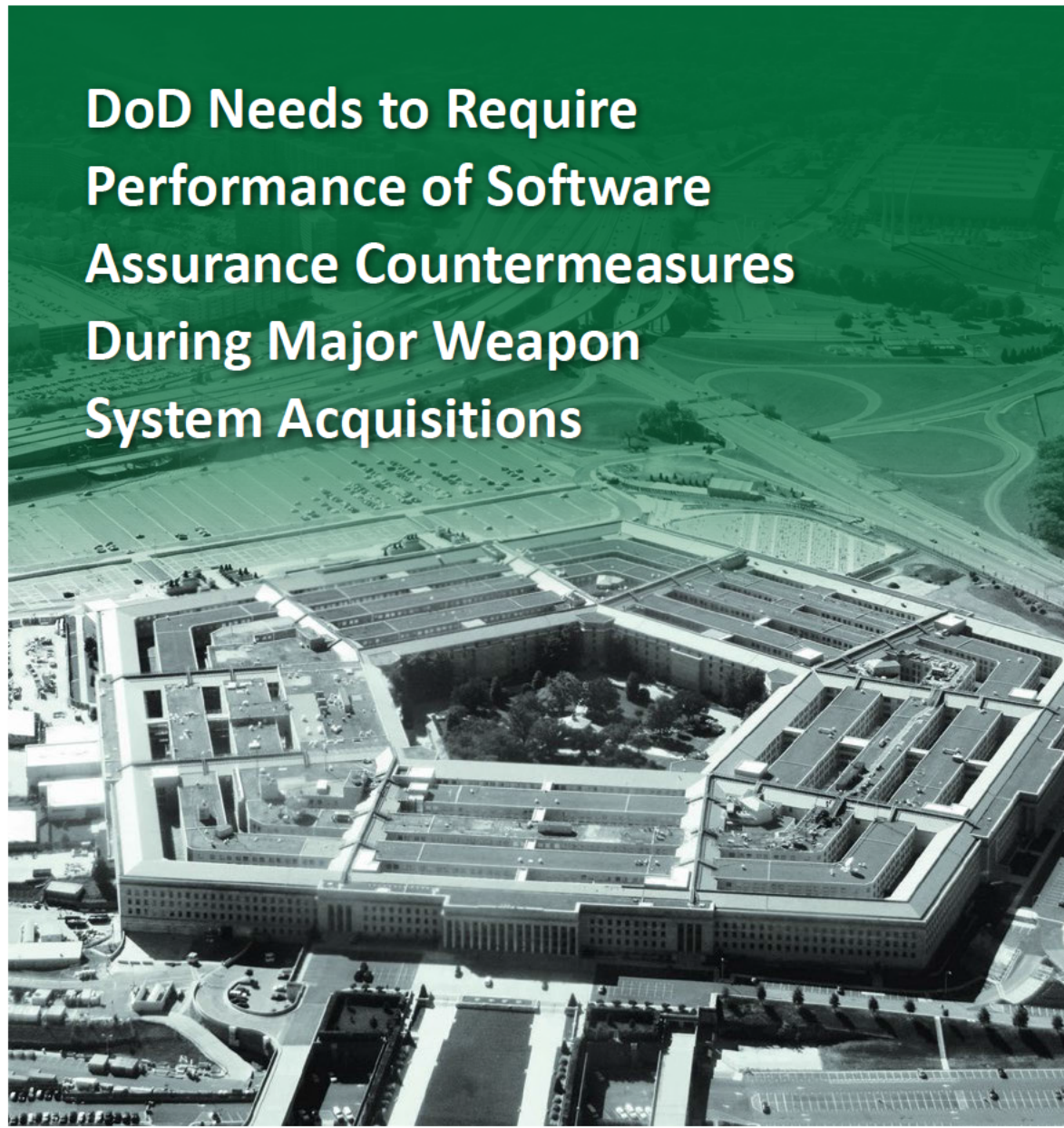# INSPECTOR GENERAL

U.S. Department of Defense

APRIL 29, 2016

DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapon System Acquisitions

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline|800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapon System Acquisitions

April 29, 2016

Objective

We determined whether critical software components for a selected major acquisition program received the required testing to reduce the risk of vulnerabilities in operational software. Specifically, we evaluated software used in the Navy's Littoral Combat Ship – Mission Modules program.

Finding

Program officials for the Navy Littoral Combat Ship – Mission Modules did not ensure all software assurance countermeasures[1] in the Program Protection Plan were fully performed while developing critical software. This occurred because DoD policy did not require that all software assurance countermeasures detailed in the Program Protection Plan be performed. In addition, DoD did not issue implementing procedures to ensure software assurance countermeasures were applied consistently across all major acquisition programs. As a result, there is an increased risk that critical software contains vulnerabilities that, if exploited, could result in mission failure.

Recommendation

We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics:

- develop and issue policy to require program offices to implement applicable software assurance countermeasures in approved Program Protection Plans throughout the lifecycle of DoD programs; and

- develop and issue procedures to guide the consistent application of software assurance countermeasures in approved Program Protection Plans.

