the priority (DSB, 2000, p. 27).

Mitigating the Cyber Threat Through Rapid Acquisition

Previous RAND research has shown that three speeds of cyber acquisition are needed to address the variety of threats that face DoD systems.

1. Days to weeks: Some threats, such as worms (e.g., Conficker, Stuxnet, Agent.btz), can evolve monthly and require an "emerging needs" acquisition process that can roll out solutions within days or weeks (Paul, Porche, and Axelband, forthcoming).
2. Six to 18 months: Due to technology refresh rates, acquisition speed on the order of months, not years, is required for cyber systems. This pace will help ensure that DoD systems keep up with the IT life cycle of commercial products.

[1] PMW 130 was established under PEO C4I in July 2010. PMW 130's primary mission is to maintain cyber security, and one of its challenges is the need to rapidly acquire and field materiel that provides cyber security.

3. Years: Acquisition of new IT systems requiring new development (i.e., those that are not commercial, off the shelf [COTS] or government, off the shelf [GOTS] systems) will follow the traditional acquisition cycle in a time-efficient manner.

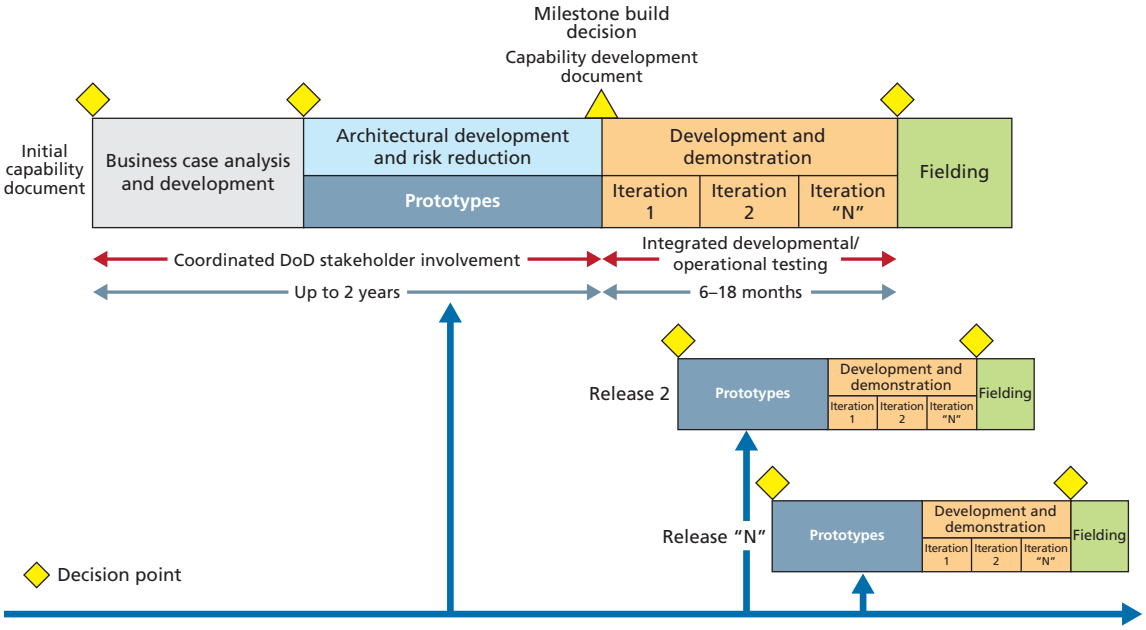
PMW 130 is focused on rapidly and proactively fielding innovative capabilities to stay ahead of the cyber threat, which requires processes for the first two cyber acquisition speeds listed here. Specifically, PMW 130's goals include acquisition and fielding cycle times that are sufficient to deliver (1) software patches in response to vulnerabilities (e.g., Conficker) within days or weeks, (2) hardware cyber security products within 12–18 months to IOC, and (3) incremental software cyber security products within six to 12 months to IOC. This six-month acquisition speed for incremental software products and 12–18 months acquisition speed for hardware products are captured in Figure 1.1, which reflects the recommendations of a National Research Council study (NRC, 2010b, pp. 73–74) and the previously mentioned DSB review (2009a, p. xi); both call for iterative and incremental development.

In addition, it should be noted that specific IT products may require different processes within each of these rapid cyber acquisition speeds (e.g., user software, intranet products, command and control products). PMW 130's main focus is computer network defense (CND) technology, so our findings and recommendations focus on the specific characteristics of its CND program. They could be applied to other types of programs where appropriate, however.

At this point, we note a number of challenges associated with cyber acquisition:

- the time it takes for requirements to be approved
- the large amounts of documentation associated with acquisition oversight
- a contracting process that is time-consuming

Figure 1.1
DSB-Proposed Model for Iterative and Incremental Development



SOURCE: DSB, 2009a, p. xi.

RAND *TR1294-1.1*

- issues related to stable funding and program objective memorandum planning
- testing and certification and accreditation (C&A)
- the installation process.

In addition, a number of considerations are unique to the afloat environment, including ship availability schedules and configuration management or change control and patching.

This list suggests that the business processes affecting new technology development and introduction require the kind of close evaluation that elicits actionable policies and will enable PMW 130 to quickly prioritize needs, make decisions about solutions, and allocate resources in a manner that meets current and anticipated cyber threats.[2]

Study Approach

To help PMW 130 move toward developing a more agile acquisition process, RAND conducted a study of how best to enable continuous IT technology and requirements development. More specifically, in this report, we present a number of acquisition-related best practices, demonstrate some applications of innovative practices, and put forward recommendations for changes in processes and procedures in response to the following questions:

- What are the existing authorities, processes, and organizations that can be used to support PMW 130's rapid acquisition objectives?
- What new authorities, processes, or organizations are needed to support PMW 130's rapid acquisition objectives?
- What are recommendations for building or leveraging a dynamic OT&E environment?
- How can budgeting and resourcing challenges to agility be mitigated?

As we answer these questions throughout this report, we also provide a series of recommendations to streamline the DoD 5000-series acquisition process for rapid acquisition of IT. This streamlined process will enable PMW 130 to rapidly and proactively field innovative capabilities that will keep it ahead of the cyber threat. As part of the study, we considered testing, C&A, ship modernization, budgeting and funding, contracting, governance, and integration and training.

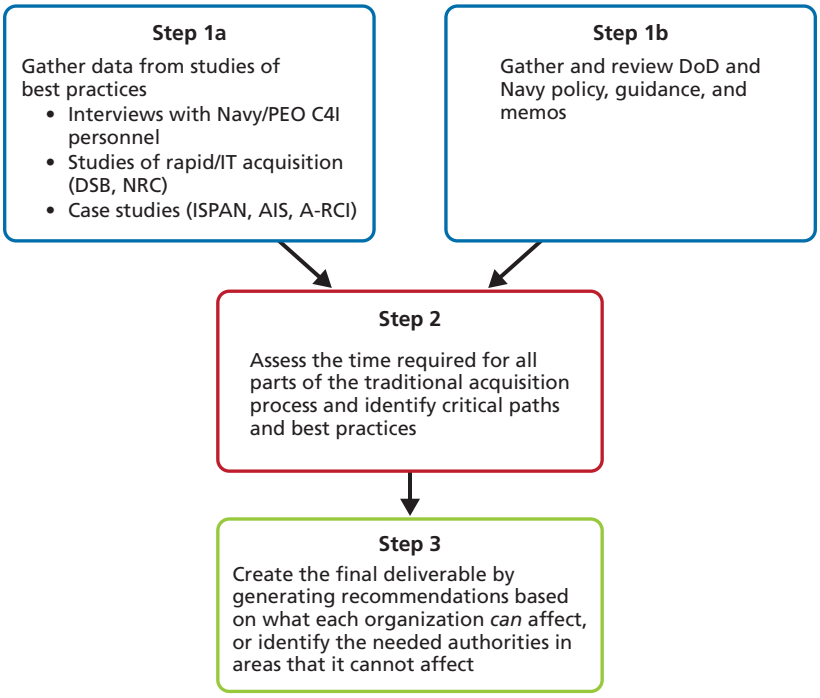
The research approach involved a review of a mix of current acquisition studies, interviews with individuals currently involved in the acquisition process, and a series of case studies. Our study approach was three-pronged, as shown in Figure 1.2.

Step 1a: Documentation of Best Practices for Rapid Cyber Acquisition

We first conducted a substantial literature review that revealed that all the services and U.S. Special Operations Command (USSOCOM) have developed urgent acquisition processes to meet emerging needs. The 2009 Secretary of the Navy Notice (SECNAVNOTE) 5000 outlines one such mechanism. It has been proposed that such processes, including the use of an

[2] We had expected that problems might have arisen from the application or interpretation of Federal Acquisition Regulations or Defense Federal Acquisition Regulations, which has been the case in other programs. But this was not true for PMW CND programs; thus, we discuss them no further.

Figure 1.2
Study Approach



NOTE: AIS = Automatic Information System; A-RCI = Submarine Acoustic-Rapid Commercial-Off-the-Shelf Insertion System; ISPAN = Integrated Strategic Planning and Analysis Network.

RAND *TR1294-1.2*

operations and maintenance (O&M) process and controls, hold value for the Navy, and we considered them in our project as options to speed acquisition and fielding times for PMW 130. The primary sources that we explored included the following:

- congressional testimony on acquisition reform
- official Navy program office briefings
- briefings and reports from the Office of the Secretary of Defense (OSD)
- Air Force, Army, and Marine Corps briefings on similar issues
- U.S. Government Accountability Office (GAO) reports
- DSB reports
- DoD Inspector General reports
- NRC reports
- directives, laws, and guidance on IT acquisition and the Navy's rapid acquisition processes
- annual reports from the Office of the Director, Operational Test and Evaluation
- major automated information system (MAIS) program annual reports
- Naval Postgraduate School documents
- prior RAND studies
- trade literature.

Step 1b: Review of Current Policy, Guidance, and Memos Related to Cyber Acquisition

In conjunction with the literature search, we examined current DoD and Navy policies, guidance, and memos related to cyber acquisition. A dynamic component of this step was following the current developments of the new IT acquisition process. Prior to the beginning of this study, Congress passed the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84), which adopted the IT acquisition process proposed by the DSB and also directed OSD to develop a plan to implement this new process. We analyzed the implications of this pending IT process for PMW 130 and current DoD and Navy policy. We also identified processes that PMW 130 could use to streamline cyber acquisition, the specific policy constraints to cyber acquisition, and the authorities to engage to remove identified constraints.

Step 2: Identification and Assessment of Critical Paths in CND Acquisition

In conjunction with the literature review, we also conducted a series of interviews with various program office personnel in the Navy, contractors, OSD personnel working on IT acquisition reform issues, National Security Agency personnel with an understanding of IT acquisition, PEO C4I acquisition process experts, and RAND subject-matter experts. The output from these interviews aided in our understanding of current cyber acquisition challenges and solutions specific to PMW 130. With information from the literature and our interviews, we were able to propose new authorities, streamlined processes, and organizational changes required to support PMW 130's rapid acquisition needs. These recommendations, presented later in this report, were shared with PMW 130 through a series of interim program briefings to PMW 130.

Step 3: Actionable Recommendations for PMW 130 (Processes and Authorities to Achieve Effective Cyber Acquisition)

The third part of the study methodology involved looking at various case-study programs with needs similar to those of PMW 130's main program, Computer Network Defense (CND). Specifically, we looked in detail at ISPAN, A-RCI, and AIS, along with various aspects of several PEO C4I rapid acquisition programs. These case studies allowed us to synthesize the obstacles and solutions for quickly acquiring and fielding IT programs in today's acquisition environment. We then gleaned challenges, best practices, and lessons learned from the literature, interviews, and case studies.

Finally, we identified actionable recommendations for PMW 130 and similar cyber acquisition programs. Some of the specific recommendations resulting from this study focus on testing and information assurance (IA) processes. Specifically, we developed recommendations for how to build or leverage a dynamic operational test environment that can support rapid acquisition. A key part of the acquisition process is the OT&E of programs under development. Recent studies (see NRC, 2010a, p. 14; DSB, 2009a, p. 63) highlight the need for continuous user testing (e.g., allowing frequent user feedback). We suggest that OT&E, as done today, can become a major burden and an obstacle to the rapid operational tempo. It is treated as a final exam that must be passed prior to fielding. OT&E should actually be an iterative process executed throughout the acquisition of a given program. Some estimates indicate that test times of eight months are not unusual. In this study, we explored options for enabling the iterative, continuous user testing sought for future PEO C4I and PMW 130 iterative developments. It also considered the efficacy of proposals to develop rapid technology testing and evaluation laboratories to enable more rapid acquisition.

We identified other actionable recommendations to address ship installation, budgeting, and resourcing issues associated with agile and evolutionary acquisition. By some accounts, a stable budget profile is needed to support multiple increments for iterative, incremental development. This may mean that there is a need for continuous streams of support for procurement, operations and support, and research, development, test, and evaluation (RDT&E). We considered this need and what it means for a PEO C4I/PMW 130 effort to support the rapid, incremental acquisition of IA and cyber security software and hardware.

We came to the conclusion that changes are needed to streamline lower-level approvals, reduced the number of milestones in these programs, reduce documentation requirements, and better coordinate the various steps in the acquisition process. Changes to policy and doctrine are also needed to establish the permanent processes that will enable PMW 130 to carry out its mission.

Organization of This Report

The next four chapters provide a more in-depth look at various problematic steps in the overall acquisition process for cyber programs. Each chapter discusses the challenges, best practices, and recommendations associated with the processes, starting with the most problematic: testing (C&A). Another challenge that is potentially difficult to navigate is the Navy Modernization Process (NMP), discussed in Chapter Three. Budgeting, funding, and contracts are covered in Chapter Four, and governance, integration and training, and emerging needs are addressed in Chapter Five. Chapter Six addresses some of the specific questions and answers tasked at the outset of this effort.

This report also includes seven appendixes. Appendix A surveys major rapid acquisition processes across DoD. Cyber acquisition has needed to use these processes to confront emerging threats in the absence of institutionalized rapid cyber acquisition. Following this survey at the DoD level, in Appendix B, we look more specifically at Navy processes that program offices can use in the event of an emerging need. We then present three case studies on rapid acquisition—one each from the Navy, Army, and Marine Corps—along with respective lessons learned in Appendix C. Appendix D provides background information on the Joint Capabilities Integration Development System (JCIDS) and incremental acquisition, as well as the "IT Box," which is a streamlined JCIDS process for IT programs. In Appendix E, we present an overview of the information we reviewed for this study. We examine the Air Force's effort to institutionalize cyber acquisition in Appendix F. Finally, in Appendix G, we review the threat from worms, a partial motivation for the rapid cyber acquisition need described in this report.

CHAPTER TWO

Testing (Certification and Accreditation): Challenges, Best Practices, and Recommendations

In this chapter, we outline the challenges that C&A and operational testing pose to PMW 130's CND program and provide specific recommendations to overcome them.[1] The bulk of the chapter focuses on required changes in the C&A process to meet the six-month acquisition requirements for CND updates, which fall within the second acquisition speed category listed in Chapter One. We briefly discuss the required changes to the C&A process for handling emerging threats (e.g., worms), which falls into the first acquisition speed category (days or weeks).

Challenges

The DSB task force report on acquisition of IT proposed general testing guidelines to accompany the new IT acquisition cycle. First, it stressed the necessity of testing; specifically, "comprehensive testing . . . is required" (DSB, 2009a, p. 50). Furthermore, "a robust testing program must also be established to minimize the introduction of new vulnerabilities." The board did acknowledge that testing had to be done differently to meet the six- to 18-month release cycle time:

> Test planning, test execution, and post deployment support cannot be based upon traditional thinking that scope and content is fixed at the beginning. Instead of a single test event, acquisition activities rely on development test events after each iteration and operational testing to support decisions to field the release. An especially important planning consideration is the use of automated testing to allow effective iterative testing of previous functionality. (DSB, 2009a, p. 53)

The National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84) directed the Secretary of Defense to "develop and implement a new acquisition process for information technology systems" based on the recommendations of the DSB report (OSD, 2010, p. 2). The Secretary of Defense provided a report to Congress on the implementation of this new acquisition process. The overriding principle is that government IT acquisition will closely follow commercial IT cycle times. At a few points, that report also discussed testing. First, it stated

[1] The many different Navy IT technologies must go through the same C&A process steps in most cases. Here, we examine the C&A process for PMW 130's CND program and make specific recommendations for this program. Other programs, such as the Navy/Marine Corps Intranet (NMCI) or the Deployable Joint Command and Control (DJC2) system may warrant different recommendations. Such a review was outside the scope of our study.

that testing and evaluation "will be structured to support iterative and incremental delivery" (OSD, 2010, p. 10). It advocated the use of integrated testing and test automation to accomplish testing for iterative and incremental delivery.

The DSB and Secretary of Defense reports provide encouragement to the IT acquisition community but do not specify any new authorities for program managers (PMs). Currently, a number of prototype programs are being tested with this new acquisition strategy, and there is a schedule to implement the proposed changes (OSD, 2010, p. 17). It was announced that OSD would include four IT templates in a planned revision of DoD Instruction 5000.02 (2008). A draft was to be completed by the end of September 2012, after our study was completed. The revision will include a streamlined test, evaluation, and certification process for IT programs (Mishory, 2011). IT PMs still face the perplexing challenge of navigating the four independent tests required of IT technology, but the latest revisions to the traditional acquisition process may provide some relief.

Our initial assessment of these four testing activities found that C&A and operational testing will be the most troublesome for PMW 130. Using CND's required cycle time as the objective, we examined each step of these test processes. We derived our detailed assessment from interviews with Navy subject-matter experts who were directly involved in the particular step, as well as outside experts and staff from programs that have successfully streamlined IT testing. We also examined quantitative data from Navy databases and portals. The analysis presented here identifies the timing of each step and associated hurdles. We then developed recommendations that can be implemented by the PM to streamline these testing processes within the confines of DoD and Navy policy. For the remaining hurdles that will prevent PMW 130 from meeting its acquisition schedule, we identified specific authorities that the program must engage to enact the remaining recommendations.

CND Testing Time Requirements

Cycle time requirements for CND necessitate fielding new capabilities every six months. Within this six-month cycle, four months are needed for development, which leaves two months for testing. This six-month cycle fits into the new IT acquisition cycle because the development and demonstration of a release is anticipated to take between six and 18 months, according to the new proposed process. Each new instantiation of CND can be considered a new release or iteration. There are three iterations per release. The latter perspective will most likely work better, as described later.[2]

Historical IT Testing Cycle Time

The current times required for IT testing will not support the CND six-month cycle time. A survey of 32 MAIS programs found that OT&E took an average of five months (Hutchison, 2010, p. 22). Although CND may not fall within this class of IT systems, test result documentation for OT&E will take 60 days for CND and similar programs in the Navy, according to one interviewee. Producing the documentation for OT&E alone will devour the two-month

[2] Three acquisition speeds are required for IT. Here, we focus on the middle speed that requires iterative capability to be fielded approximately every six months. Patching requires the fastest acquisition speed of mere weeks. PMW 160 (Tactical Networks) has an established process for this, which waives certain C&A processes. The third speed is for new IT development and follows the traditional acquisition process. We focus on the middle speed because this was the largest obstacle for our sponsor.

test window. IT systems are required to be certified and accredited. According to another interviewee, a well-designed and executed C&A process will average three months and can take longer if issues persist. These IT testing time requirements pose barriers to the rapid acquisition of IT technology.

The Certification and Accreditation Process

IA C&A is the process to ensure that an information system can provide a secure, interoperable, net-centric information management environment. The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the formal process by which an information system receives permission to operate on a DoD network. DIACAP's purpose is to ensure that the system has the appropriate set of IA controls and that they work properly (DoDI 8510.01, 2007, p. 2). On rare occasions, waivers may be requested for exceptional circumstances.

DIACAP as followed by the Navy can be summarized in a handful of simple steps. The first two—compiling the DIACAP implementation plan and the first round of coordination (concurrence on the implementation plan)—occur during development.

Early in the development phase, the program should compile a DIACAP implementation plan. The plan contains several documents that describe the system, its IA controls, and how those controls will be tested (U.S. Department of the Navy, 2008). Compiling the DIACAP implementation plan allows key players in the C&A process to become familiar with the new information system, ensures that the proper IA controls are incorporated into the design, and helps stakeholders verify that proper testing is planned. Programs that bypass the DIACAP implementation plan are at higher risk of costly redesigns and of having to go through the accreditation process multiple times.

The second step in the Navy's DIACAP process is the first coordination. The first coordination is a formal meeting organized by the Echelon II (E2) representative,[3] with representatives from the certifying authority (CA) and operational decision accreditation authority (ODAA). The outcome of this meeting is the approval of the program's IA controls and IA test plan. This approval is known as "DIACAP implementation plan concurrence."

The main C&A activities completed during testing are as follows:

1. *IA testing.* The first step in this phase is the actual testing of IA controls. In theory, the information system security engineer will conduct the test and the validator will validate the results and make a risk assessment.[4] The purpose of IA testing is to determine the potential IA risks of the new information system.
2. *CA/ODAA package review.* The results are compiled in the C&A package and uploaded to the IA Tracking System (IATS) portal. CA and ODAA representatives then review the C&A package compiled by the validator in the second step and provide a thorough review of the IA testing and risk assessment. Communication among these parties (i.e., validator, CA representative, and ODAA representative) may be required at this stage to obtain clarification, implement corrections, or conduct additional testing. A program

[3] The E2 representative is the official responsible for IA in the program's echelon. For PMW 130, the E2 is Space and Naval Warfare Systems Command (SPAWAR) 8.2.

[4] In the Navy, the program is responsible for supporting its validator and information system security engineer. Often, the validator will play both roles. According to an interviewee, because the validator is a trusted agent of the CA, the CA will appoint the validator for the program.

that does not receive DIACAP implementation plan concurrence may discover that the proper IA controls were not included or tested for.

