Cybersecurity Challenges

for Program Managers

Steve Mills ■ *Rob Goldsmith*

Cybersecurity threats to Department of Defense (DoD) acquisition programs are both challenging and complex. Program managers (PMs) have the daunting responsibility to minimize cybersecurity vulnerabilities in their systems against current and future cybersecurity threats.

To effectively address cybersecurity threats in DoD acquisition programs, PMs need a combination of the right policies, processes, people and tools. Furthermore, cybersecurity is dynamic by nature, requiring proactive engagement and expertise to minimize risk throughout the acquisition life cycle. Effective cybersecurity can only be achieved through a holistic approach that takes into account more than just information

Mills *is a former program manager from Northrop Grumman Inc. He currently is a professor of program management and information technology at the Defense Acquisition University.* **Goldsmith** *is a systems engineer and currently the Aviation and Missile Research, Development and Engineering Center Cybersecurity Lead at Redstone Arsenal, Ala.*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cybersecurity Challenges for Program Managers	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University,9820 Belvoir Road,Fort Belvoir,VA,22060-5565**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**3**	

assurance compliance. This holistic approach includes areas of known cybersecurity risk for DoD programs and provides an effective framework for developing, planning and implementing an effective cybersecurity strategy. Such a strategy must be based on the following expanded set of areas:

- Information Assurance
- Hardware/Software Assurance
- Supply Chain Risk Management
- Blue Team—Computer Network Defense/Vulnerability Analysis
- Red Team—Threat vulnerability/penetration testing

Failure to address all these areas as part of the cybersecurity effort will likely result in failure from a cybersecurity perspective. This article will briefly address revised DoD cybersecurity policy and highlight a unique Aviation and Missile Research, Development and Engineering Center (AMRDEC) cybersecurity initiative supporting DoD PMs.

New DoD Cybersecurity Policy

The focus and emphasis of cybersecurity within the DoD changed significantly with the release of DoD Instruction (DoDI) 8500.01 (Cybersecurity) and DoDI 8510.01 (Risk Management Framework for DoD Information Technology [IT]). A key purpose of these revised instructions is an attempt to align DoD cybersecurity efforts with the best practices of both private industry and other federal agencies. By doing so, DoD can leverage proven and effective processes to make DoD networks and systems more resilient against current and future cybersecurity threats. Another major focus of the revised DoD policy is to address cybersecurity risk in a manner that takes into account the unique challenges presented by such threats.

The revised DoDI 8500.01, titled Cybersecurity, provides several changes, including a revised focus. The term "Information Assurance" is no longer used and has been replaced with the term "cybersecurity." A quick review of the DoD definition for both terms reveals little change in wording but a clear change in focus. First, the cybersecurity focus has been expanded to include communications systems, communications services, wire communications and electronic communications. Implicit in the definition above is an understanding that electronic and wire communications are increasing at an exponential rate and that providing security for those forms of communication is extremely important.

Additionally, this DoD instruction places increased emphasis on operational resilience, integration and interoperability. This emphasis recognizes the critical part interoperability plays in the development, acquisition and fielding of DoD systems and our ability to operate effectively on the battlefield. Finally, the term "cybersecurity" emphasizes the concept of prevention. Incorporating cybersecurity early in the acquisition life cycle is both proactive and preventive. DoDI 8500.01 advocates incorporating cybersecurity early and continuously throughout the acquisition life cycle. The acquisition life-cycle process embodied in DoDI 5000.02 promotes the importance of "upfront and early" planning and incorporation of logistics to ensure program success. This same proactive approach should be used for early incorporation of cybersecurity in the acquisition life-cycle process and is in line with the "Shift Left Initiative" advocated by Dr. Steven J. Hutchison, Acting Deputy Assistant Secretary of Defense for Developmental Test and Evaluation.

According to Hutchison:

> The Shift Left initiative fundamentally is about improving DT&E to set the conditions for successful production and deployment. Shift Left achieves this goal through earlier identification and correction of failure modes, thereby avoiding the high costs of late cycle repair and reducing the impact to our warfighters of fielding capabilities that do not satisfy requirements. There are three key elements of Shift Left: earlier testing for interoperability, earlier testing of Cybersecurity, and conducting DT&E in a mission context.