Management Comments and Our Response

Comments from the Acting Deputy Assistant Secretary of Defense for Systems Engineering, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics, did not address the specifics of the recommendation. The Acting Deputy stated DoD guidance already requires implementation of software assurance throughout the system lifecycle and that program managers are expected to execute approved Program Protection Plans. The Acting Deputy also stated the Joint Federated Assurance Center was created to oversee the Department's hardware and software assurance resources.

Although we discuss the DoD guidance and the Joint Federated Assurance Center in this report, neither ensures that software assurance countermeasures will be consistently implemented. DoD guidance only requires program managers to plan for software assurance countermeasures and identifies Program Protection Plans as guidelines. Further, the Joint Federated Assurance Center is only a resource for program offices and program offices are not required to use its support.

Therefore, we request that management provide additional comments by May 27, 2016. See the Recommendation Table on the back of this page.

---

[1] Software assurance countermeasures are activities to counter adversarial threats that may target software.

Visit us at www.dodig.mil

Recommendation Table

Management	Recommendation Requires Comment	No Additional Comments Required
Under Secretary of Defense for Acquisition, Technology, and Logistics	Yes	

Please provide Management Comments by May 27, 2016.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 29, 2016

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS

SUBJECT: DoD Needs to Require Performance of Software Assurance Countermeasures
During Major Weapon System Acquisitions (Report No. DODIG-2016-082)

We are providing this report for review and comment. DoD did not require the performance
of software assurance countermeasures to identify and minimize software weaknesses
and vulnerabilities during major weapon systems acquisitions. As a result, there is an
increased risk that the critical software for the Littoral Combat Ship – Mission Modules
program contains vulnerabilities. If exploited, the vulnerabilities could prevent the Littoral
Combat Ship from performing its mission. We conducted this audit in accordance with
generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the
final report. DoD Instruction 7650.03 requires that recommendations be resolved
promptly. Comments from the Acting Deputy Assistant Secretary of Defense for Systems
Engineering, responding for the Under Secretary of Defense for Acquisition, Technology,
and Logistics, did not address the specifics of the recommendation. We request the Under
Secretary of Defense for Acquisition, Technology, and Logistics, provide additional comments
by May 27, 2016.

Please provide comments that conform to the requirements of DoD Instruction 7650.03.
Please send a PDF file containing your comments to audrco@dodig.mil. Copies of your
comments must have the actual signature of the authorizing official for your organization. We
cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send
classified comments electronically, you must send them over the SECRET Internet Protocol
Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at
(703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Objective

Our audit objective was to determine whether critical software components for a selected major acquisition program received the required software assurance[2] (SwA) testing to reduce the risk of vulnerabilities in operational software. Specifically, we evaluated software used in the Navy's Littoral Combat Ship – Mission Modules (LCS MM) program. See the Appendix for a discussion of our scope and methodology and prior audit coverage. See the Glossary for specialized terms used throughout the report.

Background

Nearly all modern technology systems depend on software to perform their functions. From remotely piloted aircrafts and smart bombs to self-driving vehicles and advanced fighter jets, software is crucial to the success of today's weapons systems. DoD's increasing reliance on software presents opportunities for adversaries to gain unauthorized access to data, alter data, disrupt operations, or interrupt communications by inserting malicious code or otherwise corrupting components within DoD systems.

The threat is further increased by the software industry's globalization. Because an increasing percentage of software code is written outside the United States, it is in easy reach of potential adversaries. Rather than attempt to defeat cybersecurity protections, adversaries could exploit software vulnerabilities in critical DoD systems to gain access. According to the DoD Software Assurance Community of Practice (CoP),[3] more than 80 percent of cybersecurity exploits take advantage of weak or vulnerable software in systems, networks, and major database programs. The consequences to U.S. defense capabilities can be even more severe because so many defense systems are interconnected. Therefore, defense programs must conduct early SwA planning and testing to counter adversarial threats that target software.

---

[2] Software assurance is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the software's lifecycle.

[3] DoD established a community of SwA practitioners to promote best practices and standards to achieve software security, assurance, and quality.

DoD Initiative to Protect Software

In 2012, DoD recognized the need to centralize SwA efforts and create a unified approach to address software threats and influence policy. In response, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) and the DoD Chief Information Officer established the DoD SwA CoP, which includes members from DoD and industry. The DoD SwA CoP hosts quarterly meetings where members collaborate to promote best practices and standards to achieve software security, assurance, and quality.

In early 2013, the DoD SwA CoP established three working groups to improve the DoD SwA posture. Additionally, in response to a demand for technical guidance, the CoP is developing a set of whitepapers to provide program managers and technical leads with current SwA best practices.