3. *E-Vote.* After the C&A package is reviewed, a formal coordination meeting is organized by the E2 representative. During this meeting, the C&A package is accepted by the CA, ODAA, and E2 representatives through a process called the "e-vote."[5]
4. *CA Letter.* After the e-vote, the Navy CA examines the C&A package and issues a letter.
5. *ODAA-I/authority to operate.* At this point, the ODAA makes the final accreditation decision. The CA and ODAA process the acquisition packages on a first-in, first-out (FIFO) basis, though the ODAA has the authority to prioritize packages.

Business Rules and Length of Individual Steps in the IA Process

The primary aim of our study was to identify hurdles in the critical path of cyber acquisition. To this end, we specifically analyzed each step in the C&A process, determined the likely minimum and maximum times required to complete the step, and identified the issues that were likely to cause undue delays. These estimates were derived from interviews with program and process personnel in the Navy, along with IATS data. With this information, we were able to develop estimates for how long the individual steps in the C&A process are taking for Navy programs. Table 2.1 lists the major steps in the IA process and their approximate length.

IA testing can range from one to four weeks, depending on what is being tested, the competency of the validator, and the availability of testing facilities. The CND validator with whom we spoke estimated that IA testing would take approximately 20 days.

The timing of the C&A package review (the second step) and the e-vote (the third step) is somewhat complicated and is driven by CA resources and E2 business rules. The review of the C&A package is coordinated through the E2 representative. Each E2 representative has business rules concerning the processing of the C&A package (for CND, the E2 is SPAWAR 8.2). For programs under SPAWAR's purview, requests for an e-vote coordination meeting must be submitted a maximum of 30–45 days in advance. A program does not need to complete testing before this request is made, but it must have its testing completed and C&A package uploaded 15 days prior to the scheduled coordination meeting. SPAWAR uses a FIFO paradigm to assign packages to available coordination meeting time slots. CA and ODAA representatives are shared across the Navy, and they also use a FIFO paradigm to process packages. SPAWAR limits its weekly number of collaboration meetings to six in order to match the processing speeds of the CA and ODAA representatives.

On the table is a set of proposed changes to the current business rules. According to an interviewee, SPAWAR is currently considering revising its scheduling rules to accept collaborative meeting requests a maximum of 60–90 days in advance to accommodate limited CA resources.

We examined IATS data across CND, DJC2, COMPOSE (Common PC Operating System Environment), and other programs to assess CA and ODAA timing. We found that the wait for CA assessments ranged from two to 26 days, and the wait for ODAA assessments ranged from two to 28 days. NMCI has found it safe to schedule two weeks for CA assessment and two weeks for ODAA assessment, though backlogs can add to the time required.

---

[5] The e-vote is a formal meeting organized and chaired by the E2 representative to determine whether a C&A package can move forward to CA and ODAA review.

Table 2.1
Information Assurance Process Steps and Estimated Length

	IA Process Steps and Estimated Length				
Characteristic	**IA Testing**	**CA/ODAA C&A Package Review**	**E-Vote**	**CA Letter**	**ODAA Authority to Operate**
Participants	Information system security engineer or validator	CA liaison, ODAA	CA liaison, ODAA, E2 representative, program	CA	ODAA
Minimum time (days)	7	15[a]		1	2
Mean time (days)	20			10	8
Maximum time (days)	28		1[b]	26	28
Description	PMW 130 validator estimates that IA testing will take 20 days; DJC2 could be tested in 7 days; NMCI schedules 4 weeks for testing.	SPAWAR business rules require the complete C&A package to be posted to IATS 15 days before the e-vote. New business rules are being considered by SPAWAR that will improve timing.	Formal collaboration meeting	Data from CND, DJC2, COMPOSE in IATS	Data from CND, DJC2, COMPOSE in IATS

SOURCES: Interviews conducted with program and process personnel; data from the IATS database.

NOTE: days are regular working calendar days.

[a] Current business rules affecting PMW 130 C&A package review are set up to allow package processing in no more than 15 days. This may take more than 15 days only if there are resource constraints. We were unable to find empirical data on resource constraints that cause review times to exceed 15 days, however.

[b] The e-vote can be considered a C&A milestone and consists of only a short meeting.

Overall, it appears that the C&A process can be executed well within the two-month testing window for CND if all the minimum times are closely achieved, but this has not been realized historically for the programs that we reviewed.[6] For programs with effective C&A strategies, this process still takes an average of three months, according to an interviewee. The critical point in the process is the scheduling of the e-vote. With a limited number of coordination meeting slots available, the e-vote becomes a bottleneck in the C&A process, potentially causing long wait times.

Much has been done to improve the Navy C&A process, but more is required to accommodate the timing needs of the Navy's various information systems. In the spring of 2008, the Navy implemented the recommendations from a Lean Six Sigma study to improve its C&A process. A major accomplishment was the reduction of the process from 28 steps to nine (Naval Network Warfare Command, 2008, p. 1). This new process has improved the reaccreditation rate by getting the CA and ODAA involved earlier.

Currently, C&A operates at two speeds. There is the traditional speed used for all information systems, described in detail in Chapter One. Then, there is the schedule for emerging needs. For example, the Navy required additional communication capabilities for its response to the January 2010 earthquake in Haiti. This new capability extended the architecture boundary of a particular IT system, which would have required reaccreditation. Program and ODAA representatives discussed this issue via a phone conference and, afterward, the ODAA issued a letter allowing the new system to be installed. Testing, review by CA and ODAA representatives, e-vote, and the CA letter were bypassed.

The standard C&A process works well for programs with long cycle times between accreditation (traditionally three years). For example, NMCI requires its supplier to have a new package ready 70 days before its authority to operate will expire. This gives the program sufficient time to process the C&A package through all the steps described earlier. This traditional pace does not work for programs like CND. Due to the active and continually changing nature of cyber warfare, it is anticipated that CND capabilities will need to be updated every six months. This will potentially require CND to transverse through three months or more of C&A to field a capability to protect Navy networks from cyber attacks. Other programs, like Automated Digital Network System, are facing a similar predicament.

The ODAA has the authority to direct the CA and E2 representative to prioritize processing for CND. One way is for the ODAA to ask them to drop everything and process the priority package immediately; alternatively, the ODAA can set a deadline for package processing. Priority processing of packages is rarely done, since it is very disruptive to the Navy C&A process. When it does occur, it is usually the result of flag-level prodding.

Despite Navy efforts to streamline the C&A process in the 2008 Lean Six Sigma study, it remains CND's most significant test obstacle. C&A continues to be problematic for a variety of reasons:

- Thousands of requests must be processed by limited C&A staff.
- This factor increases the lead times required for coordination meetings (i.e., SPAWAR has had to reduce the number of coordinations per week from eight to six because there are limited CA staff).

[6] We reviewed the following programs: DJC2, NMCI, and CND. There are ways to expedite the C&A process for urgent operational needs, but historically this has rarely happened and is unsustainable for iterative developments.

- The SPAWAR, CA, and ODAA FIFO processing paradigm prohibits faster processing times.
- Prioritization is very difficult under current business rules and often requires flag-level involvement.
- Prioritization is disruptive to the rhythm established by SPAWAR's current business rules.
- The CA and ODAA are under two different E2 commands.[7]
- The CA and ODAA offices are in time zones that are three hours apart, limiting the available coordination time.
- There is a lack of qualified and experienced personnel across the C&A process (e.g., validators, CA reviewer, ODAA reviewer), according to current DoD standards.

Recommendations

Despite the C&A challenges identified here, we believe that C&A may be expedited for six-month CND iterations if the following recommendations, based on best practices, are implemented:

Establish business rules that harmoniously allow two processing speeds for C&A packages. We recommend that policymakers create specific business rules that will accommodate the six-month iterative CND acquisition timelines (the second cyber acquisition speed described earlier) in a way that does not disrupt the C&A of established programs that fall within the traditional acquisition category (the third cyber acquisition speed). C&A business rules are established based on the flow of packages and resources to process the packages. Because CND acquisition is expected to have steady iterations (i.e., every six months), processing CND C&A packages under business rules that decrease the required lead times should not be disruptive to the overall process. These proposed business rules are not applicable to emerging cyber threats (e.g., Conficker worm), which requires acquisitions to be completed within days or weeks (the first acquisition speed).

If the current process is to improve, it will be necessary to change the business rules for the E2 representative and CA and ODAA. The chokepoint in the process is the E2 representative. E2 scheduling rules are set to accommodate the resource limitations of the CA staff based on the flow of packages. Programs approaching their three-year accreditation or new programs following the third (traditional) acquisition speed have greater lead times than programs like CND. Business rules can be established that still require the 30-day scheduling request (to give SPAWAR time to schedule and reschedule) but allow testing to be completed ten days before the e-vote collaboration instead of 15. (SPAWAR is in the process of increasing these requirements.) With the 30-day notice, the CA and ODAA representatives will know that the C&A package is coming and can schedule time in the ten days for its review instead of examining it in the FIFO queue. Following the e-vote, it is up to the CA and ODAA to process the package. These organizations will need to review their processes and determine how to accommodate

[7] The C&A process requires extensive communication and coordination among the players involved. There is lost opportunity for C&A synergy with the ODAA and CA in different E2 commands. Historical examples provided by an interviewee for this study showed that it only takes a simple personnel or management change in one of these commands to disrupt a program's ability to efficiently process their C&A packages.

two processing speeds. For emerging needs, it is possible for the program to bypass the e-vote and CA processing and work directly with ODAA.

Directly engage with the ODAA and SPAWAR. First, the risk of delayed CND fielding should be assessed by the ODAA to establish an appropriate C&A cycle time. Second, the ODAA should establish criteria for programs that should be processed according to this new C&A cycle time. Third, directions should be given to the E2 and CA representatives to adjust scheduling rules to accommodate the new cycle time. All these steps are within the ODAA's authority to establish priority (Schoberg, 2007, p. 1). Next, SPAWAR should be engaged to adjust its business rules to accommodate the new C&A processing speed. Now is a prime opportunity for this engagement, since SPAWAR is in the process of making changes to its scheduling rules. These changes will allow CND and programs with similar needs to pass through the C&A process more quickly, but these changes do not address the C&A resource constraints.

This recommendation is designed for the nature of PNW 130's CND program and its iterative acquisition characteristics. It is important to consider the properties of the software before considering this approach as a mechanism to compress the C&A process for other types of cyber acquisitions. It will, in effect, create a family of software types and specialized C&A processes. It is possible that C&A for Microsoft Office® programs and C&A for network software can both benefit from respective specialized C&A. This approach should be explored with caution, however, because the benefits must be understood and validated and the number of specialized C&A processes must be kept tractable.

Authorize the PM to attend to emerging acquisition needs by approving all required C&A activities and coordinate with the ODAA. Countering emerging issues, such as newly discovered viruses and worms, could benefit from having most requirements defined prior to discovery. Requirements could be written in advance, with a few exceptions (for example, "Correct the buffer overflow vulnerability in . . ."). Contracting vehicle processes, such as prequalified vendors, U.S. General Services Administration Schedule 70 approaches, and indefinite delivery/indefinite quantity (IDIQ) contracts, exist to allow for quick implementation.

Moving the C&A approval process outside the established business rules to give priority to some items is disruptive. We recommend that the development plan include elevated priority designation from the onset, which should allow the program to adjust the C&A approval agenda sooner, resulting in less impact on the overall approval process. The most urgent items can be approved outside of the normal process (as in the Haiti example). We recommend that the PM determine which C&A activities are required depending on the situation and the risks that are posed by these preestablished situations. The PM would then coordinate with the ODAA.

This recommendation aligns to what is occurring in PMW 160 with regard to its Information Assurance Vulnerability Alert (IAVA) patching. Preapproved waivers expand existing streamlining to cover more and could reduce the number of approval boards, as in the NMP process. The strong implementation of preapproved waivers should allow more activities to be carried out in parallel rather as a series, and this should also be decided during the development planning.

Obtain and maintain dedicated test facilities for use by PMW 130. There are two routes available for establishing dedicated test facilities. The program could establish and run its own test facilities, or the program could utilize the vendor's test facilities, thus outsourcing

the testing. Both the DSB and the Secretary of Defense have advocated continuous and automatic IT testing, which requires dedicated facilities (OSD, 2010, p. 10; DSB, 2009a, p. 53).

When a program depends on shared facilities, the timing between when the program is ready for IA testing and when the test facility is available may not align. It takes time for a facility to build up to the needs of a program, and, after program tests, it must tear down for other program testing. IA testing for CND is anticipated to occur at least twice a year. Additional testing may be needed to support emerging needs to counter unanticipated cyber threats. A natural solution is for CND to have its own dedicated testing environment. DJC2 has its own testing environment and has been able to release capabilities quarterly. Having control of its testing facilities has also increased confidence in the program's relationship with the ODAA representative, who has personally toured the facilities.

The second option, utilizing the vendor's test facility, is usually practiced in commercial IT software or hardware development. For example, the NMCI contractor owns and operates the NMCI test facilities with validator oversight, an arrangement that has reduced timing uncertainty in processing NMCI C&A packages. NMCI has also shown that dedicated facilities reduce uncertainty in processing C&A packages. To successfully utilize a vendor's test facilities for C&A processing, the vendor must be competent in DIACAP processes and procedures. The key to successful testing with a dedicated test facility is to develop and maintain a trust relationship with the ODAA representative. It may also be appropriate to supplement personnel and make up for other resource shortfalls by contracting with the vendor where it possesses the required capability.

Most of the vendors that develop products for DoD have extensive test capabilities. Some contracts could require testing to be done by the vendor, which would have to firewall the DoD-required testing from other processes in its operations. DoD has processes that allow vendors to test and certify critical components (including software) for aircraft, submarines, nuclear propulsion plants, nuclear weapon systems, medicines, medical supplies, medical devices, and other acquisition programs. Some vendors, in some instances, do better than DoD testers. Of course, government oversight and coordination would be required for vendor testing. In fact, one problem that the government sometimes faces is that oversight personnel have inadequate expertise compared to the vendor's personnel. Testing and the time involved present great difficulties to improving the overall acquisition process; thus, PMW 130 should expand the team with vendors where appropriate. Such an arrangement may allow some (or more) testing to occur in parallel with development.

When testing is outsourced, the CA's role would be to review and approve the test plan and the results of the tests. Appropriate processes can be put in place to ensure the independence of vendor testing from its production activities. Vendor testing is now done on a wide range of items acquired by the Navy, including medicines, submarine components, and weapon components. Smart vendors will innovate to do some testing in parallel with production while maintaining test independence. The looming budget environment will make getting more capable Navy testing a hard sell that will likely take years to accomplish.[8]

Create a dedicated CA staff position. PMW 130 could obtain dedicated CA liaison staff or part-time staff, or it could share with another program. Having a single, dedicated CA

[8] According to CAPT (ret.) Steven Sudkamp in comments on an earlier draft of this report, April 10, 2012.

staff member makes sense for large programs, like NMCI, which processes 2,000 packages per year; it makes less sense for CND, which will process approximately two per year.[9]

Currently, CA resources are constraining the C&A process. In fact, in January 2011, SPAWAR reduced its weekly collaborations from eight to six because of insufficient CA resources (SPAWAR, 2011). In addition, according to interviews conducted for this study, CA representatives (i.e., CA liaisons) are understaffed by approximately 30 percent. Programs can pay for their own CA and ODAA representatives to avoid delays in C&A processing, as demonstrated by NMCI.

[9] Although the size and complexity of the information system will determine the time required to review the C&A package, the number of packages that a program will process will be a decent indicator of the level of support required.

CHAPTER THREE

The Navy Modernization Process: Challenges, Best Practices, and Recommendations

The Navy currently conducts ship changes through the Navy Modernization Process, or NMP. Previously called SHIPMAIN, for "ship maintenance," this process was implemented to eliminate redundancies in prior maintenance processes by standardizing the planning, budgeting, engineering, and installation of shipboard improvements (Penderbrook Associates, undated).

The NMP also seeks to "maintain configuration control of the various changes made to ship systems and equipment over the life of a ship" (Schank et al., 2009, p. xviii). Despite intended efficiencies, the NMP is a long and complicated process; programs have been affected by its long-standing structural and (more recently) institutional problems resulting from a loss of experienced personnel. For example, the time needed to put a piece of equipment on a Navy ship averages 36 months—and the clock starts only once a contractor is in the pipeline for review (Grace, 2011).

Cyber acquisition programs, like PMW 130's CND, are particularly concerned with processes that can inhibit the program office's ability to provide current technology and security to Navy ships, submarines, and other vessels. Our research has found that NMP, like C&A, is an impediment to keeping the most up-to-date computing and communication technologies on in-service ships. This finding echoes evidence presented in earlier RAND research (see Schank et al., 2009).

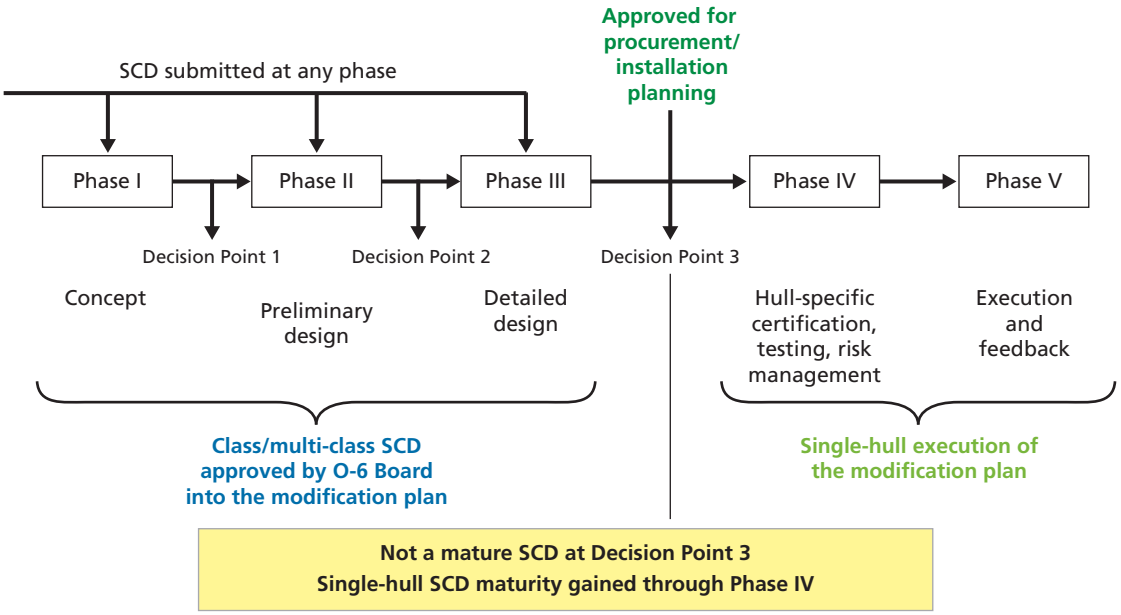
This chapter looks in more detail at the challenges that cyber programs face during the NMP. It also provides real-world data for several PEO C4I acquisition programs to determine how long the process currently takes. Finally, we share some best practices used by other programs to navigate the process, along with actionable recommendations for PMW 130, since it will use this process to enable the installation of cyber security solutions.

Challenges

We identified five challenges faced by cyber programs when entering the NMP.

The length of the NMP is mismatched to technology turnover. The NMP has many steps and typically requires approximately 30 months. It is a "five phase process with decision points at phases I–III" (PEO C4I, undated, p. 2). The five phases are Preliminary Analysis, Concept Design, Design Development, Ship Integration, and Feedback and Reporting. The first three phases require a ship change document (SCD) submission. Figure 3.1 shows the major phases and decision points in the modernization process; it is simplified to highlight the major phases and so does not show the individual steps in each phase.

Figure 3.1
PEO C4I Ship Modification Process



SOURCE: PEO C4I, undated, p. 2.

RAND *TR1294-3.1*

Part of the decisionmaking process for PEO C4I ship modification involves an "O-6 board" that reviews all SCDs. For SCDs over $50 million, once the board has approved, the SCD will move to a one- and two-star board for final approval. For SCDs over $200 million, once both boards have approved, the SCD will move on to a three-star board for final approval. These approvals occur after each phase of the SCD (Phase I, II, and III). The three boards are composed of representatives of the Fleet and the Office of the Chief of Naval Operations.

The program's technology would most likely change in the length of time it takes for a program to navigate the NMP. This is one of the main reasons that NMP "is typically viewed as too difficult and too time-consuming to implement during C4I upgrades" (Schank et al., 2009, p. xviii). The addition of a new capability during the NMP time frame would require a program to redo its SCD, potentially creating an even longer process.

NMP complexity requires program offices to have personnel with knowledge of the process. Complex processes require personnel with specialized knowledge who can navigate them efficiently. Finding personnel with specialized knowledge may be difficult and costly for smaller programs.

Hardware and software changes are treated the same way. In an earlier RAND study, Schank et al. (2009) found that having hardware and software changes go through the same process at once is problematic because they take different amounts of time to certify and test.

Alterations have to be ranked and prioritized through an approval process. SCDs must be ranked and prioritized through an "alteration figure of merit" (AFOM). Anecdotal evidence shows that this is a particularly difficult part of the process because it may take a long time to assign priority, or a program may be assigned an inappropriately low priority.

Waivers are usually needed, but the waiver approval process is time-consuming and costly. The waiver process is likewise not a good option for cyber programs. As Schank et al.

(2009) found and as various Navy organizations have noted, with waivers, an alteration can be approved within 90 days under NMP. However, the approval process itself takes time and resources. Because quick approvals are typically required for C4I upgrades, this shorter alternative should be streamlined and made easier to navigate.

The Gap Between Processing Time and Actual Installation

To understand and validate the reported lengthy timelines for programs going through the NMP, we used data extracted from the PEO C4I SPAWAR Systems Center/PEO Integrated Data Environment and Repository (SPIDER). This database is populated with information on PEO C4I programs as they proceed through the NMP and includes descriptive data, such as the program or system name, PMW number (indicating who owns the program), SCD number, and type of job being performed (i.e., installation). It also allows calculations to show the duration of various steps in the NMP for first and subsequent installations. The data pulled for the purpose of this task included the following:

- SCD phase I duration
- SCD phase II duration
- SCD phase III duration
- integrated logistics support certification duration
- installation duration
- total time from SCD through installation.

