RAND 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
Approved for public release; distribution unlimited

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

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.