Program Protection Plans

In January 2011, Congress directed the Secretary of Defense to develop and implement a strategy for assuring the security of software and software-based applications.[4] In response, the Principal Deputy USD(AT&L) issued a policy memorandum in July 2011,[5] which requires all acquisition programs to develop and submit a Program Protection Plan (PPP).[6] The PPP should describe the program's critical program information and mission-critical functions and components,[7] the related threats and vulnerabilities, and a plan for applying countermeasures[8] to minimize associated risks. PPP countermeasures include, but are not limited to:

- exportability features;
- security features;
- supply chain risk management;
- SwA;
- system security engineering;
- anti-counterfeit safeguards; and
- procurement strategies.

---

[4] Public Law 111-383, "Ike Skelton National Defense Authorization Act for Fiscal Year 2011," Section 932, "Strategy on Computer Software Assurance," January 7, 2011.

[5] Principal Deputy Under Secretary of Defense for AT&L memorandum, "Document Streamlining–Program Protection Plan (PPP)," July 18, 2011.

[6] The USD(AT&L) memorandum requirement to develop a PPP was incorporated in the interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 2013, which became policy in January 2015.

[7] Mission-critical functions are those that, if corrupted or disabled, would unacceptably reduce system effectiveness. Mission-critical components are the system elements (hardware, software, and firmware) that implement critical functions.

[8] Countermeasures are activities and actions used to mitigate (minimize) or neutralize the threats and vulnerabilities related to system functions and components.

The USD(AT&L) memorandum requires every acquisition program to submit a PPP for the milestone decision authority (MDA)[9] to review and approve at Milestone A.[10] It further requires that the PPP be updated for approval at each subsequent milestone and at the full-rate production decision. The reviews validate whether program protection planning has been sufficiently addressed. According to USD(AT&L), the PPP review and approval process is DoD's strategy for implementing SwA.

The USD(AT&L) memorandum includes a PPP outline with content and formatting guidance that can be tailored to individual acquisition programs. According to the memorandum, once approved, program officials should use the PPP to guide program protection efforts and software security measures throughout the acquisition lifecycle. The PPP outline includes a SwA Countermeasures Table, which is divided into three sections:

- Development Process;
- Operational System; and
- Development Environment.

Each section provides different vulnerability and countermeasure perspectives on SwA plans and implementation. For example, the development process includes SwA countermeasures that should be conducted during the software development process to mitigate attacks that the developed system is likely to experience when deployed.

We focused on the eight SwA countermeasures associated with the software development process, which collectively addressed the three key concepts of SwA—*confidence* that the software *functions as intended* and is *free of vulnerabilities.* Table 1 depicts the relationship between the key concepts and the eight countermeasures. See the Glossary for definitions of each SwA countermeasure.

---

[9] An MDA has overall responsibility for a program. The MDA has the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting, including congressional reporting.

[10] The Defense Acquisition System uses "milestones" to oversee and manage acquisition programs. At each milestone, a program must meet specific statutory and regulatory requirements before the program can proceed to the next phase of the acquisition process. The three acquisition milestones include: (1) Milestone A which initiates technology maturation and risk reduction; (2) Milestone B which initiates engineering and manufacturing development; and (3) Milestone C which initiates production and deployment.

Table 1. *Relationships Between SwA Concepts and Countermeasures*

Key Concept	SwA Countermeasure
Confidence	Static analysis
	Design inspection
	Code inspection
Functions as intended	Penetration testing
	Test coverage
	Common attack pattern enumeration and classification
Free of vulnerabilities	Common vulnerabilities and exposures
	Common weakness enumeration

Littoral Combat Ship Program

In February 2002, the Navy initiated the Littoral Combat Ship (LCS) Program to develop a new class of ships for operations close to shore. The LCS primary missions are to counter shallow-water mine, surface, and submarine threats.
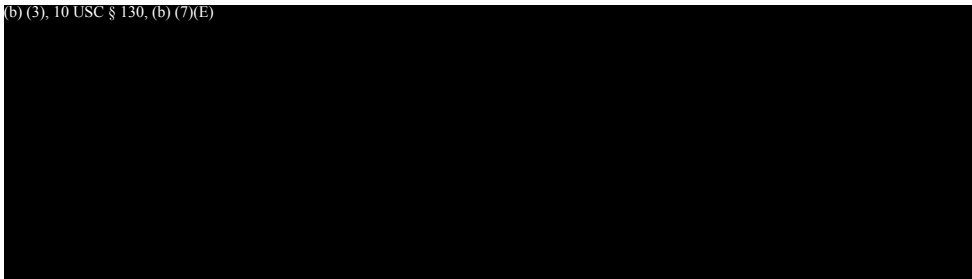

Figure. USS Independence (LCS 2), left, and USS Coronado (LCS 4)
Source: Department of the Navy

Each LCS primary mission area is represented by a Mission Package (MP), which includes the sensors, weapons, vehicles, support equipment, crew, and support aircraft required for that mission area. MPs are installed and uninstalled on the LCS seaframe[11] to alter the ship's mission orientation, as the LCS was designed to perform only one of the primary missions at any given time. The three LCS MPs are known as:

- Mine Countermeasures—detect and neutralize mine threats;
- Surface Warfare—sea security and prosecution of small boat threats; and
- Anti-Submarine Warfare—detect, classify, localize and prosecute enemy submarines.