We requested data from the SPIDER database to calculate the overall length of the NMP for PEO C4I expedited programs. We focused on expedited programs because we wanted to calculate the time required for programs that need to get through the acquisition processes quickly, and this helped us identify appropriate case studies. With this information, we were able to identify best practices and develop recommendations.

We worked with a PEO C4I contractor that was familiar with the SPIDER database. The contractor extracted and organized data on the following Navy rapid deployment capability (RDC) programs for 2008–2010:

- Automatic Identification System (AIS)
- Commercial Broadband Satellite Program (CBSP)
- Subnet Relay and High-Frequency Internet Protocol (SNR/HFIP)
- Wireless Reachback System (WRBS).

While these are not IA or CND programs per se, they are useful as case studies because they were all rapid deployment capability programs; that is, each was acquired and deployed rapidly to fulfill an urgent need in the Navy.

The data pulled from SPIDER covered only the time from when the SCD was first submitted through the first installation on a particular ship. While the data did not include modifications after the first installation, they did capture multiple variants of each system and multiple platforms. We examined the following variants: AN/URN-31(V)1, AN/URN-31(V)2, AN/USC-69(V)1, AN/USC-69(V)2, AN/USC-69(V)3, AN/USQ-195(V)1, AN/UYQ-96(V)6, AN/UYQ-96(V)7, CND-IATS, CND-OSE (Operating System Environment) V1.0, CND-OSE V1.1, and WRBS(V)1. Specific platforms included the following:

CG-54, CG-68, CVN-65, CVNs 69–74, CVN-77, DDGs 55 and 56, DDG-64, DDG-69, DDG-82, FFG-48, FFG-59, LCC-20, LHD-4, LHD-6, LPD-13, LPD-17, LPD-20, LSD-42, LSD-45, LSD-51, and MCM-4. The results of the data extraction are presented in Table 3.1.

The data in Table 3.1 provide a better understanding of how long the NMP generally takes. From these data, we found that it took an average of 18 months for each of four PEO C4I RDC programs to get through the NMP. The most time-consuming journey through the NMP was for one of the CBSP installations, which took 47 months from the time the SCD was submitted until the first installation was completed. The least time-consuming was one installation for the WRBS program, which took 3.3 months. These data are troubling because they show that, from SCD submission to completion of the first installation of an expedited program, it could take more than three months to navigate the NMP, but it will most likely be closer to 18 months or even longer. Eighteen months is unacceptable for a cyber security product installation. By the time the software or hardware installation is approved, program offices need to start over in the NMP with more up-to-date technology.

For the programs on which we collected data, Figure 3.2 shows that the actual installation times are minor compared with the processing and wait times in the NMP.[1]

Programs That Have Navigated NMP in Under 30 Days

Proceeding expeditiously through the NMP might seem difficult in light of the data presented here; however, we were able to identify instances in which programs received expedited approval of their SCDs, which is a critical approval step in the process. This approval allowed the programs to proceed with installation. We identified the following examples:

- PEO Integrated Warfare Systems (IWS) was able to move through the SCD approval process in one to two weeks.
- The period from initiation to approval of PMW 150's Global Command and Control System–Maritime (GCCS-M) SCD was 1.5 days.
- The Host-Based Security System (HBSS) was able to move through the SCD approval process in under 30 days.

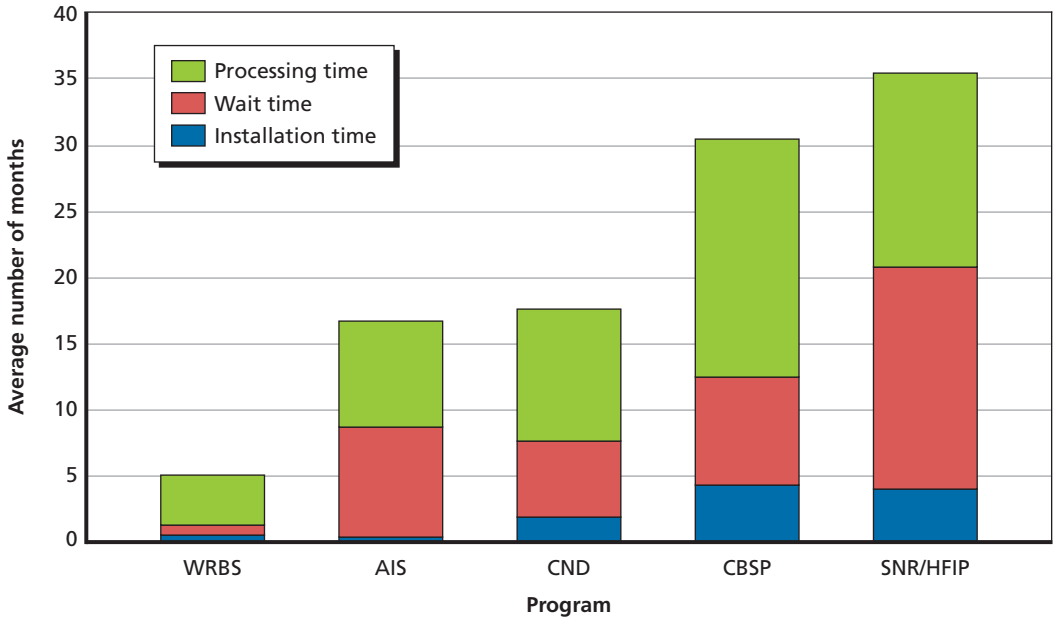
Table 3.1
Average NMP Times for Five PEO C4I Programs

	PEO C4I Programs				
NMP Wait Time (months)	**WRBS**	**AIS**	**CND**	**CBSP**	**SNR/HFIP**
Minimum	3.3	14.3	7.0	12.6	30.8
Maximum	8.7	21.5	28.1	47.3	40.0
Mean	5.1	16.8	17.6	30.3	35.4
Installation	0.6	0.4	1.9	4.4	4.0
Processing	3.8	8	10.1	18.0	14.5
Wait	0.7	8.3	5.7	8.1	16.8
Number of data points	5	6	15	4	2

SOURCE: PEO C4I SPIDER database with authors' calculations of averages.

[1] We were not able to determine within the bounds of this study why some programs took longer than others.

Figure 3.2
NMP Installation, Processing, and Wait Times for Five PEO C4I Programs



SOURCE: PEO C4I SPIDER database with authors' calculations of averages.
RAND *TR1294-3.2*

PEO IWS was able to get through the critical SCD approval portion of the NMP by maintaining open communication with several key parties involved in the process. GCCS-M program personnel spent 1.5 intense days in constant communication and benefited from the push of the PEO C4I SCD coordinator with NMP approval authorities. In the third example, a directive from the Office of the Chief of Naval Operations drove HBSS through the process in less than 30 days. We found that, under specific conditions, the NMP can be navigated rapidly; however, expedited cases require dedicated manpower that cannot be scaled to a broader level.

Recommendations

We derived a series of recommendations regarding the NMP from the best practices identified through the data analysis.

Influence upcoming changes to the NMP. PMW 130 should follow the changes to the NMP that are being discussed and try to positively affect installation times for cyber programs. Changes are in the works, but the specifics had not been announced as of this writing. These changes could potentially shorten or simplify the process, which would be important for PMW 130 and other cyber programs in the Navy.

PMW 130 should also be aware of the various circumstances in which a change can be categorized as something other than a new capability. New capabilities require the full NMP, but other types of changes allow programs to use less time-consuming methods to maneuver through the process, or the program can avoid the NMP altogether by identifying the change using the IAVA process. IAVAs (i.e., a Microsoft patch) go through the Navy Cyber Defense

Operations Command Process. An IAVA addresses severe network vulnerabilities that threaten DoD systems and information and should be fixed in under 30 days. If applicable, programs should present software changes as "patches" with no changes in capability or functionality.

Table 3.2 presents some of the general characteristics of changes or stipulations for the use of the NMP change process for emerging needs, the NMP SCD revision process, and the full NMP. The programs discussed here were concerned with rapid acquisition, were available in the SPIDER database, and fell under PEO C4I management.

Make use of "best practices" to get through the NMP in an expedited manner. The SCD should be submitted quickly, and those approving it should be contacted in advance to help them prepare for an expedited approval. Several of our interviewees advised that programs should submit their SCDs as early as possible to provide ample time for the NMP to accommodate the request. Programs should also proactively monitor documentation as it passes through the NMP.

Strong communication and knowledge of the various parts of the NMP are key to getting through the process rapidly. Specifically, a "heads-up" message to the technical assessment team will allow it to quickly focus its attention on the SCD when it comes in. The cost-benefit analysis team (typically PEO Ships) can also benefit from an alert message. Communication with the AFOM organization is very important because this is where priority is assigned to an SCD. If the AFOM is slow in assigning priority or if it assigns an inappropriately low priority to an SCD, this can create a long delay. Thus, this step warrants close attention. Finally, the Navy Modernization Board may function more smoothly with at least one voter who is familiar with the program and its acquisition needs, so contacting at least one board member in advance will help expedite the process.

Segment processes according to time constraints. The problem faced by PMW 130 can be segmented in a number of ways. One option is to divide acquisitions into three groups of activities according to time requirements:

- acquisitions that must be completed in less than 30 days, such as virus definition updates, IAVAs, simple patches
- acquisitions that must be completed within six months, such as productivity suite applications or operating system service packs or replacements
- acquisitions that take longer than six months (often much longer).

Fortunately, there is a strong correlation between the complexity of an action and the desired time to completion: Those that are needed the soonest are often the simplest.

Considering the first group, rarely does an IAVA change the radar cross-section of a ship or any of the other engineering and technical concerns on a ship. Few have significant logistic implications. Personnel issues are often minimal, although user practices may need modification, and most of any user "retraining" occurs aboard ship, not through PMW 130 or the Navy's schoolhouse. The planning process for items in this group could employ a checklist to ensure that all the possible implications (e.g., engineering, logistic, personnel) are considered. The most effective process change to encourage streamlining would be the use of preapproved waivers for applicable processes (e.g., those embedded in the NMP).

Grant the PM authority to determine what can be skipped or modified on the list of preapproved waivers. In the case of Haiti, the Navy waived a required reaccreditation in the face on an emerging need. This practice should be generalized. That is, lists of possible waivers

Table 3.2
NMP Options for Ship Changes

Characteristic	NMP Change Process for Emerging Needs	NMP SCD Revision Process	Full NMP
Stipulation for use	Requires immediate installation or reprioritization of tasking and reallocation of resources to support accelerated development and installation Safety item; mission-critical capability; addresses critical software, firmware, or other deficiencies (i.e., Strike Force Interoperability Category 1 or 2) Consists of all efforts required to correct or maintain a system's design capability, maintainability, or reparability through internal equipment modifications that do not affect shipboard distributed systems (i.e., Sustainment Types 1 and 2)	Software/firmware changes that require backfit and or forward fit but do not provide a new functionality or capability beyond the scope of the original SCD (i.e., software patches) Reinstallation of a software requirement to support a new capability/functionality[a]	A new program that will be installed for the first time Operating system that is being changed Change that provides new capability or functionality
New or revised SCD required	SCD completion required (may be new or revised, depending on the change)	Revised SCD with statement regarding the change	New SCD
Length of time based on guidance	< 30 days	Depends on SCD cost: < $50 million = 5–10 business days $50 million–$199.9 million = ~30 days > $200 million = ~90 days	31-month process

SOURCES: Information compiled from Hetkey, 2010 and interviews conducted for this study.

NOTE: IAVAs go through the Navy Cyber Defense Operations Command Process, not NMP.

[a] Specifically, the installation of the "early adopter" system required some previously installed software products (e.g., Navy Information Application Product Suite, GCCS-M Composeable FORCEnet) to reload their software.

should be prepared for emerging (and possibly other) needs, along with guides for their application to accelerate CND solutions where that is needed. For the most pressing needs, the PM should be able to make specific recommendations that are rapidly reviewed by an oversight board, and those that are approved should be applied. This is similar to a process used in the Army.

We suggest that the PM be able to discern issues that routinely do not apply to particular kinds of acquisitions. This approval should occur during the initial development planning for the acquisition. The concept of preapproved waivers is hinted at in limited ways in such approaches as the IT Box, PMW 160's process for patches, and IAVAs. Preapproved waivers expand existing streamlining to cover more of the overall process and could reduce the number of required approval boards. The strong implementation of preapproved waivers should allow more activities to be carried out in parallel rather as a series, and this should also be decided during the development planning.

The preapproved waivers may need to differentiate among software, hardware, and other considerations or have limits. An example of a limit might include increasing the electrical load on a compartment outlet circuit by no more than 10 percent (1.5 amps on a 15-amp circuit). An increase of 1 amp may need to be reported, but the waiver may allow the report to be made in parallel with other actions, rather than requiring an engineering evaluation and approval in a series with other steps. Virus definitions, IAVAs, patches, and similar modifications, should not be delayed to obtain an electrical load evaluation or approval, nor should it have to wait for most of the processes that apply to the most complex changes.

Correlatively, the PM should be granted the authority to use preapproved waivers. However, to gain approval for a substantial preapproved list, we would include representatives of stakeholders in the planning so that a plan could be produced in one meeting (and so that there is no long process to get the development plan agreement). These stakeholder representatives might be from the CA, ODAA, NMP (liaison), Naval Network Warfare Command (cyber dedicated type commander), the Navy's Tenth Fleet (FCC representative), PEO C4I, and the E2, but the fewer the better.

CHAPTER FOUR

Budgeting, Funding, and Contracts: Challenges, Best Practices, and Recommendations

Outside of testing and installation, the acquisition process also includes budgeting, funding, and contracting. This chapter looks at these issues in relation to cyber acquisition. Although these steps are not as problematic as C&A and NMP, cyber programs still face challenges in these areas. We gleaned best practices and recommendations from programs that have already dealt with budgeting, contracting, and funding challenges. Given that cyber acquisition requires a rapid acquisition tempo and incremental builds for IT acquisition, some of the challenges, best practices, and recommendations presented here relate to both rapid and IT acquisition.

Challenges

Budgeting and Funding

PMW 130's mission presents both rapid and IT acquisition budget challenges. One such challenge is the planning, programming, budgeting, and execution (PPBE) system, which is mismatched to the fast-paced IT commercial marketplace and the needs of cyber programs like CND (OSD, 2010, p. 6). This is apparent in the budgeting portion of PPBE. The budgeting process is calendar-driven and takes nearly two years from planning to the beginning of budget execution (GAO, 2010, p. 9). Not only does the budgeting process take too long, but it is also inflexible (O'Neill, 2010, p. 10). In addition, the NRC has said that the Navy's IA research budget is grossly underfunded for properly addressing escalating IA threats and challenges (NRC, 2010b, p. 90). (As a means of comparison, the Air Force's research budget is three to four times greater.) This means that programs need to be concerned with both the process and the available funding.

Because urgent needs processes have not been incorporated into the PPBE system, they face a separate list of challenges. These challenges are relevant to cyber acquisition because program offices that focus on cyber issues may need to use the rapid acquisition processes to deal with emerging needs. Several recent studies have looked at these urgent needs processes and problems. One of the budgeting challenges that rapid acquisition programs face is an uncertain future stream of funding. Urgent needs are typically funded with warfighting supplemental budgets that are not likely to continue indefinitely (DSB, 2009b, p. 6). In addition, the GAO noted in its rapid acquisition case studies that obtaining initial funding was a primary challenge for nearly half of the programs it observed (GAO, 2010, p. 7). The DSB also found that it is difficult to obtain stable, dedicated, and flexible funds for rapid efforts (DSB, 2009b, p. 28). "Color-of-money" issues are also problematic for rapid acquisition programs. These

issues tend to be universal (they are common to all acquisition programs), but they can be more problematic when funding decisions need to be made quickly, as in the case of COTS solutions (Gansler and Lucyshyn, 2008, p. 56).

Rapid acquisition programs also face challenges when money needs to be moved. There has been pushback from traditional stakeholders when funding is redirected to fulfill urgent needs (i.e., "robbing Peter to pay Paul"; Drezner, et al., 2011). At the PM level, it is difficult to move funds quickly to address these priorities (GAO, 2005, p. 51). This problem tends to be fairly universal among acquisition programs, regardless of speed and size.

Contracting Challenges

In IT acquisition, technology turnover happens frequently. Contracts must be written with the understanding that the requirements may change as the program matures. IDIQ contracts have existed for years in evolutionary acquisition to accommodate this reality, and rapid acquisition programs now frequently rely on these contracts to deal with uncertainty of quantity.[1]

Recommendations

Budgeting and Funding

Develop processes and institutions for cyber acquisitions that provide stable resources both inside and outside the program office's budget. Several recent studies have documented best practices for mitigating budgeting, funding, and contracting challenges. Maintaining stable funding and larger budget reserves to address "unknowns" is important if programs are to fulfill their acquisition plans and maintain their cost and schedule goals (Harp, 2010, p. 20). Programs need a stable budget profile to support multiple increments of iterative development (as in evolutionary acquisition or IT acquisition). Established cyber programs would likewise need this type of funding. New requirements must be funded with RDT&E dollars, but the AIS program only had procurement dollars and needed to come up with a solution to fund its emerging requirements. The program office obtained the needed RDT&E funding through the Office of Naval Research (ONR) Rapid Technology Transition (RTT) program. Because AIS was about to begin the process of integrating GCCS-M, the RDT&E funding was justified. The RTT process allowed the AIS program to use RDT&E funds for its emerging requirements, and, subsequently, the program was able to deliver greater capability than originally planned (Poor and Case, 2006).

Successful programs sometimes try to attract senior-level leadership support to help facilitate funding options (Drezner et al., 2011). This is important for traditional and rapid acquisition programs. Specifically, for rapid acquisition, programs should consider using the unit commander's O&M, Navy, funds first to fulfill rapid needs. There are limits to how these funds can be used, however. For example, requests must be less than $250,000, and this funding stream offers limited oversight and coordination (DSB, 2009b, p. 8). When the cost of an urgent need is greater than $250,000, PMs should rely on the service-level rapid acquisition

[1] According to Defense Acquisition University (2012a), evolutionary acquisition is

> The preferred DoD strategy for rapid acquisition of mature technology for the user according to DoDI 5000.02. An evolutionary approach delivers capability in increments, recognizing up front the need for future capability improvements. There are two approaches to achieving [evolutionary acquisition]: Spiral Development and Incremental Development.

processes for funding (DSB, 2009b, p. 9). After other sources are exhausted, PMs should try to access funding allocated for supplemental overseas contingency operations, research labs, and below-threshold reprogramming (DoD Inspector General, 2009, p. 39).

Outside funding may also be available for cyber resources. The following is a list of approaches outside of the traditional acquisition process that may be able to aid cyber acquisition:

- Navy rapid acquisition processes: RDC, rapid development and deployment (RDD)
- Navy laboratories: Naval Innovation Laboratory (NaIL), Enterprise Engineering and Certification labs, SPAWAR Systems Center Pacific, and SPAWAR Systems Center Atlantic
- ONR's technology transition and science and technology (S&T) programs: Future Naval Capabilities, RTT, Small Business Innovation Research/Small Business Technology Transfer, Swampworks, Technology Insertion Program for Savings (TIPS), and Tech Solutions
- Joint processes: Joint Rapid Acquisition Cell, Quick Reaction Fund, Rapid Reaction Fund, Defense Acquisition Challenge, Joint Capability Technology Demonstration, Rapid Reaction Technology Office, and Technology Transition Initiative.

In addition, the implementation of the new IT acquisition process in DoD should change the way budgeting is handled for IT acquisition programs. We recommend monitoring the process for changes and the anticipated and unanticipated consequences of those changes.

Consider having the fleet (not PMW 130) pay for software upgrades or patches for emerging needs from its operating funds. This type of reimbursable funding mechanism is ideal for uncertain but urgent funding needs. Fleet commanders, through their type commanders, can decide to cut back on hull maintenance or ship steaming hours if an unusual number of software patches will be needed in any given year. Fleet commanders have larger O&M, Navy, budgets with considerable flexibility. A fixed budget for PMW 130 has little or no flexibility to handle surges and, if underutilized, will be raided in execution years and then cut in future years.

If a fixed budget must be pursued (in the absence of a reimbursable funding mechanism) to meet emerging threats, that amount might be around $16 million. This is a very rough estimate based on one threat that occurred in the recent past that necessitated the accelerated fielding of HBSS. That effort had an estimated cost of $8 million (Program Manager, Warfare PMW 160, 2010; Lazarski, 2010). The PM indicated that there are one or two emerging threats or needs per year.

Track the level of effort and total cost of past efforts to justify a separate budget line in the future. The Conficker development effort supports this recommendation. That effort required only 70 total labor hours (two people), was paid for by PMW 130 with funding already in place for the CND program, and was considered business as usual.[2] The higher cost for the HBSS effort and the contrasting minimal cost for Conficker suggest that budgeting for emerging needs is difficult, given the wide range of solution costs.

Contracting

Develop the following rapid contracting options for cyber programs. Many options may be available to Navy programs, including the following:

[2] Figures provided by the CND program office.

- enterprise software agreements under the DoD Enterprise Software Initiative
- Navy IT Umbrella Program or other Navy enterprise license agreements through PMW 270
- Army Communications and Electronics Command's rapid contracting program[3]
- cost reimbursement, firm fixed-price (FFP), and multiple-award IDIQ contracts (Deneault, undated, p. 14)
- IDIQ processes to procure, modify, or tailor COTS products quickly
- IDIQ processes to develop hardware and software as necessary
- award fee or performance incentives to motivate contractors (Deneault, undated, p. 14).

[3] The Army Communications and Electronics Command's "Time and Materials and Firm Fixed Price Task Order" contract supports urgent needs for all federal agencies. Under that contract, programs can procure critical hardware, software, systems management, and contingency response capabilities within 19 days.

CHAPTER FIVE

Governance, Integration and Training, and Emerging Needs: Challenges, Best Practices, and Recommendations

This study set out to explore several aspects of the cyber acquisition process. In addition to testing, installation, and budgeting and contracting, we looked at governance, integration and training, and "emerging" needs. We found fewer hurdles to cyber acquisition in these latter areas. In this chapter, we explore these additional pieces of IT and cyber acquisition.