Early incorporation of cybersecurity into the DoD acquisition life cycle will likely lower overall program risk and lead to better acquisition outcomes.

The revised DoDI 8510.01, Risk Management Framework (RMF) for DoD IT, is DoD's authorization process for information technology systems and supersedes the previous process known as the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). The focus of RMF is on iteratively managing cybersecurity risk through a six-step process that includes the key component of continuous monitoring. According to *Bloomberg Businessweek*, the recent cybersecurity data breach experienced by Target stores was the biggest in U.S. history and primarily was due to lack of continuous monitoring and response. RMF uses a risk-based approach for decisions on cybersecurity versus the former approach (DIACAP) that focused on checklists and compliance. Just focusing on compliance via checklists will yield some benefit but does not sufficiently address cybersecurity risk. The goal of the RMF process in DoD acquisition programs is to incorporate RMF up front and early and in a continuous manner throughout the acquisition life cycle.

AMRDEC Cyber Integrator Initiative

AMRDEC at Redstone Arsenal, Huntsville , Ala., is proactively supporting DoD Project Management Offices (PMOs) and Program Executive Offices (PEOs) through several cybersecurity initiatives. The recent shift in DoD cybersecurity policy and the language in the 2013 and 2014 National Defense Authorization Acts (NDAAs) are forcing PMs to proactively address cybersecurity risk throughout the acquisition life cycle. Acquisition programs can mitigate cybersecurity risk by addressing it early in the acquisition life cycle and by "widening the aperture" when developing the mandatory Cybersecurity Strategy.

A noteworthy AMRDEC cybersecurity initiative is the concept of a "cyber integrator (CI)" added to the PEO/PMO staff of select DoD acquisition programs. The purpose of the CI is to lead the cybersecurity efforts within the program, which includes effective integration of cybersecurity across all functional domains, and act as principal advisor to the PM on all cybersecurity matters. The designation and empowerment of a CI as the "cybersecurity champion" within the PMO clearly puts program cybersecurity in an elevated and proactive posture. Cybersecurity encompasses additional components such as hardware, software and firmware assurance, supply-chain risk management, Blue Team/Vulnerability analysis activities and Red Team testing. These additional focus areas coupled with the integration required across all functional domains necessitate the requirement for the CI.

The potential impact of the CI really comes into focus through the use of the Cyber Dashboard, which was developed by AMRDEC and is a measurement/management tool that tracks key cybersecurity milestones and program dependencies across critical cybersecurity focus areas. The CI using the Cyber Dashboard concept is an ongoing pilot program in the Integrated Air and Missile Defense Program Office, an ACAT I program in Huntsville, Ala. The CI produces a holistic view of the system's cybersecurity posture for senior leaders in the PMO, enabling them to make decisions based on actionable information.

In addition, the CI attempts to stay informed on all new cybersecurity initiatives and communicates these to the program management. The CI works with the appropriate program office resources to help determine what support is required from outside agencies and coordinates these efforts to ensure that cybersecurity requirements are met, the overall system cybersecurity risk is effectively mitigated and that all cybersecurity-related acquisition life-cycle requirements are adequately addressed.

Cybersecurity threats will continue to be a significant threat to DoD acquisition programs. Effective mitigation of cybersecurity risks relies on several key factors. First, we must continue to look for opportunities to take the fight to the enemy and not be complacent and defensive. We must maintain a proactive posture including a situational awareness for new threats at all times. Next, we must look for innovative methods to address cybersecurity risk. The CI and Cyber Dashboard concept constitute such an approach. By designating a "cybersecurity champion" in the Project Office, we are putting increased emphasis and resources toward securing our systems against cybersecurity threats.

Finally, we must identify and resource a new and expanded legion of cybersecurity warriors to take the fight to the enemy. We need to find and incentivize personnel with the right technical acumen and leadership to get the job done. DAU and AMRDEC look forward to the challenge.

The authors can be contacted at **Steve.Mills@dau.mil** *and* **Rob.Goldsmith@amrdec.army.mil**.