In April 2011, the LCS Program was separated into two different Acquisition Category I programs: the LCS Seaframe Program and the LCS MM Program. Program Manager, Ship 420 was designated as the program office for the LCS MM Program to develop the common computing infrastructure and communication services needed for MPs to operate on the LCS and communicate with multiple unmanned vehicles.

(FOUO) In April 2013, LCS MM officials developed a PPP for the LCS MM program that was approved by the MDA in June 2013. Based on an assessment and criticality analysis, the PPP identified ▮(b) (7)(E)▮ LCS MM critical software components:

(b) (3), 10 USC § 130, (b) (7)(E)

(FOUO) (b) (3), 10 USC § 130, (b) (7)(E)

We focused on evaluating SwA for the ▮(b) (3), 10 USC § 130▮ software because of its significance to LCS operations.

---

[11] An LCS with no MPs installed is referred to as an LCS seaframe.

Review of Internal Controls

DoD Instruction (DoDI) 5010.40[12] requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses relating to SwA testing for Acquisition Category I programs. Specifically, DoD policy issued by USD(AT&L) did not require that the SwA countermeasures detailed in the PPP be implemented and DoD did not issue implementation procedures to ensure SwA countermeasures were applied consistently. We will provide a copy of the report to the senior official responsible for internal controls in USD(AT&L).

---

[12] DoDI 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Software Assurance Countermeasures Were Not Fully Performed

(FOUO) LCS MM program office officials did not ensure all SwA countermeasures detailed in the PPP were fully performed while developing the [(b) (3), 10 USC § 130] critical software.

This occurred because DoD policy required that a PPP be prepared, but the policy did not require that all SwA countermeasures in the PPP be performed. In addition, DoD did not issue implementing procedures to ensure software assurance countermeasures were applied consistently across all major acquisition programs.

(FOUO) As a result, there is an increased risk that the [(b) (3), 10 USC § 130] software contains vulnerabilities that, if exploited, could prevent the LCS from performing its mission.

LCS MM Officials Did Not Ensure All SwA Countermeasures Were Fully Performed

(FOUO) LCS MM officials did not ensure all SwA countermeasures contained in the PPP were performed while developing the [(b) (3), 10 USC § 130] critical software. In April 2013, the LCS MM program office developed the Milestone B PPP,[13] which was approved by the MDA in June 2013. The PPP documented [(b) (3), 10 USC § 130, (b) (7)(E)] ▮▮▮▮▮▮▮▮▮▮▮▮▮▮

> LCS MM officials did not ensure all SwA countermeasures contained in the PPP were performed while developing the [(b) (3), 10 USC § 130] critical software.

(FOUO) We identified deficiencies related to the performance of [(b) (7)(E)] of the [(b) (7)(E)] SwA countermeasures documented in the PPP. Table 2 describes the SwA countermeasures that were performed, partially performed, or not performed for the [(b) (3), 10 USC § 130] critical software components.

---

13 [(b) (7)(E)] ▮▮▮▮▮▮▮▮▮▮

(FOUO) Table 2. (b) (3), 10 USC § 130 *SwA Countermeasures*

(FOUO) Countermeasure	Deficient	Deficiency or Performance Explanation
(b) (3), 10 USC § 130, (b) (7)(E)		
		(FOUO)

 * SwA countermeasures identified as deficient were either not performed or partially performed.

DoD Policy Does Not Require Performance of SwA Countermeasures and Lacks Implementation Procedures

Although DoD policy[14] requires acquisition program offices to address SwA through program protection planning, it does not require that the SwA countermeasures contained in PPPs be performed, or provide implementation procedures for consistent application of those countermeasures. USD(AT&L) instituted program protection planning as DoD's strategy for delivering trusted systems and achieving SwA.[15] In January 2013, Congress tasked USD(AT&L), in coordination with the DoD Chief Information Officer, with developing and implementing a baseline SwA policy.[16] The legislation stated that the baseline SwA policy must require the use of automated vulnerability analysis tools and risk-based remediation strategies during the entire lifecycle of covered systems[17] and translate the remediation strategies into contract requirements.

In April 2014, DoD briefed Congress on its implementation status, identifying DoDI 5000.02 as the baseline SwA policy requiring automated SwA tool use and practice across the DoD acquisition lifecycle. However, the Instruction does not contain any SwA implementation requirements, but rather reiterates the requirement that program managers plan for SwA in their PPP. Furthermore, the Instruction recognizes program protection as an ongoing risk management process and identifies PPPs as guidelines for the program, rather than requirements. According to the Deputy Director, Lifecycle Risk Management and Cybersecurity/ Acquisition Integration, Office of the Deputy DoD Chief Information Officer for Cybersecurity, DoD did not issue policy to require that the SwA countermeasures contained in the PPP outline be implemented. In addition, the Deputy Director stated there were no plans to write a singular policy for SwA. The Deputy Director stated the Department relies on engagement with program offices during the PPP review and approval process to provide guidance on SwA implementation.