Challenges

Governance

Cyber acquisition faces challenges resulting from IT acquisition governance in the Navy primarily because this governance is widely dispersed. According to VADM Harry Harris, assistant to the Chairman of the Joint Chiefs of Staff, "Alignment and authority issues preclude achievement and execution of effective IT governance" (Harris, 2008). There is also some redundancy in oversight that lengthens the acquisition process, and delays tend to occur when a program's schedule is not a priority (OSD, 2010). Furthermore, large, detached acquisition teams are often unable to meet schedule demands (OSD, 2010). Another challenge is balancing between small, incremental releases and configuration management in the field (DSB, 2009b). Finally, we found that it was challenging to field capabilities with short cycle times against the challenges of ship availability, shipyard schedules, deployments, and fleet readiness (Rieken and Gunderson, 2010).

Integration and Training

We also found challenges involving integration and training, including the following:

- proliferation of C4I (often piecemeal), which complicates integration by straining power, cooling, and other support functions
- open architectures are not yet prevalent for software or hardware
- inadequate training and proficiency among PMs and vendors, especially in the areas of IA and interoperability, which can cause preventable problems later in the acquisition process (McCarthy, 2010).

Process for Emerging Needs

A new acquisition process needs to be institutionalized to provide PMW 130 with the necessary authorities to address emerging needs. For example, we found that emerging needs generated from immediate threats, such as a new network virus, lie outside the CND program and

present a whole host of challenges, including those regarding resource availability. The 2009 SECNAVNOTE 5000 outlines one alternative mechanism for the Navy, but a DoD Inspector General assessment of this process concluded that incomplete guidance and procedures caused unnecessary confusion and delays (DoD Inspector General, 2009, p. 18).

Recommendations

Governance

Foster agile governance that is responsive to the rapid response demanded by IT. For IT technicians, change is an almost daily occurrence that necessitates a quick and ready response. However, delays at critical points seem to be at the heart of most of the challenges cited in this report. DSB and OSD offer two "best practices" that are appropriate for fostering responsive governance:

- Elect only vendors with experience and good past performance that are committed to working on key IT programs (DSB, 2009b).
- Support open-architecture principles to prevent integration issues in future incremental releases (DSB, 2009b).

Adopt continuous fielding strategies that effectively plan and coevolve around ship availability, shipyard schedules, deployments, and fleet readiness. The procedure for program governance should provide frequent in-process reviews rather than traditional milestone reviews (OSD, 2010). The acquisition path needs to be "risk-appropriate" and based on IT capability. (There are different needs when simply updating Microsoft Word® and when upgrading nuclear command and control capabilities; OSD, 2010).

Govern programs of record at the lowest level possible, with effective accountability mechanisms. Best practices suggest that acquisition governance should be integrated into a single decision support framework, with requirements, acquisition, and funding in one governance body (OSD, 2010).[1] Funding, requirements, and acquisition for programs of record need to be overseen by one body, similar to DoD's Business Capability Lifecycle (BCL) framework. Reviews should be designed as "frequent, in-process reviews" to address and resolve issues in a more efficient manner, and the schedule must be a priority for everyone involved (OSD, 2010). Create acquisition teams that have the required proficiency but are also sufficiently small and nimble to meet schedule demands.

Integration and Training

We identified several integration best practices during the course of this study, from which we offer the following recommendations:

- Incorporate adequate design margins in programs (Schank et al., 2009).
- Maintain similar C4I configurations across ship types (Schank et al., 2009).
- Employ an open-architecture design philosophy (Schank et al., 2009).

[1] This has been effectively done by DoD business systems and mentioned in an OSD report to Congress as an effective way to streamline IT acquisition (OSD, 2010).

- Train and brief vendors on C&A testing and procedures before and during development (project interviews).

Acquisition for Emerging Needs

Our analysis suggests that the traditional acquisition process, as it now exists, needs to be accelerated in response to unique IT demands and especially to accommodate emerging cyber threats. We offer the following recommendations to help inform the development of an appropriate process.

Designate a funding source specifically to fulfill urgent needs when a materiel solution is expected to be under a given threshold. The Army used a threshold of $100,000 for its corresponding requirement. A short needs statement or document should also be developed to specify requirements, and it should include realistic requirements only. For contracting, we recommend the use of a small acquisition team that is closely integrated with the contractor. In addition, programs should use COTS, GOTS, or some other mature solution—that is, one with a technology readiness level (TRL) of 8 or higher.

Support emerging acquisition needs with a formalized process that is separate from the traditional acquisition process. This process needs to be streamlined, agile, and able to accept an 80-percent solution (e.g., have relaxed requirements).[2] The effort should be carried out by a separate, dedicated acquisition organization with the delegated authority to acquire its own solutions. Finally, an option to transition rapid developments to formal programs should be available if the need is to be sustained across the field.

Establish preapproved requirements and contracting mechanisms for the simplest and shortest-term needs. When countering emerging threats, such as viruses and worms that are discovered "in the wild," most requirements could be defined prior to discovery; thus, the program would need to provide only the description of the problem to be fixed. There are a few exceptions that could not be written in advance, however (for example, "Correct the buffer overflow vulnerability in . . ."). There are contracting approaches to implement a response quickly, including prequalified vendors, U.S. General Services Administration Schedule 70 approaches, and IDIQ contracts.[3]

Address emerging needs with two processes progressing at two possible speeds. The first speed would require extremely responsive internal development (in hours to days) to support rapid prototyping. Figure 5.1 shows one example of how this process can be applied.

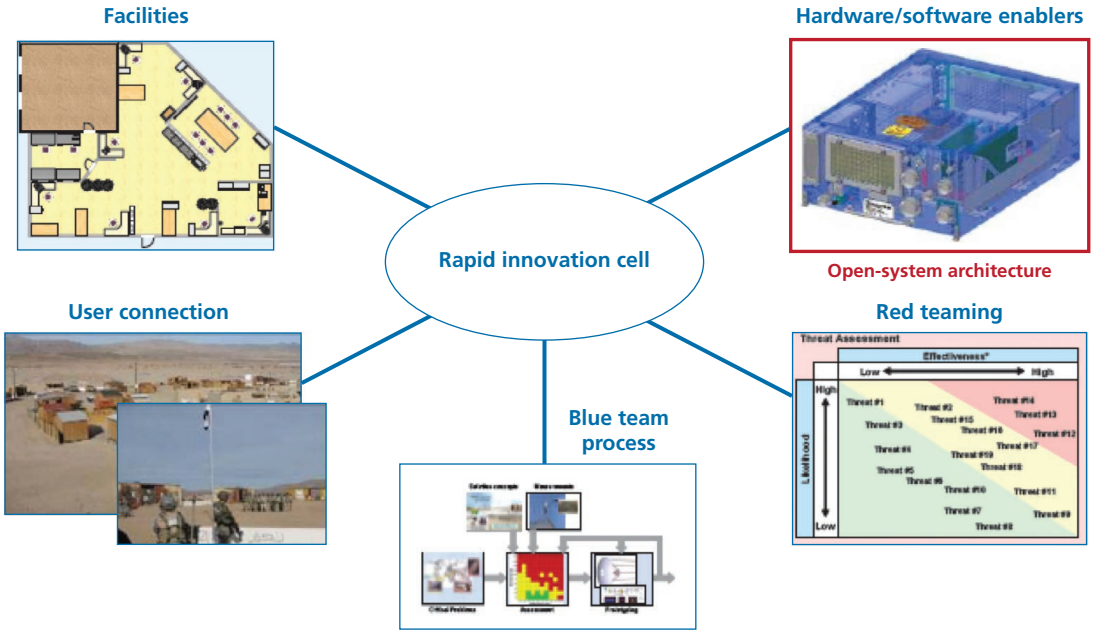
The second, a medium speed, would fulfill a requirement for a solution in approximately six months. The process can quickly deploy COTS and GOTS components in a manner similar to the Army's Rapid Equipping Force (REF) or the Air Force's Cyber Safari. There may be other ways to elevate the execution priority for C&A packages where warranted, and these should be employed as well.

---

[2] As a reviewer noted, both testing and user communities must agree to deploy a capability that fulfills the requirement immediately, despite the fact that the program may operate at a level less than that stated in the official requirement.

[3] According to CAPT (ret.) Steven Sudkamp in comments on an earlier draft of this report, April 10, 2012.

Figure 5.1
Example of Rapid Innovation of Structure to Fulfill an Immediate Need



SOURCE: Walden, 2008, slide 18.

RAND *TR1294-5.1*

CHAPTER SIX

Summary and Conclusions

In PEO C4I and the rest of the Navy, rapid acquisition or fielding does occur except with special prioritization and exceptional treatment, both of which require resources that may not be routinely available to PMW 130 and its cyber program. New agile methods outlined in the DSB report (2009b) that seek iterative and incremental development on six-month cycles will be difficult to achieve without new authorities at the PM or PEO level and a change in the approach to budgeting.

In this chapter, we summarize the findings and recommendations offered throughout the report in a way that directly addresses the four initial questions presented in Chapter One:

- What are the existing authorities, processes, and organizations that can be used to support PMW 130's rapid acquisition objectives?
- What new authorities, processes, or organizations are needed to support PMW 130's rapid acquisition objectives?
- What are recommendations for building or leveraging a dynamic OT&E environment?
- How can budgeting and resourcing challenges to agility be mitigated?

We also recommend a number of study directions that may help the Navy, and PEO C4I in particular, to continue moving forward in improving acquisition policy.

What are the existing authorities, processes, and organizations that can be used to support PMW 130's rapid acquisition objectives?

Our assessment found that current acquisition processes, especially C&A and NMP, need to change to accommodate the required iterative cycle times of PMW 130's CND program. However, at least three processes are noteworthy among those that that can be leveraged to accelerate acquisition (many more are listed in Appendix B): the RDC and RDD urgent needs processes and the JCIDS IT Box.

PMW 130 can use RDC and RDD if it needs to combat an emerging threat that is not covered by its CND program. The JCIDS IT Box process is currently used to reduce the time it takes to develop and approve IT requirements. Existing Navy labs, such as the Enterprise Engineering and Certification and virtual labs and the RDD NaIL, offer facilities that may be able to expedite testing. For the installation process, we recommend that PMW 130 use the expedited NMP because it provides the best opportunity to reduce lengthy ship modernization timelines. For budgeting, PMW 130 will need to rely on its program of record's budget for emerging needs related to CND. In the case of emerging needs not covered by RDD and RDC, the program may also turn to ONR's RTT program.

What new authorities, processes, or organizations are needed to support PMW 130's rapid acquisition objectives?

We recommend that PMW 130 pursue approval authorities at the lowest appropriate level. For example, using the PM as the milestone decision authority (MDA) could reduce approval times for various parts of the acquisition process. This was a lesson learned in the A-RCI program, and it may also benefit PMW 130. Another recommendation is to give the PEO the authority to allow cyber programs to tailor acquisition instructions to expedite processes and meet critical deadlines. It also may be expedient for the Secretary of the Navy to designate PEO C4I as the decision accreditation authority or CA for cyber programs to accelerate C&A. PMW 130 should pursue new risk models, continuous testing, and stable funding while relying on existing O&M, Navy, technology insertion processes for emerging needs that can be supplanted by design and prototyping activities. PMW 130 could also benefit from a requirements validation process that is streamlined as in the USSOCOM approach of holding a video teleconference within 48 hours to validate an urgent requirement (Paul, Porche, and Axelband, forthcoming). Finally, benefits may be gained by having PEO C4I or Fleet Cyber staff specifically dedicated to "emerging needs acquisition," which is similar to the time demands of "cyber acquisition."

What are recommendations for building or leveraging a dynamic OT&E environment?

PMW 130 should continue its plans to leverage Enterprise Engineering and Certification and virtual labs. It should also conduct testing on docked ships to save time and money and to ensure a more realistic test environment. Using open architecture in testing is also beneficial. In addition, vendors should be trained and briefed on C&A testing and procedures early on so that they are able to work efficiently with the processes and do not get bogged down under time constraints. Finally, PMW 130 should employ automated IA tools for faster C&A.

How can budget and resourcing challenges to agility be mitigated?

As mentioned earlier, we recommend pursuing a reimbursable funding mechanism for emerging needs. Because fleet commanders have large, flexible O&M budgets, PMW 130 should consider using these operating funds to pay for software upgrades or patches for emerging needs. This is preferable to a fixed budget, which could be taken away if underutilized. Finally, we recommend that PMW 130 leverage any budgeting or funding outlined in the "804 report" issued by the Office of the Secretary of Defense, especially if the IT color-of-money issue is eased by Congress.[1] This may make it easier to expeditiously obtain the type of funding needed for emerging cyber threats.

Future Work

Although the conclusions resulting from this study should help inform PMW 130's decision-making, there are still many questions that need to be answered regarding the rapid acquisition of cyber capabilities. In particular, it will be important to establish some guidelines for how cyber programs, and the CND program in particular, will structure future changes as

[1] The report, *A New Approach to Delivering Information Technology Capabilities in the Department of Defense*, was issued in response to Section 804 of the fiscal year 2010 National Defense Authorization Act. Section 804 directs DoD to develop and implement a new acquisition process for IT systems based on the recommendations of a March 2009 DSB report (DSB, 2009a).

"patches." Defining the implications of a patch in relation to cyber acquisition will have bearing on appropriate processes and cycle times. One approach that we recommend is to establish new business rules to accommodate faster C&A process times for CND. This recommendation will require a new set of business rules that allow the two speeds to work harmoniously.

Another potential future topic for examination could be the feasibility of constructing a "vendor scorecard" to measure a vendor's ability to deliver rapid cyber capabilities. We also recommend looking further into the DIACAP process to identify what should change for this process to work effectively with agile acquisition. Finally, it will be useful to monitor current pilot programs (e.g., ISPAN) following the new 804 iterative and incremental acquisition cycle and glean lessons learned from those programs for future use.

APPENDIX A

Survey of Rapid Acquisition Processes

This appendix surveys rapid acquisition processes across DoD using data from a DSB study of rapid acquisition and several other sources. It provides information on how long these processes take and general information on the rapid acquisition options available in each service. This appendix also highlights cyber acquisition's unique characteristics and its similarity to other rapidly fulfilled urgent needs.

Recent studies have gathered information on these processes (DSB, 2009a; Schaefer, 2010; GAO, 2010). These studies have reviewed USSOCOM (e.g., the Special Operations Research, Development, and Acquisition Center, formerly Special Operations Acquisition and Logistics), the Army (e.g., REF), the Air Force, the Navy, the Marine Corps, and other DoD rapid acquisition processes. Each has its own means of communicating capability needs from the field to its rapid acquisition organization, as summarized in Tables A.1 and A.2. The tables list the various streamlined acquisition methods, along with the minimum, maximum, and average times it has taken for these processes to generate, validate, and acquire solutions. These processes can be used to acquire capabilities below the Acquisition Category (ACAT) I level.

In Table A.1, the first part of the process is generating the urgent need. The data show that joint needs are generally processed the fastest, with a median time of 58 days, while it takes the Air Force the longest, with a median time of 118 days. In contrast, it only takes the Air Force 32 days to validate a need. The Marine Corps averages the longest time to validate a need, at 90 days. Finally, the Air Force is again the fastest for achieving IOC, at 120 days, while the joint process takes the longest, at 341 days. U.S. military organizations not captured in the table, such as the Army, fall in between these lowest and highest times.

Table A.2 provides further background on the various rapid acquisition processes across DoD. In particular, the table identifies the rapid acquisition process and organization, the type of information in the capability need document, the primary guidance document for each process, the organization responsible for approving the need, whether there is a specific fund for the need, the general timeline to IOC, and the percentage of the solution that a process is trying to achieve.

Appendix B focuses specifically on Navy rapid acquisition.

Table A.1
Time Needed to Address Urgent Needs

Phase	Median Time (days)	Minimum Time (days)	Maximum Time (days)
Generation			
Joint need	58	2	277
Marine Corps	103	52	199
USSOCOM	70	1	575
Navy	107	12	435
Air Force	118	45	240
Validation			
Joint need	38	1	255
Marine Corps	90	44	168
USSOCOM	49	1	575
Navy	78	21	176
Air Force	32	8	75
Initial operating capability			
Joint need	341	72	969
Marine Corps	142	27	252
USSOCOM	177	5	552
Navy	206	112	385
Air Force	120	59	180

SOURCE: DSB, 2009b, p. 23.

NOTE: These times include generation, validation, and initial implementation for the urgent need.

Table A.2
DoD-Wide Rapid Acquisition Processes

Characteristic	Joint/DoD	U.S. Army	U.S. Marine Corps	U.S. Navy	USSOCOM	U.S. Air Force
Rapid Acquisition Process	Joint urgent operational need	Operational needs statement and REF "10-liner" (a 10-line request statement)	Urgent universal needs statement	Urgent Needs Process	Special Operations Capabilities Integration Development System	Rapid Response Process
Rapid response organization	Joint Rapid Acquisition Cell, Joint Improvised Electronic Device Defeat Organization	REF	Marine Corps	Navy	Special Operations Research, Development, and Acquisition Center	Air Force
Capability need document	Joint urgent operational need statement; immediate warfighter need; Joint Improvised Explosive Device Capability Approval and Acquisition Management Process	Operational needs statement (ONS); REF "10-liner"	Urgent universal needs statement	RDC; Abbreviated Acquisition Process; urgent operational need (UON)	Combat mission needs statement/nine-liner	Combat capability document
Primary guidance document	Chairman of the Joint Chiefs of Staff Instruction 3470.01 (July 15, 2005)	Equipment Common Operating Picture user's guide	Marine Corps Order 3900.17 (October 17, 2008)	SECNAV Note 5000 (March 15, 2009)	USSOCOM Directive 71-4 (June 9, 2009)	Air Force Instruction 63-114 (January 4, 2011)
Approval	Budget Office Director Board	Headquarters, U.S. Department of the Army	Marine Requirements Oversight Council	Chief of Naval Operations	Deputy commander, USSOCOM	Air Force Chief of Staff
Funding	No specific fund	No specific fund	No specific fund	No specific fund	Combat mission needs fund	No specific fund
Timeline to IOC	Immediate warfighter need: 120 days Joint urgent operational need: 120 days to 2 years	REF: 90–360 days ONS: 90 days to 2 years	60 days is a target deadline (per Marine Corps Order 3900.17)	Less than 2 years	180 days to 2 years	60 days
Solution goal (%)	70–80	80	None specified	None specified	80	None specified

SOURCE: Adapted from Claggett, 2007; Schaefer, 2010; and DSB, 2009b.

NOTE: The "solution goal" is the acceptable percentage of capability needed. In other words, would an operational user accept 80 percent of the desired capability to field the solution faster?

APPENDIX B

Navy Rapid Acquisition Options

Emerging needs are common in cyber acquisition. Given that no formal expedited processes have been institutionalized in the Navy specifically for emerging cyber needs, it is beneficial for those in the Navy who are involved with cyber acquisition. These processes give PMs options that are not available through the traditional acquisition process.

Background on Navy Rapid Acquisition

Navy guidance identifies a need requiring rapid acquisition as a UON (Greenert and Etter, 2007, p. 2). According to a DoD Inspector General audit of the Navy's rapid acquisition process, from 2004 to 2009, the Navy initiated 13 rapid acquisition efforts for UONs. Those efforts used $104.8 million in RDT&E funds and $172.4 million in procurement dollars (DoD Inspector General, 2009, p. i). In the audit, the Inspector General found that the Navy had adequate processes in place to identify and validate these needs; however, these processes were not well understood by those using them.[1] The report identified four limitations of the existing processes:

- Navy PEOs do not control initial procured quantities in the acquisition strategies, which exposed the Navy to the risk of significant acquisitions of unproven equipment.
- Guidance for UON program planning was lacking.
- Navy program sponsors did not request that the Operational Test and Evaluation Force perform quick-reaction assessments of materiel solutions designated as RDD efforts.
- Quick-reaction assessments were needed to provide an independent, early evaluation of the operational effectiveness and suitability of materiel solutions before deployment (DoD Inspector General, 2009, p. i).

Specific Navy Urgent Needs Processes

The Navy process for UONs is specifically explained by the Secretary of the Navy in SECNAVNOTE 5000, dated March 12, 2009. The purpose of the memo is "to define the Department of the Navy (DON) Urgent Needs Process (UNP) and provide and refine guidance for the submission, processing, and response to urgent needs" (SECNAVNOTE 5000, 2009).

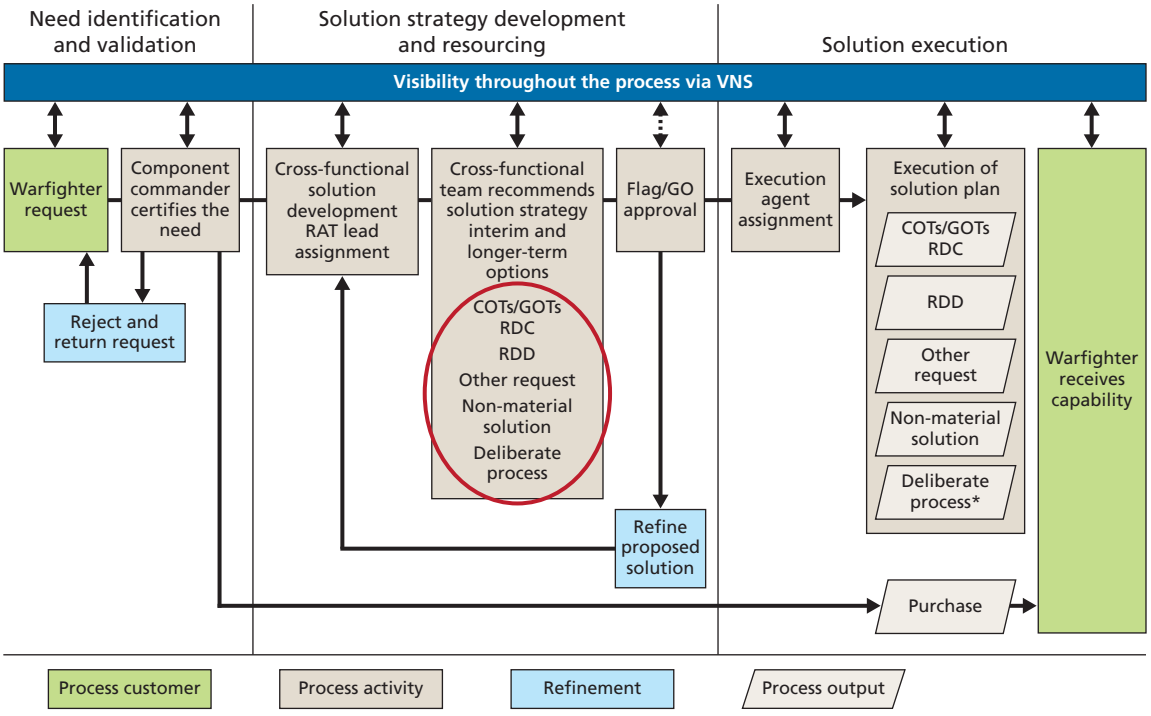
[1] Navy program managers have not had to deal with rapid acquisition as often as their counterparts in the Army, which could explain some of the unfamiliarity with these processes.

Figure B.1 shows the processes for needs identification and certification, solution strategy development and resourcing, and solution execution as identified in this guidance.

The red circle in the figure identifies the specific options that PMs can use to fulfill an urgent need, ranging from obtaining a COTS/GOTS solution to using the traditional "deliberate" process when other options are not appropriate. As shown, the Navy provides a wide range of options. The specific options are listed, along with their purposes in Table B.1.

The processes and institutions in Table B.1 can be used to fulfill an urgent need in the Navy, according to Navy guidance (Greenert and Etter, 2007, p. 2). Most are not official rapid acquisition processes, however. Specifically, they are technology transition and S&T research processes that can help provide a capability that has already been developed or can assist in developing a new capability. They are identified in Navy guidance as ways of shortening the traditional acquisition process. It is important to note that Navy guidance does not just focus on its RDC process. It also works to provide a wide array of options for PMs, who should be aware of and understand these processes to find ways of fulfilling needs outside the traditional process. There are other alternatives that may fit a need and have accompanying budgets that can be utilized. Table B.2 provides additional information on these processes. The table was compiled from a variety of sources, including Navy guidance and process websites. It shows the Navy processes, their duration and dollar limits, and potential decisionmaking authorities. As the table indicates, there are a variety of rapid acquisition and S&T and transition efforts in the Navy that can be leveraged.

Figure B.1
Navy Urgent Needs Processes



*DoD 5000.02 Interface.

SOURCE: Defense Science Board, 2009b, p. 45, Figure B-5.

RAND *TR1294-B.1*

Table B.1
Navy Rapid Acquisition, S&T, and Technology Transition Processes

Process	Purpose
Abbreviated Acquisition Process	Alternative to rapid acquisition in traditional process
ASN(RDA) pursues tailored ACAT program of record	Alternative to rapid acquisition in traditional process
Future Naval Capabilities	Technology transition
Naval Innovation Laboratory (NaIL)	Navy rapid acquisition decisionmaker and solution provider
Rapid Deployment Capability (RDC)	Navy rapid acquisition process
Rapid Development and Deployment (RDD)	Navy rapid acquisition process
Rapid Development and Deployment Committee (RDDC)	Navy rapid acquisition decisionmaker
Rapid Technology Transition (RTT) program	Technology transition
Small Business Innovation Research/Small Business Tech Transfer	Technology transition
Swampworks	S&T research
Technology Insertion Program for Savings (TIPS)	Technology transition
Tech Solutions	S&T research
Urgent capability need/urgent operational need (UON)	Identifies and validates Navy urgent need

NOTE: ASN(RDA) = Assistant Secretary of the Navy for Research, Development, and Acquisition.

The Navy has two specific, dedicated rapid acquisition processes: RDC and RDD. The next two sections describe these rapid acquisition processes in more detail using Navy instructions and guidance.

Navy Rapid Deployment Capability Process

The Navy's RDC process was established in December 1996, prior to both Operation Iraqi Freedom and Operation Enduring Freedom. Thus far, the need for this process has been minimal compared to that for the Army's REF, which has processed thousands of urgent needs.[2] As of April 2009, the Navy was tracking nine RDC solutions with RDT&E costs of $86.1 million and procurement costs of $172.4 million (DoD Inspector General, 2009, p. 24). The RDC process is specifically designed for PMs to acquire commercial or developmental products as materiel solutions to newly discovered threats or urgent safety situations. The process uses tailored procedures designed to expedite technical, programmatic, and financial decisions and expedite the procurement and contracting processes. RDC efforts are initiated by a memorandum request prepared by the program sponsor or requirements division and validated by the Office of the Deputy Chief of Naval Operations for the Integration of Capabilities and Resources (N8)/Command Master Chief. The validated request is then forwarded to ASN(RDA) for approval. If approved, that office forwards the RDC requirement to the

[2] The DSB estimated that 6,400 of the 6,700 UONs examined in its study were for redistribution of inventory. However, the Army still has a significant amount of experience in this area (300 needs versus only 20 for the Navy; DSB, 2009b, p. 22).

Table B.2
Navy Rapid Acquisition, S&T, and Technology Transition Process Durations, Funding Limits, and Authorities

Process	Project Duration	Total Project Funding	Decisionmaking Authorities
Abbreviated Acquisition Process	No limit	Weapon system programs: < $50 million total IT system programs: < $30 million total	Possible MDAs: cognizant PEO, system command commander, direct reporting PM, or designated flag officer, senior executive service official, or PM; ASN(RDA) or designee for programs not assigned to a PEO, system command, or DRPM; OT&E (waives testing)
ASN(RDA) pursues tailored ACAT program of record	No limit	Any amount	For ACAT IVT (ACAT IV test programs), MDA is the same as in the Abbreviated Acquisition Process
Future Naval Capabilities	Unavailable	Unavailable	A 3-star Navy and Marine Corps board of directors (the Technical Oversight Group) approves the capabilities
Rapid Deployment Capability (RDC)	Up to 2 years	Requests should be at or below ACAT III funding thresholds	Office of the Deputy Chief of Naval Operations for the Integration of Capabilities and Resources (N8)/ Command Master Chief, ASN(RDA)
Rapid Development and Deployment (RDD)	Up to 1 year	Up to $10 million	RDDC members, NaIL director
Rapid Technology Transition (RTT) program	Up to 2 years	Up to $2 million	ONR Director of Technology Transition Initiatives (03TTX) administers the RTT program under the guidance of the RTT Executive Review Group
Small Business Innovation Research/Small Business Technology Transfer	Up to 6 years	Up to $2.4 million	Navy system commands evaluate and select
Swampworks	1–3 years	Unavailable	ONR (decisionmaker is unclear)
Technology Insertion Program for Savings (TIPS)	Up to 2 years	Up to $2 million	Managed by ONR, Office of Transition (03T)
Tech Solutions	Up to 2 years	Unavailable	Chief of Naval Research

SOURCES: Policy guidance, official Navy websites, and other official documentation.

appropriate PEO, system command, or direct-reporting PM. The PEO, system command, or direct-reporting PM then develops and approves a comprehensive RDC strategy. The strategy includes specific expediting measures, a plan of action and milestones (such as transition to an ACAT program), and a plan for logistics and long-term maintenance support. Acquisition of RDC supplies lasts less than two fiscal years before the program transitions to an ACAT program of record. Capabilities requiring extensive RDT&E do not normally qualify for RDC, and solutions typically involve technology at TRL 8 or higher (Etter, 2006, pp. 1–2).

Navy Rapid Development and Deployment Process

The Navy's second rapid acquisition process was established 11 years after the RDC process and started funding RDD solutions in 2007. The RDD process is intended to provide rapid development, integration, and testing of new prototype solutions when there is no existing no COTS product or nondevelopmental item. NaIL is the execution agent for the RDD

program, addressing validated naval (Navy or Marine Corps) urgent needs that require the rapid (270-day) development of solutions not readily available off the shelf (SECNAVNOTE 5000, 2005, pp. 2–6). The RDD Committee is a subcommittee of the Navy's Technology Oversight Group. Its function is to approve RDD proposals to meet urgent warfighter needs (SECNAVNOTE 5000, 2005, pp. 3–5).

Proposals are submitted by Navy requirements organizations with advice from the NaIL director. The RDD Committee approves release of RDD startup funds, identifies sources of reprogrammed funding to complete each project, and advocates PPBE follow-up. Committee members include each voting and nonvoting Technology Oversight Group member, and the Assistant Secretary of the Navy, Financial Management and Comptroller, designates a representative. Representatives from the Office of the Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/7), commanding general of the Marine Corps Combat Development Command, and ASN(RDA) co-chair the committee. They appoint an executive secretary, who invites others as needed (SECNAVNOTE, 2005, pp. 3–5).

Solutions typically involve technology at TRL 6 or higher, which is generally a representative model or prototype system that has been demonstrated in a relevant environment. As of April 2009, the Navy was tracking four RDD solutions that required RDT&E expenditures of $18.7 million. No procurement is needed for RDD solutions (DoD Inspector General, 2009, p. 31).

Brief Descriptions of Other Navy Acquisition Options

Abbreviated Acquisition Process. The Abbreviated Acquisition Process can be used for small programs or modifications that cannot be considered ACAT IV or above. These solutions should not need OT&E. Navy guidance presents the following thresholds for using the process:

- For weapon systems programs
  - Development total expenditure < $10 million, and
  - Production or services expenditure < $25 million/year, < $50 million total
- For IT system programs:
  - Program costs/year < $15 million, and
  - Total program costs < $30 million. (SECNAVINST 5000.2C, 2004, Enc. 2, p. 13)

ASN(RDA) pursues tailored ACAT program of record. Navy policy says that if the other urgent needs processes are not appropriate, then a tailored ACAT program of record can be used to trim to acquisition process timeline (SECNAVNOTE 5000, 2009, p. 5). This can be accomplished using a variety of methods while operating within the regulations of the traditional acquisition process. For example, a program may use certain types of contracts, such as IDIQ, to allow more flexibility in purchasing the solution, or it can use incremental builds in its acquisition strategy. The latter is useful for a program that may require continuous software updates over time.

Future Naval Capabilities. This ONR program works to quickly close identified warfighting gaps by bundling discrete but interrelated S&T products that deliver a measurable improvement within a five-year time frame. A three-star Navy and Marine Corps board of directors, the Technical Oversight Group, approves the capabilities based on their contribution to closing S&T capability gaps (ONR, undated[a]).

Rapid Technology Transition (RTT) program. ONR's RTT program facilitates the timely and effective acquisition and fielding of novel and promising technologies. RTT is structured to bring transition efforts to closure quickly and to provide execution-year funding for a rapid start, bridging the gap until the program of record can fund the completion of the technology insertion (ONR, undated[b]).

Small Business Innovation Research/Small Business Technology Transfer (SBIR/SBTT). These DoD programs provide significant early-stage research and development funding to small technology companies (SBIR) and to companies working directly with research institutions (SBTT). Qualified small businesses that are interested in addressing naval technology needs can submit proposals for projects that can ultimately transition to the fleet. Funding for this program is not appropriated but is provided annually under the statutory 2.5 percent set aside from ONR extramural RDT&E funds (ONR, undated[c]).

SwampWorks. This ONR program is charged with investigating "innovative, high-risk, and disruptive technologies and concepts." The program is capable of modeling how new technologies might mature, thus improving the cost-effectiveness of the IT enterprise. SwampWorks efforts are smaller in scope to those of other programs dedicated to other kinds of prototypes; SwampWorks is expected to deliver meaningful results in less than three years (ONR, undated[d]).

Technology Insertion Program for Savings (TIPS). ONR's TIPS works to procure and release appropriate COTS and late-state development technologies to eliminate immediate capability deficiencies and gaps. By increasing the rate at which new cutting-edge technologies are inserted into Navy acquisition programs, TIPS can significantly reduce O&M support costs. TIPS provides execution-year funding for a rapid start (ONR, undated[e]).

TechSolutions. This ONR web-based process enables sailors and marines to actively suggest technological solutions that may improve mission effectiveness. It aims to provide the fleet and force with prototypes that rapidly respond to needs and quickly deliver 60- to 80-percent solutions. The process also enables the rapid transition of technologies and delivers a demonstration or prototype within 12 months (ONR, undated[f]).

APPENDIX C

Case Studies of Successful Rapid and IT Acquisition

Navy Case Study: A-RCI

In the Navy, one of the most well-regarded examples of a successful, rapid IT acquisition effort is the Submarine Acoustic-Rapid COTS Insertion (A-RCI) program (Dillard and Ford, 2009; Johnson, 2004, 2007; Boudreau, 2006).[1] A-RCI is a towed array sensor. The program was established to implement a new approach to designing and fielding sonar systems. Because of cost limitations, a new unique system was not affordable, so the program had to develop solutions at a much lower cost than that required under traditional DoD acquisition approaches.

By many accounts (e.g., Dillard and Ford, 2009; Johnson, 2004, 2007; Boudreau, 2006), the program was successful. According to Johnson (2004), the program could deliver a device with sufficient performance and within budget based on the following assumptions:

- Competition for ideas would result in a better product at a reduced cost.
- COTS options provided low-cost, high-performance general-purpose processing technologies.
- Deployed forces in the Navy could be tapped to provide rapid, hands-on customer feedback.

A-RCI set out to use what the DSB now calls an incremental, iterative acquisition process. The program recognized early that its device needed the following:

- improvements on an almost continuous basis
- the ability to provide frequent capability upgrade iterations
- a phased development process integrating continuous upgrades and relying on open architectures to enable such evolutionary acquisition.

Key lessons learned from the A-RCI effort, as reported in a number of studies (Dillard and Ford, 2009; Johnson, 2004, 2007; Boudreau, 2006), are as follows:

- Set frequent upgrade release dates and do not let those dates slip. Note that the first iteration was released 18 months after the identification of initial requirements; subsequent upgrades occurred every 12 months (Johnson, 2004; Dillard and Ford, 2009; Boudreau, 2006).
- Make requirements flexible to meet iteration deadlines.

[1] The A-RCI program is also known as the AN/BQQ-10(V) sonar.

- Delay as long as possible the selection of technologies and products for each iteration.
- Use an open architecture and COTS products. In this case, "legacy" sensors were used. Key processors were replaced with COTS PC technology and COTS software.
- Use a "prime" coordinator as the integrator and multiple solution suppliers.

A-RCI has been deemed successful by many metrics in terms of delivery, cost, and performance.

Delivery. Initial improvements were installed on the first ship 18 months after the milestone decision (in 1997). By 2004, the product was installed in more than 50 submarines with four generations of hardware and software upgrades—faster than in most comparable acquisition programs.

Cost. Cost savings included a 60-fold decrease in "real processing costs" (Johnson, 2004).

Performance. According to Johnson (2004), A-RCI delivered a sevenfold increase in the submarines' towed array sensor performance.

According to Boudreau (2006), another key to the success of A-RCI was that the program was able to "locate the authority to include or delay meeting requirements with the program managers." According to that study, "continuous streams of RDT&E, Procurement, and Operations and Support accounts were required to support A-RCI."

Army Case Study: Defense Readiness Reporting System–Army

The Army also had a notable success with agile development. In PEO Command, Control, and Communications–Tactical, Portia Crowe led a project to modernize the Defense Readiness Reporting System–Army. The notable aspects of this project were a reliance on rapid prototyping, early and repeated engagement with stakeholders and those dictating requirements (regarding, for example, security and IA), and user acceptance. The project was fielded in nine months and added more capabilities two months after that. It focused heavily on the integration of multiple contracting teams, incorporated parallel processes with rapid prototyping, and ensured the participation of security staff from the beginning. The project team met program milestones and reviews with flexible definitions. Strengths of the project included a much shorter cycle to development and successful deployment with continued support. One weakness was its reliance on individual entrepreneurship among the project leads and team: Scaling was difficult with no central authority.

Crowe noted that part of the program's success stemmed from the ability to work directly with people who could inform her of how best to treat documentation, meet security policy, and speed up testing. Aligning the right people was a significant challenge that could be mitigated by centralizing expertise.

Marine Corps Case Study: Commercial Hunter

The motivation for the Marine Corps project Commercial Hunter was that the truly cutting-edge technology resides in research organizations, such as universities. By funding this research itself, the Marine Corps hoped to gain access to that knowledge and potential products resulting from the work. What this meant, of course, was that the Marine Corps would only par-

tially own the results of its spending, and those studies would be tied to the academic calendar. The process unfolded as follows:

- Funded universities were to anticipate the next generation of threats and prepare the technology to confront them.
- A "red cell experiment" was successfully used to test this approach. In this experiment, experts work with the government and contractor to test various scenarios. Such tests are usually conducted when DoD is trying to identify the requirements for a system or when it is trying to test a system with some operational scenarios.
- The program tied outside experts closely to Marine Corps requirements identification and relied heavily on outside development.

The strengths of Commercial Hunter included lower cost and reduced time relative to traditional acquisition programs, as well as the ability to leverage cutting-edge technology development.

Its weaknesses stemmed from the shared ownership of the technology development. In addition, such a program is scalable only if there is a ready supply of universities and experts, and such an approach is not applicable for technology with a TRL below 6.

APPENDIX D

JCIDS and Incremental Acquisition

Acquisition for the U.S. military has evolved to accommodate new technologies, processes, management concepts, and lessons learned over time. Acquisition policy today is summarized in the DoD 5000 series of documents (DoDD 5000.01, 2007; DoDI 5000.02, 2008), JCIDS policy documents available through Defense Acquisition University), and recent legislation, such as the Weapon Systems Acquisition Reform Act of 2009 (WSARA; Carter, 2010b) and its 2010 update, the Implementing Management for Performance and Related Reforms to Obtain Value in Every Acquisition Act (IMPROVE) (see Ittig, Schecter, and Sivertsen, 2010).[1] The latter two are sufficiently recent that their impact was not yet recorded in the DoD 5000 series or experienced in acquisition programs as of this writing. Figure D.1 depicts the Defense Acquisition System. As the figure suggests, the process is deliberate and lengthy, typically requiring years to execute (Cluck, 2009).

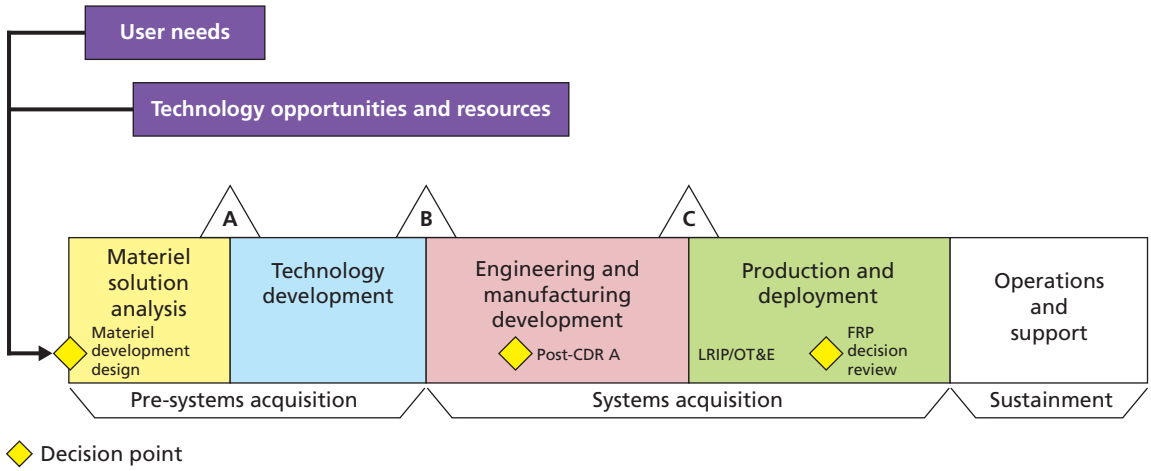
Figure D.1 is a simplified view of a portion of the current defense acquisition process. Acquisition programs are typically initiated either when a military user identifies a need that has not been satisfied by a current or envisioned acquisition program or when technology evolves to the point that a need can be satisfied in a way that is markedly superior to that currently provided or planned. This initiates a materiel solution analysis, represented by the yellow box in Figure D.1.

Acquisition Phases

In the materiel solution analysis phase, more fully depicted in Figure D.2, the JCIDS process involves first performing a capability-based assessment that validates whether a new capability is required to satisfy the need. This capability is published as a DOTMLPF (doctrine, organization, training, materiel, leadership and education, personnel, and facilities) capabilities requirement if it can best be met by one or more of the nonmateriel DOTMLPF components, such as doctrine or training. Alternatively, it is published in an initial capabilities document if a materiel solution is recommended. An analysis of alternatives, also shown in Figure D.2, is the next step, undertaken to determine the best materiel approach.

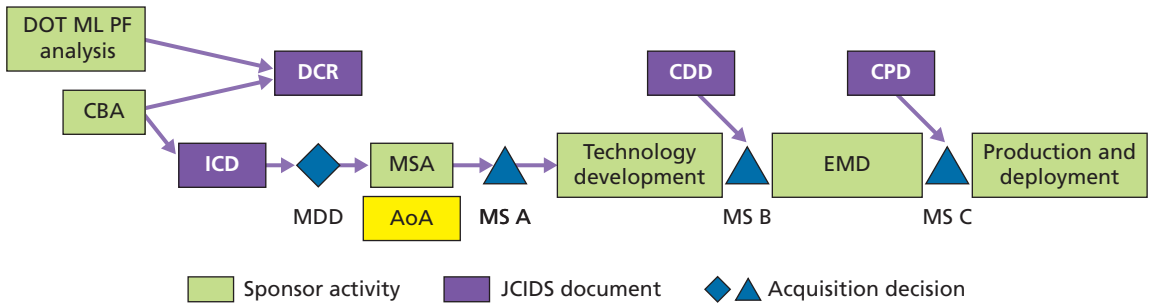
[1] WSARA of 2009 enacted sweeping changes to the way in which acquisition was conducted, including establishing new program groups in OSD (such as Cost Assessment and Program Evaluation), eliminating old positions, and instituting new legal requirements for the way in which projects are managed. There has also been extensive discussion of the difference between MAISs and major defense acquisition programs (MDAPs). Additionally, the National Defense Act of 2010 adopted almost all of the recommendations set forth by a DSB study of IT purchasing (DSB, 2009a).