---

[14] Principal Deputy USD(AT&L) Memorandum, "Document Streamlining – Program Protection Plans," July 18, 2011; and Interim DoDI 5000.02, "Operation of the Defense Acquisition System," November 25, 2013, issued as final on January 7, 2015.

[15] According to the DoD report to Congress, "Report on Department of Defense Strategy for Assuring the Security of Software and Software-based Applications for all Covered Systems," September 28, 2011.

[16] Public Law 112-239, National Defense Authorization Act for FY 2013, Section 933, "Improvements in Assurance of Computer Software Procured by the Department of Defense," January 2, 2013.

[17] As defined by the National Defense Authorization Act for FY 2013, a covered system is any DoD critical information, business, or weapons system that is: (1) a major system, as defined in section 2302(5), title 10, United States Code; (2) a national security system as defined in section 3542(b)(2), title 44, United States Code; or (3) a DoD-funded information system categorized as Mission Assurance Category I in DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002.

The FY 2013 National Defense Authorization Act further requested that DoD identify and brief Congress on the "state-of-the-art of SwA analysis and test" capabilities. In response, DoD sponsored and funded the Institute for Defense Analyses report[18] to facilitate effective SwA decision-making in DoD and influence DoD policy. The report concluded that DoD program managers and their staff need information and guidance on software evaluation tools and techniques, and when they need to apply those tools and techniques.

During the audit, officials from the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation, Naval Sea Systems Command, and LCS MM program office expressed concern over the lack of policy and implementation procedures. LCS MM officials stated that they did what they could within their budget and schedule to ensure that SwA countermeasures were performed given the lack of requirements and instructions. However, DoD did not issue procedures or implementation instructions to facilitate consistent application of SwA countermeasures in the PPP outline. USD(AT&L) should develop and issue policy to require program offices to implement the SwA countermeasures contained in the PPP, and standardize procedures for consistent application of SwA across DoD.

> DoD did not issue procedures or implementation instructions to facilitate consistent application of SwA countermeasures in the PPP outline.

Increased Risk of Mission Failure

(FOUO) Because SwA countermeasures were only partially performed, there is an increased risk that the [(b) (3), 10 USC § 130] software contains weaknesses or vulnerabilities that could result in mission failure. [(b) (3), 10 USC § 130, (b) (7)(E)]

_____

[18] Institute for Defense Analyses, "State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation," July 2014.

[19] (b) (3), 10 USC § 130, (b) (7)(E)

The SwA countermeasures listed in the PPP are assurance activities designed to reduce risk by verifying that the software functions as intended and is free of vulnerabilities. Therefore, if SwA countermeasures are not fully performed, there is an increased risk that the LCS MM critical software contains vulnerabilities or will not function as intended. LCS MM officials took action to address risk to critical software components by incorporating SwA testing requirements in the draft request for proposal for the next LCS MM contract. That action will address the deficiencies identified in our audit specific to the LCS MM and therefore, we are not making any recommendations to the LCS MM program office.

> If SwA countermeasures are not fully performed, there is an increased risk that the LCS MM critical software contains vulnerabilities.

Management Actions

In response to a Congressional mandate in the FY 2014 National Defense Authorization Act,[20] the Deputy Secretary of Defense chartered the Joint Federated Assurance Center (JFAC) to promote trust and assurance in the defense system hardware and software across program lifecycles. The JFAC is a federation of existing DoD organizations that have a shared interest in promoting software and hardware assurance in defense programs, systems, and supporting activities. The JFAC is scheduled to achieve initial operational capability in March 2016 and will be a resource for program offices to obtain SwA policies, guidance, standards, best practices, training, and testing support.

In September 2015, the JFAC awarded $1.13 million in contracts to purchase SwA tools for allocation across DoD to support the performance of SwA countermeasures. However, acquisition program offices were not required to use the JFAC as a resource. Although the JFAC should provide SwA assistance to acquisition programs, it will not ensure performance of SwA countermeasures. Therefore, DoD policy and procedures are necessary to ensure SwA countermeasure performance.

---

[20]   Public Law 113-66, National Defense Authorization Act for FY 2014, Section 937, "Joint Federated Centers for Trusted Defense Systems for the Department of Defense," December 26, 2013.

Management Comments on the Report

Although not required to comment, the Deputy Program Manager for the LCS MM program provided comments to the draft report. The Deputy Program Manager stated that program office representatives previously discussed the draft report with the audit team and had no comments on the draft report. For the full text of the Deputy Program Manager's response, see the Management Comments section of the report.

Recommendation, Management Comments, and Our Response

Recommendation 1

We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics:

   a. **Develop and issue policy to require program offices to implement the applicable software assurance countermeasures in approved Program Protection Plans throughout the lifecycle of DoD programs.**

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

The Acting Deputy Assistant Secretary of Defense for Systems Engineering, responding for USD(AT&L), disagreed, stating that the recommended action has already been completed through reissuance of DoD Instruction 5000.02. The Acting Deputy stated that the Instruction requires the implementation of SwA throughout the system lifecycle. Specifically, the Instruction states:

> Program managers will incorporate automated software vulnerability analysis tools throughout the life cycle and ensure remediation of software vulnerabilities is addressed in PPPs, test plans, and contract requirements (as required by section 933 of [Public Law] 112-239, Reference (l).

The Acting Deputy also stated that DoD Instruction 5000.02 assists in planning and focusing a program's software assurance efforts by describing the information program managers must include in their PPPs, such as a program's critical program information and mission-critical functions and components. Furthermore, the Acting Deputy stated the Instruction states that program managers are expected to execute approved program plans, such as the PPP.

Our Response

Comments from the Acting Deputy did not address the specifics of the recommendation. As stated in this report, DoD Instruction 5000.02 was identified as the baseline SwA policy, requiring acquisition program offices to address SwA through program protection planning. However, the Instruction does not contain SwA implementation requirements but rather reiterates the requirement that program managers plan for SwA in their PPP. Furthermore, as stated in this report, the Instruction recognizes program protection as an ongoing risk management process and identifies PPPs as guidelines for the program, rather than requirements. In addition, during the audit, officials from the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation and the Naval Sea Systems Command expressed concern that DoD policy did not define SwA requirements or mandate the performance of SwA countermeasures in the PPP. Therefore, we request that USD(AT&L) provide additional comments on the final report to describe planned actions and completion dates for developing and issuing policy to ensure implementation of applicable SwA countermeasures in PPPs.

> **b. Develop and issue procedures to guide the consistent application of software assurance countermeasures in approved Program Protection Plans.**

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

The Acting Deputy Assistant Secretary of Defense for Systems Engineering, responding for USD(AT&L), agreed, stating that the Deputy Secretary of Defense chartered the JFAC to oversee the Department's hardware and software assurance resources that provide support to acquisition programs. The Acting Deputy stated that the JFAC is moving forward with a set of initiatives to improve expertise and raise awareness and proficiency of hardware and software assurance acquisition professionals.

Our Response

Comments from the Acting Deputy did not address the specifics of the recommendation. Although the Acting Deputy agreed with the recommendation, she only referenced the work of the JFAC and did not provide corrective actions, planned or taken, or a planned completion date for developing procedures. As stated in this report, the JFAC is a resource for program offices to obtain SwA

policies, guidance, standards, best practices, training, and testing support. However, we also noted that program offices were not required to use the JFAC and the JFAC will not ensure performance of SwA countermeasures. Additionally, according to the JFAC charter, it is the responsibility of USD(AT&L) to integrate JFAC hardware and software assurance findings into DoD acquisition policy, guidance, and processes. Therefore, we request that USD(AT&L) provide additional comments on the final report to describe planned actions and completion dates for when USD(AT&L) will develop and issue procedures to guide the consistent application of SwA countermeasures.

Appendix

Scope and Methodology

We conducted this performance audit from February 2015 through March 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(FOUO) We interviewed officials from the Deputy Assistant Secretary of Defense for Systems Engineering and the DoD Chief Information Officer. Additionally, we interviewed officials from the LCS MM program office and the contractor responsible for developing the ▌(b) (3), 10 USC § 130▐ software.

(FOUO) We obtained and analyzed LCS MM program documents to include:

- LCS MM Contract Award, January 14, 2012;

- Statement of Work for the LCS MM Program, Revision F, July 18, 2013;

- LCS MM—Acquisition Category IC Program Protection Plan, Version 1.0 Supporting Milestone B, April 25, 2013;

- Software Development Plan for the Littoral Combat Ship – Mission Module Program, August 8, 2012; and

- (b) (3), 10 USC § 130 ███████████████████████████████████████

We compared LCS MM documents to SwA Federal and DoD policies, standards, and best practices, including:

- Public Law 112-239, "National Defense Authorization Act for Fiscal Year 2013," January 2, 2013, Section 933, "Improvements in Assurance of Computer Software Procured by the Department of Defense;"

- Principal Deputy Under Secretary of Defense for AT&L memorandum, "Document Streamlining—Program Protection Plan (PPP)," July 18, 2011;

- DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012;

- DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014;

- Deputy Assistant Secretary of Defense for Systems Engineering and DoD Chief Information Officer, "Software Assurance Countermeasures in Program Protection Planning," March 2014; and

- Defense Information Systems Agency Security Technical Implementation Guide, "Application Security and Development, Version 3, Release 9," October 24, 2014.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Use of Technical Assistance

(FOUO) We were assisted by a software engineer from Naval Surface Warfare Center Corona who helped analyze and interpret the results of criticality analyses, the selection of tools and techniques (countermeasures) for SwA and software code analysis, and the remediation reports for software products associated with LCS MM. Additionally, the software engineer evaluated the LCS program's (b) (3), 10 USC § 130 ███ computer software configuration items against the cybersecurity requirements of DoDI 8500.01.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO), the DoD Inspector General, and the Naval Audit Service issued nine reports discussing software assurance risks and vulnerabilities. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD Inspector General reports can be accessed at http://www.dodig.mil/pubs/index.cfm. Naval Audit Service reports are not available over the Internet.