Figure D.1
The Defense Acquisition Life Cycle



SOURCE: Defense Acquisition University, 2009.
NOTE: LRIP = low-rate production. FRP = full-rate production.
RAND *TR1294-D.1*

Figure D.2
JCIDS Process and Acquisition Decisions



SOURCE: Adapted from Defense Acquisition University, undated.
NOTE: EMD = engineering and manufacturing development.
RAND *TR1294-D.2*

For example, the validated need is to defeat a new form of enemy undersea vessel, which could be done, in principle, by using new or improved airborne, surface, or subsurface materiel means. In this hypothetical example, one of these options would be selected. The conclusion of the analysis of alternatives is documented in a materiel development decision that includes the selection of the lead DoD component(s) for the ensuing program and the appropriate milestone (A, B, or C) at which to initiate the program.

Other main phases depicted in Figure D.2 include the technology development phase, which is followed by the engineering and manufacturing development phase. In that phase, technologies are integrated into a system, net-centric considerations are addressed as part of the system design process, system prototypes are tested and demonstrated, the implementation or means of manufacturing are designed, and the plans and preliminary design of the logistics and training system are developed. This process is thoroughly reviewed, as are life-cycle

cost, schedule, and system performance estimates. If the outcome is satisfactory, the program is allowed to enter the production and deployment phase. Produced units, with their trained operators, support personnel, and logistical supplies, are then deployed.

Incremental Acquisition

Under DoD incremental acquisition policy, what has been described so far actually happens several times in a program's life cycle, as shown in Figure D.3.[2] In this process, a second increment begins its technology development when the first increment is in EMD. Similarly, a third increment starts when the second increment is in its EMD phase. The size of the increments, the number of increments, and the prior increment's progress when the next increment is started all depend on the particulars of the program. Not shown in detail in Figures D.1, D.2, or D.3 or included in our discussion are the large number of reviews, tests, analyses, process checks, and milestones in each phase of a program's life cycle.

Recent Revisions

Acquisition policy has changed frequently in recent years. Underlying these changes is the strong dissatisfaction in Congress, DoD, and the military departments with the large number of acquisition programs that have failed to meet one or more of the following: delivery on schedule, acceptable life-cycle costs, or provision of expected capabilities. The revisions mandate new processes, such as attempts to integrate competitive prototyping at every stage of the life cycle, performance assessments and root-cause analyses, annual reviews of MDAP system engineering management plans, and additional program milestone reviews, as well as new and modified DoD organizations that are responsible for these processes and assurance of their use.

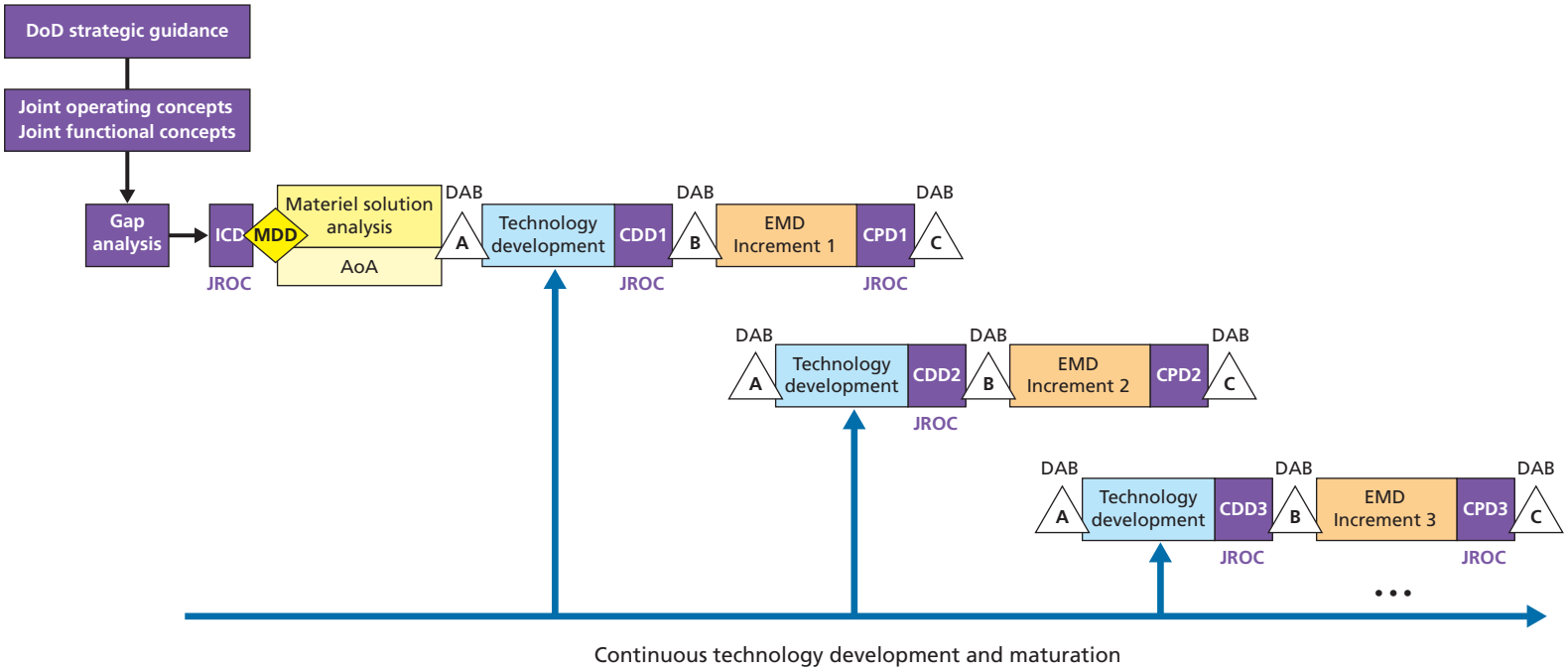
The net result is increased management complexity and increased nominal program length, with the expectation that lower program cost and improved technical capability will be delivered at an earlier date. In terms of schedule, this means that although the nominal program length is increased, the actual date on which acceptable deliveries will be provided will be earlier because the process reduces program schedule slippage by more than the nominal date was extended.

In summary, there is still the belief that program schedules can and should be reduced. For example, in 2010, then–Secretary of Defense Robert Gates expressed dissatisfaction with the planned schedule for the Army's ground combat vehicle, a program started in 2009. The schedule called for the first vehicle delivery within seven years. Secretary Gates believed that this could be accelerated by at least one year (Bennett, 2010).

---

[2] The first horizontal sequence in Figure D.3—from the creation of the initial capabilities document through Milestone C—is a section of what appears in Figure D.1. The production and deployment phase and the operations and support phase would follow the Milestone C shown in Figure D.3, as in Figure D.1. However, it is often the case that major acquisition systems take more than ten years to progress from statement of need to operation. Given that such systems are dependent on state-of-the-art technologies that evolve at rapid rates, a system could quickly become obsolete and no longer provide the superior warfighting capability necessary for success. Incremental acquisition avoids this by fielding systems in small increments—say, several years of production—followed by successive lots incorporating improved technology.

Figure D.3
Incremental Acquisition



RAND *TR1294-D.3*

Exceptions to JCIDS

The formal acquisition process is generic and meant to apply to the broad acquisition needs of DoD. However, it recognizes that there are times when it can be modified, or tailored, as a function of the product or service being acquired or the circumstances under which the acquisition is being pursued. Most prominent of these cases are the special terms for major software acquisition that apply when nonweapon system software, such as accounting or business records software, is to be installed on an existing computer (see DoDD 5000.01, 2007; DoDI 5000.02, 2008).

Urgently needed capabilities may need to be acquired rapidly—within weeks, months, or (at most) two years—to be effective. Under such circumstances, JCIDS has some provisions: While compliance with JCIDS is required for fielding long-term solutions, but this is not the case for short-term solutions. Specifically, the *Defense Acquisition Guidebook* (Defense Acquisition University, 2012b, para. 2.3.1.2) allows the PM and MDA to "tailor the phases and decision points to meet the specific needs of the program. Tailoring should consider program category, risk, urgency of need."

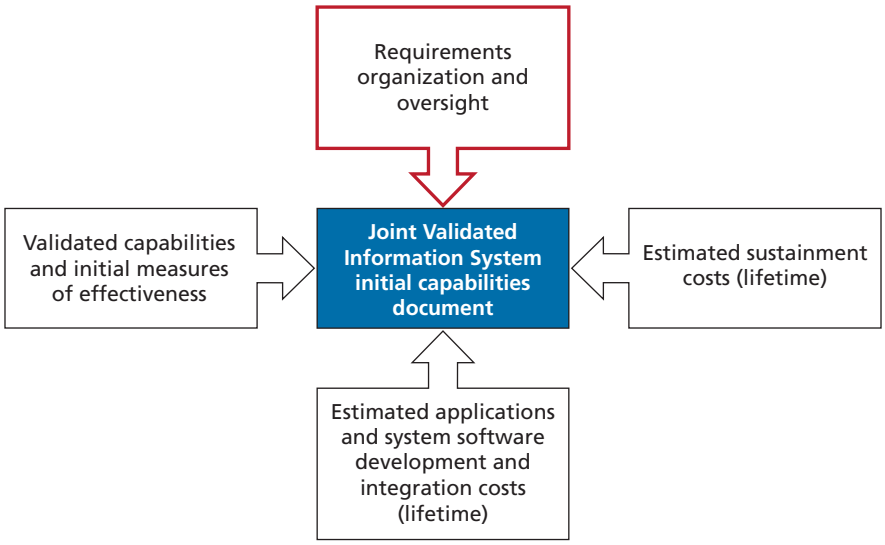
The JCIDS IT Box

The IT Box is a modified version of JCIDS designed specifically for IT programs. It was created because the current process "does not allow programs to provide the required flexibility to take full advantage of evolving commercial information technology" (U.S. Joint Chiefs of Staff, undated, p. 3). The IT Box model is intended to provide programs with "greater flexibility to incorporate evolving technologies, and achieve faster responses" (DoD, 2012, p. B-15). The previous version of the manual (January 31, 2011) was more specific:

> The purpose of the "IT Box" is to describe the overall bounds of an IT program in order to facilitate program initiation, as well as to reduce subsequent return trips to the JROC for approval of improved capabilities as the program is executed. The information in the chart will be provided to the JCB [Joint Capabilities Board]/JROC as part of the approval process for any IT program CDD [capability development document]. For programs beyond Milestone B, the IT Box will be included in the approval process for their CPD. The IT Box can be used for programs in which system costs exceed $15 million (including RDT&E and procurement). In addition, although hardware development is not permitted, software development is. The IT Box cannot be used for defense business systems or "systems which are an integral part of a weapon or weapon system which enables weapon capabilities and are considered part of the weapon system program. (U.S. Joint Chiefs of Staff, undated, p. 5)

Figure D.4 provides an illustration of the four sides of the IT Box, which present a program's pertinent requirements information to JCB and JROC members in an abbreviated form. General information included on the four-sided chart (as shown in Figure D.4) is as follows: organization and oversight of the program; lifetime sustainment costs; integration, application, and system software development; and validated capabilities and initial measures of effectiveness.

Figure D.4
Four Sides of the IT Box



SOURCE: DoD, 2012, p. B-17, Figure B.2.
RAND *TR1294-D.4*

Pros and Cons of the IT Box

The IT Box has been used for the past several years across the services. It is a relatively new acquisition concept, so lessons learned are still being collected. However, the Joint Chiefs of Staff provides the following guidance:

- Key performance parameters in IT program capability development documents should be briefed with "initial minimums" only, rather than traditional thresholds or objectives.
- Program acquisition unit cost and average procurement cost do not apply to IT acquisition; a different metric must be used.
- For incremental acquisition, ensure that the IT Box describes the entire IT program and not just a single increment, if possible (U.S. Joint Chiefs of Staff, undated, p. 14).

The Joint Chiefs of Staff also identified some pros to using the IT Box. The IT Box is "the right thing to do for IT programs" because it "provides required flexibility for IT program success and allows more effective support to the Warfighter." However, there must be close coordination among all parties for this concept to be successful (U.S. Joint Chiefs of Staff, undated, p. 15).

APPENDIX E

Review of Cyber and IT Acquisition Literature

The process of purchasing software and software-intensive goods has been the focus of ongoing debates and legislation. In this appendix, we briefly review the literature on this subject.

Legislation

WSARA enacted sweeping changes to the way in which acquisition is conducted, including establishing new program groups in OSD (such as Cost Assessment and Program Evaluation), eliminating old positions, and instituting new legal requirements for the way in which projects are managed. In the context of this legislation, there has been extensive discussion of the difference between MAIS programs and MDAPs. Additionally, the National Defense Act of 2010 adopted almost all of the recommendations set forth by a 2009 DSB study of IT purchasing (DSB, 2009a).

At a general level, the purchase of IT components is recognized as too slow to get modern tools into the hands of warfighters. Legislation and policy changes intended to address this problem have focused heavily on trying to speed up the purchasing process, recognizing that the uniform DoD 5000-series system for acquisition is too burdensome. The changes have attempted to adopt the best practices of the commercial sector and tailor them to the particular needs of the military.

Chief among the conceptual changes is a move toward what is called *agile development*. Agile processes emphasize the quick creation of smaller pieces of a potentially larger program. Large deliverables are broken into constituent units, which can then be prototyped and tested far more quickly than would be the case if the entire program had been built before testing occurred.

National Research Council Report

The 2010 NRC report *Achieving Effective Acquisition of Information Technology in the Department of Defense* focuses on software on COTS computers that is not embedded in weapon systems. The report's authors conclude that the DoD IT acquisition process is too lengthy compared with commercial systems developed using agile methods. There should be more focus on the product and less on oversight, paper, and processes. Products can be developed in pieces and then aggregated to both get the capabilities required and achieve better customer satisfaction. They also recommend that products be tested frequently by users. Some examples

cited in the report are Command Post of the Future, Tactical Ground Reporting System, Joint Network Node, Blue Force Tracker, and Force XXI Battle Command Brigade and Below.

Defense Science Board Report

A March 2009 report by the DSB Task Force on the Acquisition of Information Technology focuses on business systems; information infrastructure; command and control; intelligence, surveillance, and reconnaissance; embedded IT in weapon systems; and IT upgrades to fielded systems. It concludes that the JCIDS conventional process is too cumbersome and should be retained only for efforts requiring significant scientific, engineering, hardware development and for the integration of complex systems. A new acquisition policy for IT is needed, and a workforce must be trained for it. The acquisition policy recommended by the task force would produce the first increment of capability in three and a half years and subsequent increments in 18 months or less. The authors suggest that the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Vice Chairman of the Joint Chiefs of Staff should lead this effort, with support from the DoD Chief Information Officer, Office of Program Analysis and Engineering (now the Office of Cost Assessment and Program Evaluation), the Office of the Director of Defense Research and Engineering, OT&E personnel, the Office of the Under Secretary of Defense (Comptroller), users, and others.

Other Reports

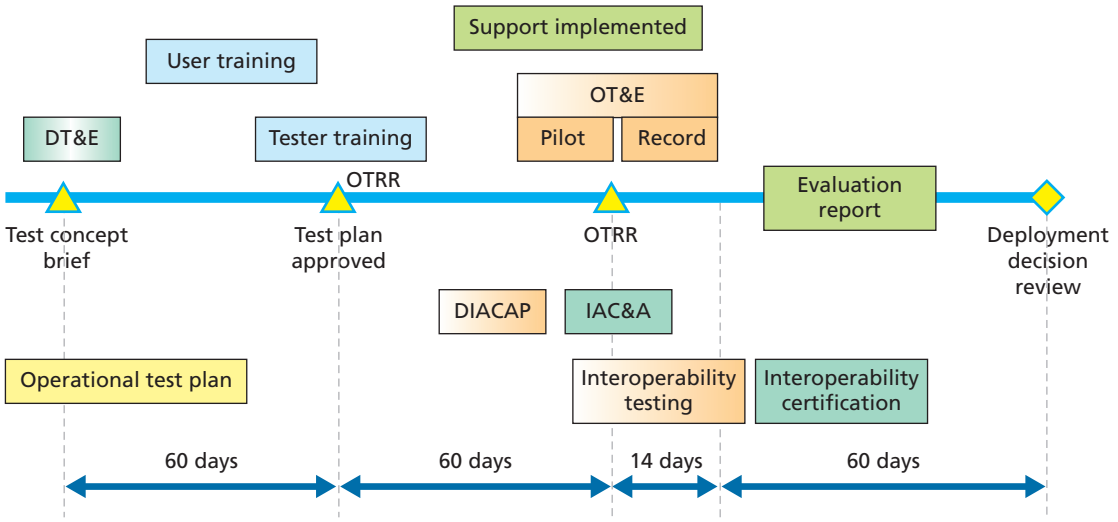
The new legislation and the DSB and NRC reports have set the stage to change the current acquisition process to one that is more agile and able to meet DoD IT needs. Although these reports set the path forward in their recommendations, they lack specific details on many facets of agile IT acquisition. Many others have written on the specific areas of funding, governance, testing, and fielding for agile IT acquisition. In this section, we highlight key publications that address the details of agile IT acquisition realization.

Testing

The literature advocates for a new test and evaluation model to enable agile IT acquisition. Currently, IT acquisition requires four types of testing activities that are conducted by separate organizations and approved by separate authorities: developmental testing, operational testing, interoperability testing, and IA testing. Hutchison (2010) illustrates some of the high-level activities across these four areas of testing, as shown in Figure E.1.

Current legislation and the DSB and NRC reports do not discuss testing in great detail, even though it can be a major inhibitor to agile IT acquisition (Campbell, 2010, p. 10). The DSB report does recommend "making schedule the priority for releasing available capability and not requiring (or expecting) a 'yes' vote from every functional organization prior to decision milestones" (DSB, 2009a, p. 48). The breadth of literature in the area of testing for agile IT acquisition discusses many specifics for meeting scheduling demands. These areas include acceptance of an 80-percent solution, integrated test teams, early prototyping and user involvement, continuous and integrated developmental and operational testing, proper risk-based testing, data collection, and streamlining documentation.

Figure E.1
Testing Activities for IT



SOURCE: Hutchison, 2010, p. 25.
NOTE: DT&E = developmental test and evaluation. OTRR = operational test readiness review.
RAND *TR1294-E.1*

The philosophy behind agile IT acquisition is to move away from the "big bang" (everything at once) and toward incremental releases of capability, such as the 80-percent solution (Hutchison, 2010, p. 22; DSB, 2009a, p. 36). To this end, Hutchison (2010) suggests that programs "build a little, test a little (learn a lot), field a little." Adopting this philosophy requires testing and experiments to identify the strengths and weaknesses of the system and allows enhancement initiatives through the increment's releases (Nair and Cohen, 2006, p. 3). Under this paradigm, testing should not be a pass/fail event but should make risk transparent so that decisionmakers can acknowledge and understand the risks as capabilities are released (DSB, 2009b, p. 25). In addition, DoD culture needs to adapt and accept that more frequent releases will "allow opportunities to continually address integration and interoperability issues" (DSB, 2009a, p. 50). Testing and releasing the 80-percent solution has long been a practice in the commercial sector when software capabilities are released with known bugs (Campbell, 2010, p. 17).

Early prototyping of IT capabilities and user involvement (i.e., in beta testing) is central to agile IT acquisition. Technologically savvy operational users should be involved in a continuous feedback process that starts early in the development stage and spans multiple releases of capabilities (AFEI, 2010, p. viii). The effectiveness of this early and continual user involvement depends on vendor support that is contractually specified (AFEI, 2010, p. viii). Furthermore, prototyping should support a strategy of "start small, scale rapidly" while continuously monitoring the performance of desired capabilities (Hutchison, 2010, p. 27). Early integration will expose design flaws, inadequacies, and failure modes early on, when the program is small and problems are easy to remedy (Nair and Cohen, 2006, p. 17). A DoD Inspector General report found that early user involvement and prototyping for Navy urgent needs—specifically, "working with the fleet to demonstrate prototype performance even before beginning the actual acquisition efforts"—has proved useful (DoD Inspector General, 2009, p. 16). New legislation and DoD policies strongly support early user involvement and

prototyping (Public Law 111-84, 2009; SECNAVIST 5000.2D, 2008; SECNAV M-5000.2, 2008; DoDI 5000.02, 2008).

An effective integrated test team (ITT) is required to eliminate inefficiencies during the IT testing process. The separate testing agencies and decision authorities for IT testing cause undue inefficiencies, delays, and unnecessary retesting (Hutchison, 2010, p. 23). Currently, IT acquisition is required to pass through four different stovepiped testing regimes governed by separate agents, as shown in Table E.1.

To enable agile IT acquisition, the separate IT test organizations and decision authorities should be integrated, or at least synchronized, to avoid unnecessary testing delays (Hutchison, 2009, p. 9; Mosser-Kerner, 2010, p. 5). Rieken and Gunderson (2010) identified this as a major inhibitor in PEO C4I. Specific ITT models have been put forth by OSD and the Defense Information Systems Agency (DISA) (Hutchison, 2009, p. 8; Mosser-Kerner, 2010, p. 8). Table E.2 highlights the major elements of the OSD and DISA test team models.

ITT involvement needs to start very early in the acquisition process. Early involvement of the ITT is necessary to reduce the risk of surprises in the late stages of acquisition (Wilson, Mosser-Kerner, and Wissink, 2010, p. 3). Elements of the ITT should be involved in the requirements process to help focus requirements on mission accomplishment and testability (Quintrall, 2010, p. 17). NRC (2010a, p. 58) suggests that this involvement happens before coding begins. The *Defense Acquisition Guidebook* places the responsibility on the PM to coordinate the different testing activities into an efficient continuum, but DoD policy, in general, lacks in terms of fully integrating IA and interoperability testing into a single testing continuum as advocated by the literature (Defense Acquisition University, 2012).

One strategy for integration currently in use and supported by policy is integrated developmental and operational testing. OSD defines integrated testing as "the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation and reporting by all stakeholders particularly the develop-

Table E.1
IT Test Agents and Authorities

Activity	Test Agent	Conditions	Customer	Reference
DT&E	Program management office/ contractor/government developmental test organization	As determined by program management office	Program management office	DoD 5000 series
OT&E	Operational test agency	Operationally realistic, typical users	MDA	Title 10; DoD 5000 series
Joint Interoperability Test Certification	Joint Interoperability Test Command	Applicable capability environments	J6 (Command, Control, Communications, and Computers)	DoDD 4630.5; DoDI 4630.08; CJCSI 6212.01D
Security test and evaluation (IA C&A)	Operational test agency; Defense Intelligence Agency; Field Security Office; National Security Agency	Operational, lab	Designated approving authority	DoDI 8510.01; DIACAPa

SOURCE: Hutchison, 2009, p. 9.

[a] DIACAP C&A does not complete the requirement for IA testing according to the policy of OSD's Office of the Director of Operational Test and Evaluation.

Table E.2
OSD and DISA Test Team Models

OSD Integrated Test Team Model	DISA Capability Test Team Model
DT&E, OT&E, IA, interoperability, program management office, system engineering personnel; defines roles and responsibilities	Accommodates "sprint" IT acquisition by integrating DT&E and OT&E, C&A, and interoperability testing into one team
Establishes new test and evaluation model based on ACATs	Philosophy of the capability test and evaluation team strategy is "one team, one time, one set of conditions"
Creates innovative approaches to testing	Test events are risked-based
Test strategies based on risk assessments and capability definitions that govern test intensity and type	One report is provided to all decision authorities: MDA, decision accreditation authority, and interoperability certifier
Data management strategy to collect and disseminate meaningful data to stakeholders	Decision authorities sign one test and evaluation master plan
Test and evaluation process is scalable, repeatable, rigorous, and aligned with risk and IT cycle times	Test designs are mission-focused to ensure buy-in from all authorities
Test team has necessary expertise	Utilizes beta testing with users that includes mature support structure

ment and operational test and evaluation communities" (McQueary and Finley, 2008, p. 1). In addition to integrated testing, agile IT acquisition requires testing that "executes continuously as capabilities are developed" (Campbell, 2010, p. 13). Continuous testing needs to be guided by one overarching approach that has the flexibility to cover all the planned capabilities in the increment (Campbell, 2010, p. 12). Because the test documentation is time-consuming, requiring approximately 60 days to complete, Campbell (2010, p. 18) suggests using simple stoplight tables to quickly and efficiently report test results, as shown in Table E.3. Automated testing should also be included in the continuous testing strategy that allows previous functionality to be iteratively tested (AFEI, 2010, p. viii).

DOT&E policy establishes the extent of developmental and operational testing that a program must complete by two risk factors: failure potential and mission impact (Office of the Director of Operational Test and Evaluation, 2003, p. 11). Agile IT acquisition adds another risk dimension due to its tight scheduling demands—that is, the risk of delayed capability. Mosser-Kerner (2010, slide 10) advocates that T&E processes should be scalable, repeatable, and rigorous while aligning with the assessed risk level and schedule demands of agile IT. Campbell (2010, p. 17) stresses that testing should correlate with the risk of new *added* functionality. The DSB has identified "risk-adverse" cultural barriers that need to be realigned to match actual risk levels (DSB, 2009b, p. 25). Hutchison (2009, p. 8) advocates that testing should focus on critical risk factors based on the type of acquisition being pursued (GOTS, COTS, or new development), as shown in Table E.4.

Governance

The governance and leadership required for agile IT acquisition pose many challenges under the current structure and authorities established in the DoD 5000-series acquisition process. The agile IT acquisition literature concerning governance discusses open architecture, proper empowerment and oversight, proper training and knowledge, unnecessary redundancy, and single decision authorities.

Table E.3
Example of Streamlined Operational Testing Documentation

	Mission Statement: System T supports strategic and satellite communication across the full range of military operations			
Key Performance Parameter or Support	**Does System T enable communication over XMS, XLT, and FLT/EE satellite constellations?**	**Does System T support satellite and payload control?**	**Can System T be maintained to meet mission taskings?**	**Can System T be sustained to meet mission taskings?**
Operations capability	G		G	G
Interoperability	R			
Strategic services quality	G			
Capacity	Y			
Communication security	R			
Communication quality	G			
Survivability	G		G	
Satellite control quality				
Payload control quality				
Maintainability			G	
Reliability			R	
Availability			Y	G
Information assurance				R
Logistics supportability				Y
Training quality				Y
Compatibility				

SOURCE: Campbell, 2010, p. 18.

NOTE: Light shading indicates that the capability is "effectiveness-centric"; dark shading indicates that the capability is "suitability-centric"; no shading indicates an operational capability.

Table E.4
IT Testing, by Critical Risk Factor

IT Acquisition Strategy	Capability Maturity/Risk	Critical Test and Evaluation Issues
Adopt	Capability in use in DoD	Scalable performance and support
Buy	Capability in use in commercial sector	Scalable performance and support; secure; interoperable
Create	New capability to be developed	Scalable performance and support; interoperable; effective, suitable, and survivable

SOURCE: Hutchison, 2009, p. 8.

Agile IT acquisition is an iterative approach to delivering capabilities in short cycle times. The effective use of open-architecture principles is necessary to ensure that future releases will seamlessly integrate into the system (DSB, 2009b, p. 35). Boudreau (2006, p. xv) presents a detailed case study of the A-RCI/Advance Process in Build and the use of a modular open-system approach. The approach was successful because interfaces, standards, and protocols were rigorously controlled. This governance disciple ensured that A-RCI models worked together properly.

Another element that made A-RCI a success was the mandate, empowerment, and the top cover that senior leadership provided. Due to budget constraints and the critical need for new capabilities, senior leadership established a mandate to "make something happen." With this mandate, senior leadership empowered midlevel leaders and managers by providing top cover and the freedom to innovate. This balanced strategy yielded significant performance and logistic improvements for A-RCI, despite obstacles caused by operational testing and JCIDS reviews (Boudreau, 2006, p. 28).

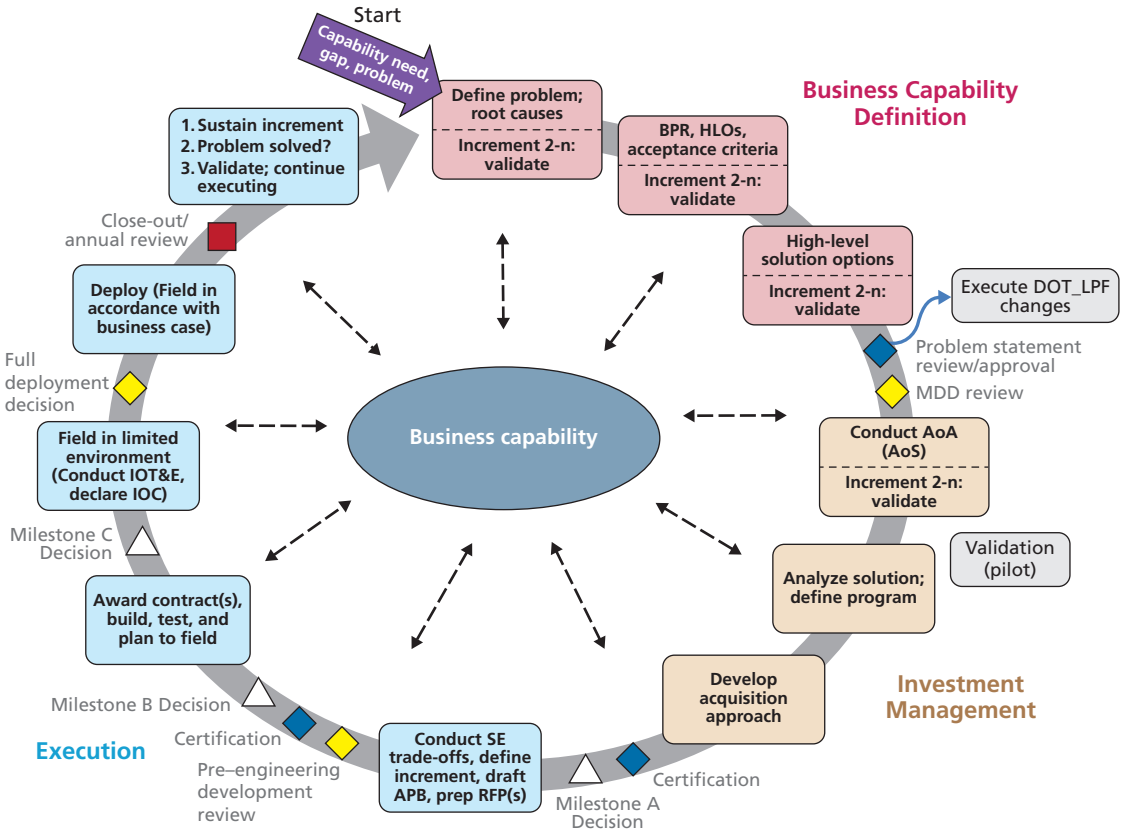
Another important aspect of governance in agile IT acquisition is ensuring that all players are properly trained and knowledgeable. A foremost challenge posed by urgent acquisition is a lack of understanding about the process among the people involved, which can cause unnecessary delays and escalations (DoD Inspector General, 2009, p. 13). McCarthy (2010) observed that inadequate training and proficiency among PMs and vendors, especially in the areas of IA and interoperability, can cause preventable problems to arise in the later stages of the acquisition process.

As illustrated by the multiple test organizations involved in IT acquisition, discussed earlier in this appendix, multiple authorities cause undue redundancies and delays (OSD, 2010, p. 5). The BCL framework, which has been used for the acquisition of defense business capabilities, merges three major DoD processes and authorities: requirements, acquisition, and funding authorities (i.e. JCIDS, operation of the Defense Acquisition System, and the Investment Review Board/Defense Business System Management Committee; Business Transformation Agency, undated). OSD (2010, p. 4) lists the following benefits to the BCL model:

- It provides an effective model for consolidating oversight requirements, acquisition, and funding.
- Program documentation is streamlined and effective.
- Streamlined governance and tiered accountability provide noticeable efficiencies.
- Program implementation strategies are flexible and effective.

- Independent risk assessment is balanced.
- In 2010, then–Under Secretary of Defense for Acquisition, Technology, and Logistics Ashton Carter approved the use of the BCL model for business defense systems as part of DoD's implementation of the agile IT acquisition process (Carter, 2010c, p. 1). Figure E.2 shows a high-level schematic of the BCL process.

Figure E.2
BCL Process



SOURCE: Office of the Deputy Chief Management Officer, 2012, slide 6.

NOTE: DOT_LPF refers to nonmateriel solutions (i.e., doctrine, organization, training, materiel, leadership and education, personnel, and facilities, or DOTMLPF, but without the "materiel" component).
APB = acquisition program baseline. BPR = business process reengineering. HLO = high-level outcome. RFP = request for proposal. SE = systems engineering.

RAND *TR1294-E.2*

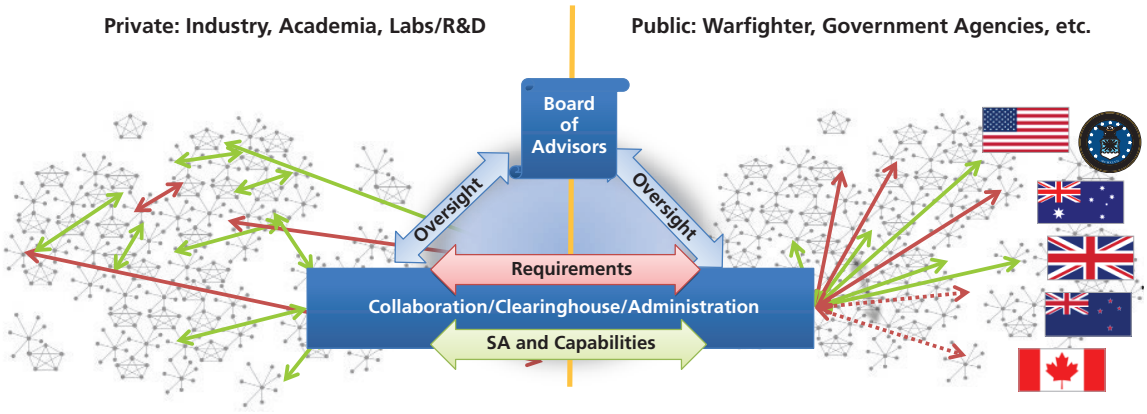
APPENDIX F

Air Force Cyber Acquisition

The Air Force has considered multiple acquisition approaches at various operational tempos (OPTEMPOs) for cyber programs. It also has explored novel ways to formalize a public-private brokerage to leverage the speed and agility of private industry. According to Riley Repko, senior adviser for cyber operations and transformation to the Air Force Deputy Chief of Staff for Operations, Plans, and Requirements (2009, p. 1), "An effective way to deal collectively with threats from cyberspace is through public-private collaboration and investment."

The term *Big Safari* refers to an Air Force rapid procurement effort that has been used successfully for the MC-12W aircraft. This success spurred some in the Air Force to try to extend the concept to the cyber domain. The term *Cyber Safari* was coined for this variation on the Air Force's Big Safari approach. Some of the aforementioned ideas are presented in Figures F.1 and F.2.

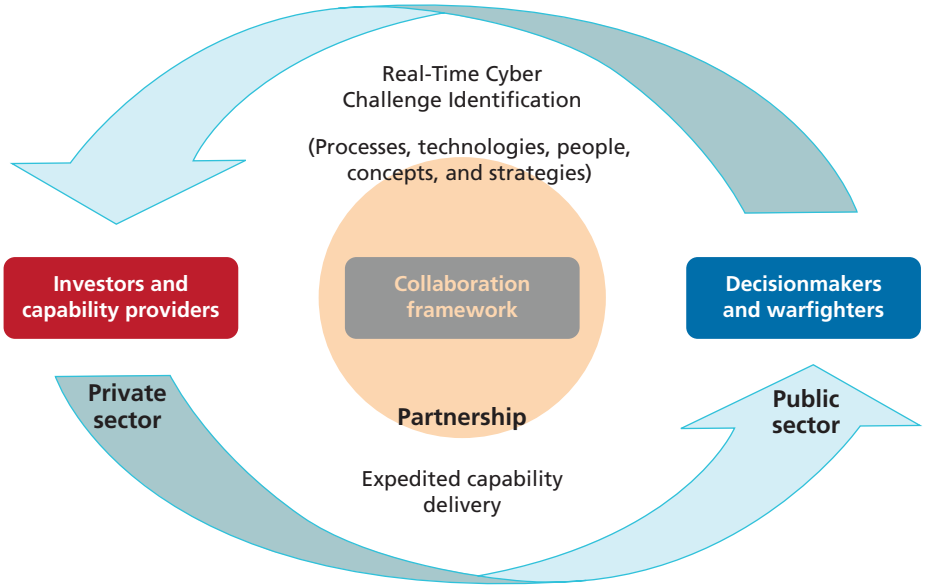
Figure F.1
Illustration of Desired Collaboration for Air Force Cyber Acquisition



SOURCE: Repko, 2009, p. 6.

RAND *TR1294-F.1*

Figure F.2
Potential Private-Sector Partnership Roles in Air Force Cyber Acquisition



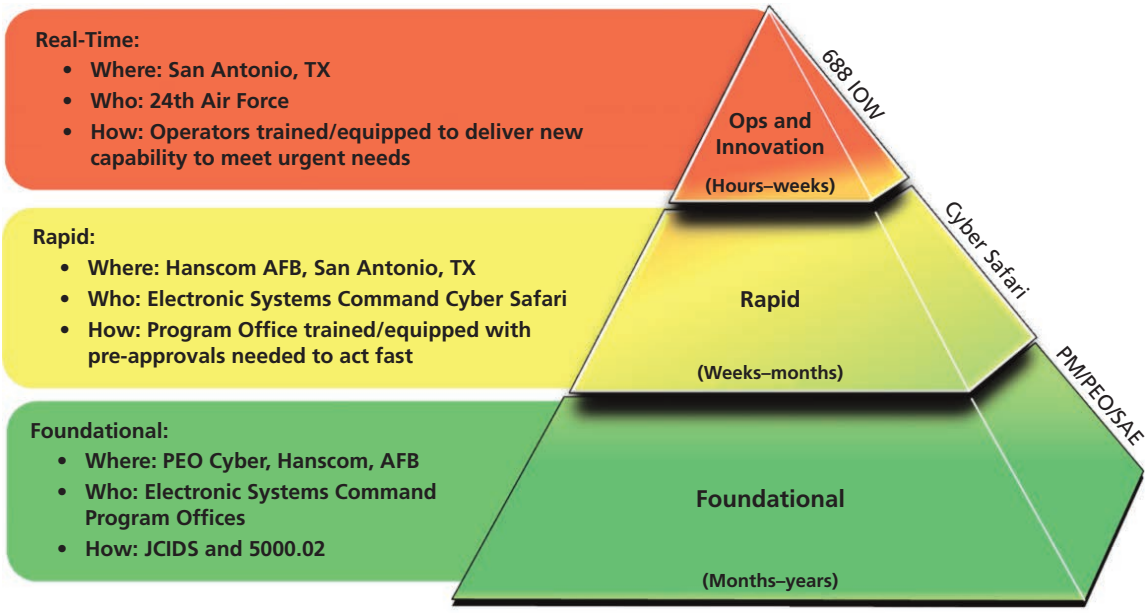
SOURCE: Repko, 2009.
RAND *TR1294-F.2*

Recognizing the Need for Varying OPTEMPOs

The need for varying acquisition speeds has been a central consideration,[1] as demonstrated in Figures F.3 and F.4. Three OPTEMPOs are identified in the figures: hours to weeks, weeks to months, and months to years. Under this concept, the fastest OPTEMPO requires work to be done in-house (by the 688th Information Operations Wing). The medium-speed effort is to be handled by the proposed Cyber Safari organization. Traditional program management offices are to handle the programs with the slowest OPTEMPOs.

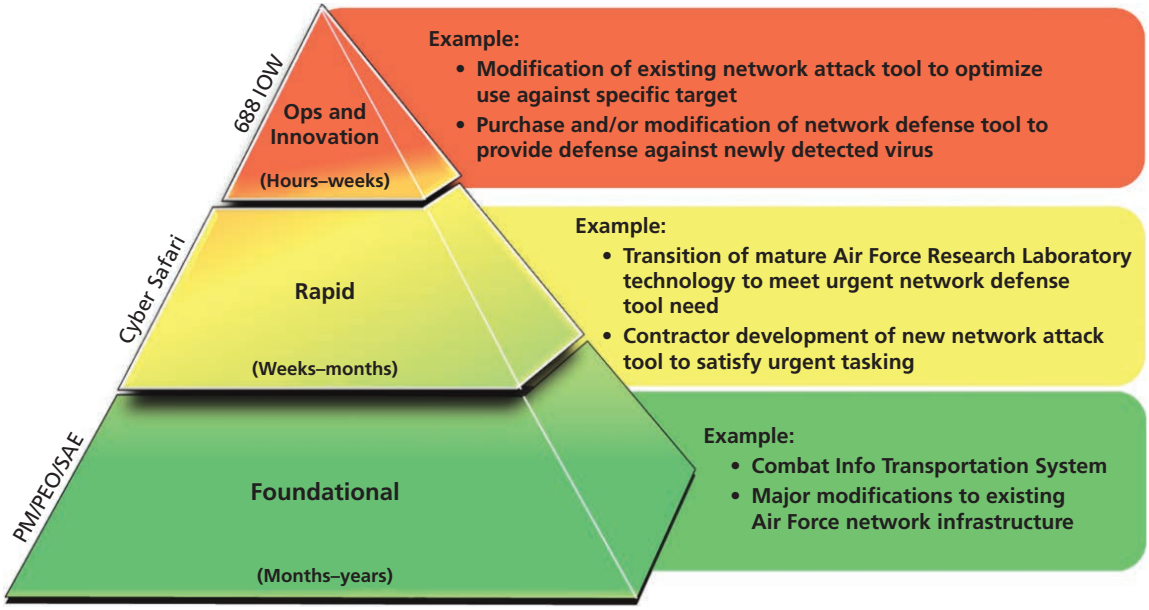
[1] Larry Coe at Air Force Materiel Command's Electronic Systems Center at Hanscom Air Force Base, who assisted us over the course of this project, has been a primary advocate of this viewpoint.

Figure F.3
Air Force Cyber Acquisition OPTEMPO Considerations



SOURCE: Kehler and Hoffman, undated.
NOTE: SAE = service acquisition executive.
RAND *TR1294-F.3*

Figure F.4
Air Force Cyber Acquisition Considerations with Examples



SOURCE: Kehler and Hoffman, undated.
RAND *TR1294-F.4*

APPENDIX G

Worms

In this appendix, we provide background on computer worms, the threat they pose, and the vulnerabilities they can exploit.

A worm is an unwanted software program that is surreptitiously implanted to allow someone else to control a computer or system. As defined at the Army's Information Assurance Training Center (undated), "A worm is stand-alone software that does not require a host file to propagate. It doesn't even require human interaction; the computer merely needs to be turned on with its services running." To defend computers against worms, the typical course of action is to patch them with special "anti-malware" code for each worm and each of its variations.[1]

Agent.btz

Agent.btz was a worm that successfully compromised classified military computer networks in 2008. According a 2008 *Los Angeles Times* article, Agent.btz was malicious software (malware) that was able to spread to any flash drive plugged into an infected computer and was specifically designed to attack military networks (Barnes, 2008).[2]

In an article published in *Foreign Affairs*, then–Deputy Secretary of Defense William Lynn described the events as follows:

> [An] infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. (Lynn, 2010)

According to Lynn, it was "the most significant breach of U.S. military computers ever." This risk of spreading the malware to other networks prompted the military to ban the drives.

[1] For additional background on worms and their characteristics, see Porche, Sollinger, and McKay, 2011.