GAO

GAO-14-322, "F-35 Joint Strike Fighter: Problems Completing Software Testing May Hinder Delivery of Expected Warfighting Capabilities," March 2014

GAO-13-652T, "Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment," May 21, 2013

GAO-12-579T, "IT Supply Chain: Additional Efforts Needed by National Security-Related Agencies to Address Risks," March 27, 2012

GAO-12-361, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," March 2012

GAO-11-75, "Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities," July 2011

DoD Inspector General

DODIG-2014-081, "Army Integrated Air and Missile Defense Program Needs to Improve Software, Test, and Requirements Planning," June 9, 2014 (Document is FOUO)

DODIG-2013-115, "The Navy's Management of Software Licenses Needs Improvement," August 7, 2013

DODIG-2012-142, "Summary Report of FY 2011 Inspections on Security, Intelligence, Counterintelligence, and Technology Protection Practices at DoD Research, Development, Test, and Evaluation Facilities," September 28, 2012

Navy

N2011-0047, "Certification and Accreditation of Information Systems within the Marine Corps," August 2, 2011

Management Comments

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

APR 06 2016

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS AND CYBER
OPERATIONS, DEPARTMENT OF DEFENSE OFFICE OF
INSPECTOR GENERAL

SUBJECT: Department of Defense Inspector General Draft Audit Report, "DoD Needs to
Require Performance of Software Assurance Countermeasures During Major
Weapon System Acquisitions" (Project No. D2015-D000RB-0125.000)

We received the subject draft report, dated March 8, 2016, and reviewed your
recommendations to the Under Secretary of Defense for Acquisition, Technology, and Logistics.
Responses to your recommendations are attached.

Thank you for the opportunity to review and comment on the draft report. My staff point
of contact is ███████████. Reach him at ██████████ or ███████████.

Kristen J. Baldwin
Acting, Deputy Assistant Secretary of Defense
Systems Engineering

Attachment:
As stated

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments (cont'd)

DOD IG DRAFT REPORT – DATED MARCH 8, 2016
DOD IG PROJECT NO. D2015-D000RB-0125.000

"DOD NEEDS TO REQUIRE PERFORMANCE OF SOFTWARE ASSURANCE
COUNTERMEASURES DURING MAJOR WEAPON SYSTEM ACQUISITIONS"

OFFICE OF THE UNDER SECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY,
AND LOGISTICS) (OUSD (AT&L)) RESPONSE TO RECOMMENDATIONS

RECOMMENDATION 1.a.: Develop and issue policy to require program offices to implement the applicable software assurance countermeasures in approved Program Protection Plans throughout the lifecycle of DoD programs.

OUSD(AT&L) RESPONSE: Disagree.

Discussion: This action has been completed, via reissuance of the DoDI 5000.02, "Operation of the Defense Acquisition System" in fiscal year 2015. The updated DoD 5000.02, page 86 of Enclosure 3, now requires the implementation of software assurance (SwA) throughout the system lifecycle:

> "Program managers will incorporate automated software vulnerability analysis tools throughout the life cycle and ensure remediation of software vulnerabilities is addressed in PPPs, test plans, and contract requirements (as required by section 933 of P.L. 112-239, Reference (l)."

To assist in planning for and focusing a program's software assurance efforts, DoD 5000.02 Enclosure 3 page 86 also notes:

> "Program managers will describe in their PPP the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement. Countermeasures should include anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations in accordance with DoD Instruction 5200.39 (Reference (ai)), DoD Instruction 5200.44 (Reference (aj)), and DoD Instruction 8500.01 (Reference (x))… Countermeasures should mitigate or remediate vulnerabilities throughout the product life cycle, including design, development, developmental and operational testing, operations, sustainment, and disposal."

DoD policy also requires managers of acquisition programs to execute their programs in accordance with approved plans, such as the PPP. DoD 5000.02, section 5.a.(4)(c) states:

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments (cont'd)

"Program Managers, under the supervision of Program Executive Officers (PEOs) and CAEs, are expected to design acquisition programs, prepare programs for decisions, and execute approved program plans."

RECOMMENDATION 1.b.: Develop and issue procedures to guide the consistent application of software assurance countermeasures in approved Program Protection Plans.

OUSD (AT&L) RESPONSE: Agree.