[2] As defined by the Army's Information Assurance Training Center (undated), "Malware is an acronym that stands for malicious software and it comes in many forms. Generally speaking, malware is software code or snippets of code that is designed with malice in mind and usually performs undesirable actions on a host system."

Conficker

Conficker is a worm that may be amassing a massive botnet ("Conficker Worm Stealing Identitites," 2009).[3] The purpose of this botnet is unclear. According to a Symantec report, it is a highly sophisticated worm that automatically propagates and shields itself from the effects of certain network defenses (Falliere, Murchu, and Chien, 2011). It is certainly capable of orchestrating a massive distributed denial-of-service attack (or even just an effective spam campaign).

The worm is smart: It is programmed to avoid Internet protocol addresses belonging to security companies, and it uses encryption to disguise what it is trying to do. The worm directs machines that share this malware to communicate with each other so the worm can update itself. In this way, it is constantly morphing.

Like Agent.btz, Conficker can infect hosts or computers via removable drives (e.g., portable flash drives). Microsoft has offered hundreds of thousands of dollars for information on the developers of Conficker.

Stuxnet

The Stuxnet worm, discovered in 2010, targeted Iranian nuclear facilities (see Falliere, Murchu, and Chien, 2011). By many accounts, the worm was intended to allow its authors to control the Siemens machinery that operates Iranian nuclear power plants, despite the fact that these controllers are not directly connected to the Internet. The worm was apparently capable of causing harm even without direct human control. In other words, it was embedded with the instructions it needed to cause the desired effect. This is a serious innovation and a potentially effective means of cyber attack.

Unlike Agent.btz and Conficker, Stuxnet appears to have been designed to cause kinetic effects (i.e., physical destruction). Furthermore, it was could not only compromise standard laptops and operating systems, but it was able to take control of proprietary industrial systems. Worse, it targeted specific devices in specific locations. It is the malware equivalent of a precision-guided missile. In a sense, its existence is proof that any "smart" device with a processor and memory can be targeted.

For this reason, Stuxnet represents a vexing new threat. Industrial controllers are clearly vulnerable, as are processors inside individual tanks, vehicles, and, of course, desktop computers, and all of these systems could be targeted. A direct connection to the Internet is not a precondition for vulnerability to such a cyber attack.

Worms mutate quickly. Each mutation of a worm requires new software to protect against it. A skilled adversary can create strains on a daily basis in response to patches. For these reasons, we conclude that the speed of acquisition of cyber is uniquely fast within the realm of IT acquisition.

---

[3] Conficker is also known as a variant A of Win32.Donadup. Botnets, or bot networks, are made up of vast numbers of compromised computers that have been infected with malicious code and can be remotely controlled through commands sent via the Internet (Wilson, 2008, p. 5). They can be used by state actors or criminals to execute a distributed denial-of-service attack or to produce spam, or for some other nefarious purpose.

Zero-Day Exploits

A so-called zero-day exploit is a term for any malware that exists but has not been seen and thus has no signature.[4] Stuxnet is an example of a zero-day exploit. Network defense approaches that rely on signatures to detect an attack are prevalent. Zero-day exploit attacks stand a great chance of going undetected long after damage has been done. This means that the need to react to a zero-day exploit, once it is eventually discovered, must be measured in hours or days because damage (or the potential for damage) is accumulating.[5] By some accounts, the Iranian government took many months to discover and respond to Stuxnet after it was discovered.

This discussion of emerging threats to IT systems makes clear that acquisition in this area must be not only quick and agile but also sophisticated, responsive, and highly predictive.

---

[4] A signature is a recognizable pattern or characteristic of malware that allows antivirus software or other intrusion detection systems to spot it.

[5] The damage could be malware-guided physical destruction of a computer-controlled device or system or the loss of classified or sensitive data.

Bibliography

AFEI—*See* Association for Enterprise Information.

Air Force Instruction 63-114, *Quick Reaction Capability Process*, Washington, D.C., January 4, 2011.

Association for Enterprise Information, *Industry Perspectives on the Future of DoD IT Acquisition*, Arlington, Va., 2010.

Barnes, Julian E., "Pentagon Computer Networks Attacked," *Los Angeles Times*, November 28, 2008. As of October 19, 2012:
http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28

Bennett, John T., "Gates: Speed FCS Replacement, Define Future USMC Role," *DefenseNews*, May 7, 2010.

Boudreau, Michael, *Acoustic Rapid COTS Insertion: A Case Study in Spiral Development*, Monterey, Calif.: Naval Postgraduate School, October 30, 2006.

———, "Brief for Dr. Porche visit 5-13-10," briefing, May 13, 2010.

Business Transformation Agency, U.S. Department of Defense, "Business Capability Lifecycle (BCL)," web page, undated. As of October 19, 2012:
http://www.bta.mil/products/bcl.html

Campbell, Robert C., Jr., *Developing a More Flexible Operational Test and Evaluation Process for Information Technology*, thesis, Maxwell AFB, Ala.: Air War College, Air University, February 17, 2010.

Carter, Ashton B., Under Secretary of Defense for Acquisition, Technology, and Logistics, "Approval of Integrated Strategic Planning and Analysis Network (ISPAN) Increment 2," memorandum, March 29, 2010a.

———, "Directive-Type Memorandum (DTM) 09-027: Implementation of the Weapon Systems Acquisition Reform Act of 2009," memorandum, incorporating change 1, October 21, 2010b.

———, "Interim Acquisition Guidance for Defense Business Systems (DBS)," memorandum, November 15, 2010c.

Claggett, David, "Joint Rapid Acquisition Cell," briefing, Defense Intelligence Agency acquisition conference, "Capability Partners in the Global War on Terror," May 16, 2007.

Cluck, James, Director, Center for Acquisition and Logistics, U.S. Special Operations Command, "SOCOM Acquisition Perspective to NDIA," briefing, March 20, 2009. As of October 18, 2012:
http://www.ndia-cfl.org/news/defense_forum/2009/SOAL_NDIA_20Mar09v2.pptx

"Conficker Worm Stealing Identities," United Press International, April 13, 2009.

Defense Acquisition University, "Automatic Identification System (AIS), Rapid Deployment Capability (RDC), Lessons Learned," August 7, 2006. As of October 19, 2012:
https://acc.dau.mil/CommunityBrowser.aspx?id=107863

———, "CDD, CPD Evolutionary Acquisition Increments," *ACQuipedia*, last updated September 26, 2012a. As of November 10, 2012:
https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=0c92a060-9d07-4847-bbdf-b11f30d900f7

———, *Defense Acquisition Guidebook*, Ft. Belvoir, Va., October 9, 2012b. As of October 19, 2012:
https://dag.dau.mil/Pages/Default.aspx

Defense Science Board, *Report of the Defense Science Board Task Force on Defense Software*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 2000. As of October 19, 2012:
http://www.acq.osd.mil/dsb/reports/ADA385923.pdf

———, *Report of the Defense Science Board Task Force on 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 2009a. As of October 19, 2012:
http://www.acq.osd.mil/dsb/reports/ADA498375.pdf

———, *Report of the Defense Science Board Task Force on the Fulfillment of Urgent Operational Needs*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 2009b. As of October 19, 2012:
http://www.acq.osd.mil/dsb/reports/ADA503382.pdf

Deneault, Leslie, Defense Acquisition University, "Contracting in a Changing Environment," briefing, undated.

Dillard, John T., and David N. Ford, *From Amorphous to Defined: Balancing Risks in Evolutionary Acquisition*, Ft. Belvoir, Va.: Defense Acquisition University, October 2009.

DoD—*See* U.S. Department of Defense.

DoDD—*See* U.S. Department of Defense Directive.

DoDI—*See* U.S. Department of Defense Instruction.

Drezner, Jeffrey A., Megan McKernan, Douglas Shontz, Shara Williams, and Marc Robbins, *Rapid Acquisition of Army Command and Control Systems*, unpublished RAND research, 2011. Not available to the general public.

DSB—*See* Defense Science Board.

Etter, Delores M., Assistant Secretary of the Navy for Research, Development, and Acquisition, "Rapid Deployment Capability Acquisition Process," memorandum, December 4, 2006.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," version 1.4, Cupertino, Calif.: Symantec Corporation, February 2011. As of October 31, 2011:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Gansler, Jacques S., and William Lucyshyn, *Commercial-Off-the-Shelf (COTS): Doing It Right*, College Park, Md.: Center for Public Policy and Private Enterprise, University of Maryland, September 2008.

GAO—see U.S. Government Accountability Office.

Grace, Joseph A., "Time for Government to Dump Its 8-Tracks," *Signal Magazine*, February 2011. As of October 18, 2012:
http://www.afcea.org/content/?q=node/2529

Greenert, VADM Jonathan W., Vice Chief of Naval Operations, and Delores M. Etter, Assistant Secretary of the Navy for Research, Development, and Acquisition, "Navy Urgent Needs Process Implementation," memorandum, July 26, 2007.

Harp, Tim, Deputy Assistant Secretary of Defense for C3ISR and IT Acquisition, keynote address at MITRE 12th semiannual Software Assurance Forum, McLean, Va., March 10, 2010.

Harris, VADM Harry, "Memorandum for CNO," September 18, 2008.

Hetkey, Scott, NMP Interests, *Spiral Software Development, Emergent SCD Process, IAVA Requirements, SCD Revision Process, and ST1/ST2 Implementation*, Program Executive Office for Command, Control, Communications, Computers and Intelligence, July 21, 2010. Not available to the general public.

Hutchison, Steven, "Test and Evaluation and the ABCs: It's All About Speed," *ITEA Journal*, Vol. 30, No. 1, March 2009, pp. 7–10.

———, "Test and Evaluation at the Speed of Need," *Defense AT&L*, March–April 2010, pp. 21–27.

Information Assurance Training Center, U.S. Army Signal Center, "Information Assurance Fundamentals (IAF) Training, Lesson 6: Malware," web page, undated. As of October 19, 2012: https://ia.signal.army.mil/IAF/IASOLesson6.asp

Ittig, Kristen, Ronald A. Schecter, and Suzanne Sivertsen, "House Armed Services Committee Unanimously Approves Defense Acquisition Reform," Arnold and Porter LLP, April 2010.

Johnson, William M., "The A-RCI Process—Leadership and Management Principles," *Naval Engineers Journal*, Vol. 116, No. 4, October 2004, pp. 99–106.

———, "ARCI—A Historical Perspective," briefing presented to the Submarine Sonar Technology Panel, July 2007.

Kehler, Gen C. Robert, and Gen Donald Hoffman, U.S. Air Force, "Cyber Update and Way Ahead," briefing, undated.

Kenyon, Henry S., "Collaboration Enables Strategic Missions," *Signal Magazine Online*, January 2, 2010. As of October 18, 2012: http://www.afcea.org/content/?q=node/2157

LaRussa-Martin, Christina, *PMW 160 Tactical Networks Testing LSS Define-Improve Toll Gate*, U.S. Navy Program Executive Office Command, Control, Communications, Computers and Intelligence, September 30, 2010.

Lazarski, CDR Ed, Program Executive Office Command, Control, Communications, Computers and Intelligence, PMW 130.2, "Computer Network Defense Increment 2: Acquisition Coordination Team (ACT) Brief," briefing, November 23, 2010. Not available to the general public.

Lynn, William III, Deputy Secretary of Defense, "Defending a New Domain," *Foreign Affairs*, September–October 2010, pp. 97–108.

Marine Corps Order 3900.17, *The Marine Corps Urgent Needs Process (UNP) and the Urgent Universal Need Statement (Urgent UNS)*, Washington, D.C., October 17, 2008.

McCarthy, Bill, Deputy Director, U.S. Navy Operational Test and Evaluation Force, "2010 NDIA T&E Symposium OTA Commanders' Roundtable: A Navy Perspective on Information Assurance—Having Systems That Work When Needed," briefing, March 2, 2010. As of November 9, 2012: http://www.dtic.mil/ndia/2010test/TuesdayBillMcCarthy.pdf

McQueary, Charles E., and James I. Finley, *Definition of Integrated Testing*, Washington D.C.: Office of the Secretary of Defense, 2008.

Mishory, Jordana, "Pentagon to Include IT-Acquisition Templates in 5000.02 Revision," *Inside the Pentagon*, July 7, 2011.

Mosser-Kerner, Darlene, "Defense Information Technology: An Integrated T&E Model," briefing presented at the Annual Naval Postgraduate School Acquisition Research Symposium, May 12, 2010.

Nair, Vijay, and Michael L. Cohen, eds., *Testing of Defense Systems in an Evolutionary Acquisition Environment*, Washington, D.C.: National Academies Press, 2006.

National Research Council, *Achieving Effective Acquisition of Information Technology in the Department of Defense*, Washington, D.C.: National Academies Press, 2010a.

———, *Information Assurance for Network-Centric Naval Forces*, Washington, D.C.: National Academies Press, 2010b.

Naval Network Warfare Command, *New C&A Process Guide*, version 1.0, 2008.

NRC—*See* National Research Council.

O'Neill, Malcolm Ross, Assistant Secretary of the Army for Acquisition, Logistics, and Technology, "Army Acquisition Challenges and Opportunities," briefing presented at the National Defense Industrial Association Executive Seminar, April 20, 2010. As of October 18, 2012: http://www.dtic.mil/ndia/2010Atlanta/ONeill.pdf

Office of the Deputy Chief Management Officer, U.S. Department of Defense, "BCL Overview," briefing, July 2012.

Office of the Director of Operational Test and Evaluation, Office of the Secretary of Defense, *Guidelines for Conducting Operational Test and Evaluation for Software-intensive Systems*, Washington, D.C., June 16, 2003.

Office of Naval Research, "Future Naval Capabilities (FNCs)," web page, undated(a). As of October 18, 2012: http://www.onr.navy.mil/en/Science-Technology/Directorates/Transition/Future-Naval-Capabilities-FNC.aspx

———, "Rapid Technology Transition (RTT) Program," web page, undated(b). As of October 18, 2012: http://www.onr.navy.mil/Science-Technology/Directorates/Transition/Technology-Transition-Initiatives-03TTX/Rapid-Technology-Transition-RTT.aspx

———, "Small Business Innovation Research (SBIR)/Small Business Technology Transfer (STTR)," web page, undated(c). As of October 18, 2012: http://www.onr.navy.mil/en/Science-Technology/Directorates/Transition/SBIR-STTR.aspx

———, "SwampWorks," web page, undated(d). As of October 18, 2012: http://www.onr.navy.mil/Science-Technology/Directorates/office-innovation/swampworks-innovation.aspx

———, "Technology Insertion Program for Savings (TIPS)," web page, undated(e). As of October 18, 2012: http://www.onr.navy.mil/Science-Technology/Directorates/Transition/Technology-Transition-Initiatives-03TTX/Technology-Insertion-Program-Savings-TIPS.aspx

———, "TechSolutions," web page, undated(f). As of October 18, 2012: http://www.onr.navy.mil/Science-Technology/Directorates/office-innovation/tech-solutions-innovation.aspx

Office of the Secretary of Defense, *A New Approach for Delivering Information Technology Capabilities in the Department of Defense*, Washington, D.C., November 2010. As of October 19, 2012: http://dcmo.defense.gov/documents/OSD%2013744-10%20-%20804%20Report%20to%20Congress%20.pdf

ONR—*See* Office of Naval Research.

OSD—*See* Office of the Secretary of Defense.

Paul, Christopher, Isaac R. Porche, and Elliot Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces*, Santa Monica, Calif.: RAND Corporation, forthcoming.

Penderbrook Associates, "Representative Projects: System Lifecycle/Sustainment Support," web page, undated. No longer available.

PEO C4I—*See* Program Executive Office, Command, Control, Communications, Computers and Intelligence.

Poor, Bob, and Randy Case, "Rapid Deployment Capability in Action: The Automatic Identification System," *Defense AT&L*, November–December 2006, pp. 20–23.

Porche, Isaac R. III, Elliot Axelband, Bruce J. Held, Jerry M. Sollinger, and Christopher Paul, *Cyber Acquisition for the Army*, unpublished RAND research, 2011.

Porche, Isaac R. III, James Dryden, Kathryn Connor, Bradley Wilson, Shawn McKay, Kate Giglio, and Juan Montelibano, *Finding Services for an Open Architecture: A Review of Existing Applications and Programs in PEO C4I*, Santa Monica, Calif.: RAND Corporation, MG-1071-NAVY, 2011. As of October 18, 2012: http://www.rand.org/pubs/monographs/MG1071.html

Porche, Isaac R. III, Jerry M. Sollinger and Shawn McKay, *A Cyberworm that Knows No Boundaries*, Santa Monica, Calif.: RAND Corporation, OP-342-OSD, 2011. As of October 19, 2012: http://www.rand.org/pubs/occasional_papers/OP342.html

Program Executive Office, Command, Control, Communications, Computers and Intelligence, "Modernization Process," briefing provided to the authors, undated.

Program Manager, Warfare PMW 160, "Host-Based Security System (HBSS) Accelerated Fielding Proposal, Version 3.0," June 2010. Not available to the general public.

Prothero, Greg, Defense Acquisition University, "Developing Requirements," briefing, course CLR 252, undated.

Public Law 111-84, The National Defense Authorization Act for Fiscal Year 2010, October 28, 2009.

Quintrall, Mickey, Office of Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, "Integrated Testing and Independent Evaluation Using Design of Experiments," briefing presented at National Defense Industrial Association Test and Evaluation Conference, March 3, 2010.

Repko, Riley, "The Collaboration Imperative for Cyberspace Stakeholders," white paper, Office of the Air Force Deputy Chief of Staff for Operations, Plans, and Requirements, 2009.

Rieken, Dan, and Chris Gunderson, *PEO C4I Position Paper Re Accelerated IT On-Boarding via Enhanced Cybersecurity Posture*, unpublished working paper, November 3, 2010.

Roby, Cheryl J., Acting Assistant Secretary of Defense for Networks and Information Integration, "Approval of Integrated Strategic Planning and Analysis Network (ISPAN) Increment 2 Build Decision," memorandum, September 2, 2010.

Schaefer, Carl E., *Getting the Warfighter What They Need and When They Need It*, Maxwell AFB, Ala.: Air War College, Air University, February 17, 2010.

Schank, John F., Christopher G. Pernin, Mark V. Arena, and Susan K. Woodward, *Controlling the Cost of C4I Upgrades on Naval Ships*, Santa Monica, Calif.: RAND Corporation, MG-907-NAVY, 2009. As of October 18, 2012:
http://www.rand.org/pubs/monographs/MG907.html

Schoberg, Paul, *Expedited Certification Review*, Navy Certification Authority, 2007.

SECNAVIST—*See* Secretary of the Navy Instruction.

SECNAVNOTE—*See* Secretary of the Navy Notice.

Secretary of the Navy Instruction 5000.2C, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System*, Washington, D.C., November 19, 2004.

Secretary of the Navy Instruction 5000.2D, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System*, October 16, 2008.

Secretary of the Navy M-5000.2, *Department of the Navy Acquisition and Capabilities Guidebook*, December 2008.

Secretary of the Navy Notice 5000, *Rapid Research, Development, Test and Evaluation Response to Urgent Global War on Terrorism Needs*, Washington, D.C., October 19, 2005.

———, Department of the Navy Urgent Needs Process, Washington, D.C., March 12, 2009.

Simpson, Terry, and Marv Langston, "Maritime ISR Enterprise Acquisition Review: Detailed Findings and Recommendations," briefing, October 15, 2010.

Sullivan, Michael, U.S. Government Accountability Office, *Defense Acquisitions: Rapid Acquisition of MRAP Vehicles*, testimony before the House Armed Services Committee, Defense Acquisition Reform Panel, GAO-10-155T, October 8, 2009.

Space and Naval Warfare Systems Command, *Rapid Deployment Capabilities (RDCs): Addressing Faster Delivery*, April 5, 2011.

SPAWAR—*See* Space and Naval Warfare Systems Command.

"Timeline," *Conficker Working Group*, April 26, 2009. As of May 5, 2011:
http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline

U.S. Department of Defense, *Manual for the Operation of the Joint Capabilities Integration and Development System*, January 19, 2012. As of October 19, 2012:
https://acc.dau.mil/adl/en-US/267116/file/41245/JCIDS%20Manual%20-%2019%20Jan%202012.pdf

U.S. Department of Defense Directive 5000.01, *The Defense Acquisition System*, May 12, 2003, certified current as of November 20, 2007.

U.S. Department of Defense Inspector General, "Rapid Acquisition and Fielding of Materiel Solutions by the Navy," December 15, 2009.

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

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

U.S. Department of the Navy, *DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook*, version 1.0, July 15, 2008.

U.S. Government Accountability Office, *Best Practices: Better Support of Weapon System Program Managers Needed to Improve Outcomes*, Washington, D.C., GAO-06-110, November 2005.

———, *Warfighter Support: Improvements to DoD's Urgent Needs Process Would Enhance Oversight and Expedite Efforts to Meet Critical Warfighter Needs*, Washington, D.C., GAO-10-460, April 2010.

U.S. Joint Chiefs of Staff, "The Modified JCIDS Process for IT or IT Box," briefing, undated.

U.S. Special Operations Command Directive 71-4, *Special Operations Forces Capabilities Integration and Development System*, Washington, D.C., June 9, 2009.

Walden, Randy, U.S. Air Force Rapid Capabilities Office, "Rapid Prototyping: Leapfrogging into Military Utility," briefing presented at the ninth annual National Defense Industrial Association Science and Engineering Technology Conference, April 16, 2008.

Weigelt, Matthew, "4 Lessons in Rapid Acquisition Learned from DOD's New ATVs," *Defense Systems*, October 20, 2009. As of October 18, 2012:
http://defensesystems.com/articles/2009/10/19/acq-rapid-acquisition.aspx

Wilson, Beth, Darlene Mosser-Kerner, and Tom Wissink, "Erasing the Line with Title 10: Best Practices in Integrated Testing," briefing presented at the National Defense Industrial Association Test and Evaluation Conference, March 3, 2010.

Wilson, Clay, Botnets, *Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Washington, D.C.: Congressional Research Service, RL32114, January 29, 2008.