Discussion: We agree there is a need to continue to assist programs by developing and promulgating best-practices for software assurance. The Deputy Secretary of Defense chartered the Joint Federated Assurance Center (JFAC) in February 2015 to oversee the Department's hardware and software assurance resources that provide support to acquisition programs. The JFAC is advancing a series of initiatives to improve the laboratory capabilities and expertise, and raise the awareness and proficiency of acquisition professionals in hardware and software assurance. The initiatives include:

- JFAC technical tasks that contribute to consistent application of software assurance countermeasures in approved Program Protection Plans:
  - Air Force-led "Software Assurance Integrated Product Team" will encourage developers to apply SwA procedures across the software development lifecycle (completed 01/2016)
  - Army-led "Embedded SW Assurance Lifecycle" provides integrated software assurance environment and procedures, and encourages continuous, consistent and automated source code analysis and security assessment across the software development lifecycle (completed 01/2016)
  - Results of both projects have been disseminated and will be made available via the JFAC web portal
- Negotiation, procurement and distribution of an initial set of JFAC-provided software assurance tool licenses for use by Military Department software assurance providers and program managers (completed 03/2016)
- Declaration of JFAC Initial Operational Capability (IOC) (04/2016)
- Upgrade and rehost of JFAC community support website (07/2016); development and activation of classified sites (09/2016)
- Update of the State-Of-the-Art-Resource products to refresh software assurance tool applicability guidance (12/2016)

LCS MM Program Office Comments

DEPARTMENT OF THE NAVY
PROGRAM EXECUTIVE OFFICER
LITTORAL COMBAT SHIPS
1333 ISAAC HULL AVE, SE
WASHINGTON NAVY YARD, DC 20376

IN REPLY REFER TO
5000
Ser 420/018
4 Apr 16

Office of Inspector General
United States Department of Defense
Readiness and Cyber Operations
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear Sirs:

In response to your electronic mail messages of 8 March █████████ and 18 March ███████████, the Littoral Combat Ships Mission Module program office has reviewed your draft report, "DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapon System Acquisitions," March 8, 2016 (Project No. D2016-D000RB-0125.000).

Representatives of the program office previously discussed the draft report with your audit team. The program office does not have any comment of the draft report.

The LCS Mission Modules point of contact for this matter is the undersigned. I can be reached at ██████████ or ████████ ████████.

Sincerely,

A. K. Schuler

A. K. SCHULER
Deputy Program Manager
Littoral Combat Ships Mission Modules
By direction of the Program Executive Officer

Glossary

Acquisition Category I: A program that is designated by USD(AT&L) as a Major Defense Acquisition Program; or that is estimated to require eventual expenditure for Research, Development, Test and Evaluation of more than $480 million or procurement of more than $2.79 billion (FY14 constant dollars).

Code Inspection/Review: Human analysis of software source code to identify indicators of security weaknesses or vulnerabilities.

Common Attack Pattern Enumeration and Classification: Department of Homeland Security-sponsored catalog of common attack patterns that can be used by program personnel to understand how their systems may be attacked and how to defend them.

Common Weakness Enumeration: Department of Homeland Security-sponsored listing of common software weaknesses that can occur in software's architecture, design, code, or implementation that can lead to exploitable security vulnerabilities. Software weaknesses are flaws, faults, bugs, vulnerabilities, and other errors in software implementation, code, design, or architecture that, if left unaddressed, could result in systems and networks being vulnerable to attack.

Common Vulnerabilities and Exposures: Department of Homeland Security-sponsored compilation listing publicly known information security vulnerabilities and exposures in commercial off-the-shelf and open-source software that are often used by malicious actors to attack systems.

Critical Component: A component that contains information and communications technology, including custom, commercial, or otherwise developed software, and which delivers mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

Design Inspection: Visual examination of design documents targeting architectural and design level weaknesses/vulnerabilities.

Joint Federated Assurance Center: The JFAC is the federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities. The JFAC develops, maintains, and offers software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across DoD.

Littoral Combat Ship: A fast, agile, networked surface ship optimized for operations close to shore, otherwise known as the littorals. The primary LCS missions include countering littoral mine, surface, and submarine threats to assure maritime access for Joint Forces.

Mission Module: The configuration of mission systems and support equipment that installs into the LCS seaframe through standard interfaces.

Mission Package: A mission package consists of mission modules, mission crew detachments, and a support aircraft. When installed on an LCS, a mission package provides the capability required to perform missions in a specific warfare area.

(FOUO) (b) (3), 10 USC § 130

Penetration Testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. Tests can range from "what if" exercises to full-blown attacks on operational systems.

Program Protection Plan: A risk-based, comprehensive, living plan that captures the program's critical program information, mission-critical functions, and component associated threats, vulnerabilities, and countermeasures. A program protection plan is meant to help programs ensure that they adequately protect their technology, components, and information.

Seaframe: An LCS with no mission packages installed.

Software Assurance: The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the lifecycle.

Static Analysis: Performed using automated tools to analyze source code before it is compiled to detect coding errors, insecure coding constructs, and other indicators of security vulnerabilities or weaknesses that are detectable at the source code level.

Test Coverage: Units or metrics that provide standards for test completeness (that is, percentage of statements exercised, number of function points tested, etc.)

Acronyms and Abbreviations

CoP	Community of Practice
JFAC	Joint Federated Assurance Center
LCS	Littoral Combat Ship
LCS MM	Littoral Combat Ship – Mission Modules
MDA	Milestone Decision Authority
MP	Mission Package
(FOUO)	(b) (3), 10 USC § 130 ██████████████
PPP	Program Protection Plan
SwA	Software Assurance
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098