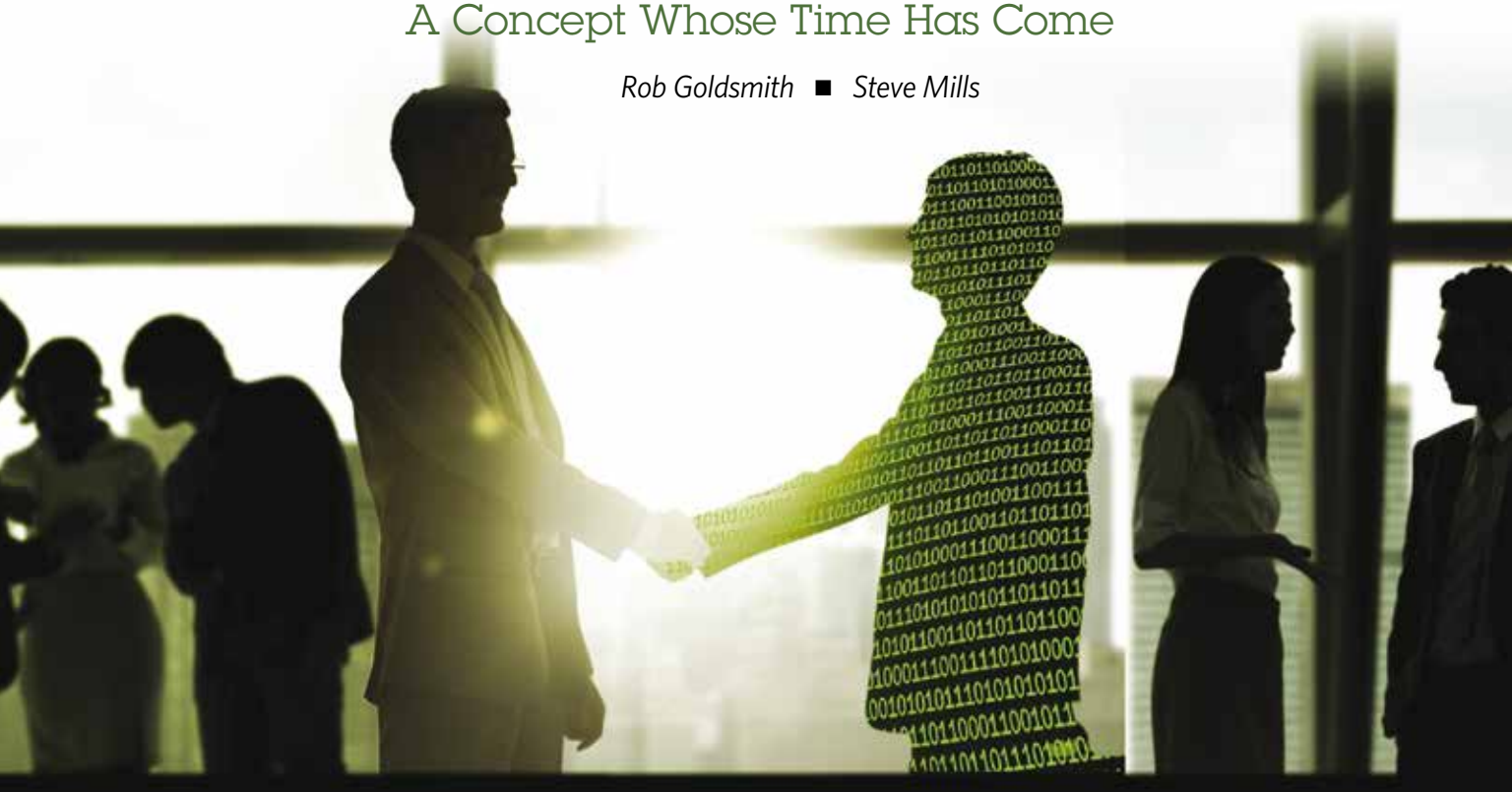
Cyber Integrator

A Concept Whose Time Has Come

Rob Goldsmith ■ *Steve Mills*



Effective cybersecurity in Department of Defense (DoD) acquisition programs is a top concern for both DoD program managers (PMs) and the DoD as a whole. What can be done to help DoD PMs meet this challenge? An emerging concept is the establishment of a "Cyber Integrator" (CI) at the Program Executive Office (PEO)/Major Defense Acquisition Program (MDAP) level, to help address cybersecurity risk in DoD acquisition programs. The purpose of the CI is to lead the cybersecurity efforts within the PEO/MDAP, and that role includes effectively integrating cybersecurity across all functional domains and acting as principal advisor to the PM on all cybersecurity matters. A CI by itself will not mitigate all the cybersecurity challenges faced by DoD PMs, but based on the emerging results of an ongoing Aviation and Missile Research, Development, and Engineering Center (AMRDEC) pilot program, the CI concept appears to be a step in the right direction.

Making a Case for the Cyber Integrator

To appreciate the potential value of the CI concept, consider a comparison between the impact of sustainment on the DoD acquisition life cycle and that of cybersecurity. Such a comparison brings to light common themes that strongly suggest lessons learned about sustainment in the acquisition life cycle are applicable to cybersecurity.

Goldsmith *is a systems engineer and currently the Aviation and Missile Research, Development and Engineering Center Cybersecurity Lead at Redstone Arsenal, Alabama.* **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.*

Sustainment has always been an important component of the DoD acquisition life cycle, but all too often has not been recognized as such. Diminishing sustainment to an afterthought in the engineering process can have significant negative impacts on the viability, performance and overall success of our DoD weapon systems. Sustainment now is a recognized activity spanning the entire life cycle. The concept of sustainment as a design consideration is validated when reviewing the DoD Integrated Product Support Elements. The elements of Design Interface and Sustainment Engineering support this assertion. Sustainment in acquisition programs is proactive. The clear goal for sustainment is to "Bake in sustainment, don't bolt it on." Is cybersecurity any different? Shouldn't our goal for cybersecurity be the same? Should cybersecurity be treated as a design consideration? Should cybersecurity be considered "upfront and early" rather than later in the acquisition life cycle?

Such a comparison brings to light common themes that strongly suggest lessons learned about sustainment in the acquisition life cycle are applicable to cybersecurity.

Sustainment is recognized as a critical component of DoD acquisition programs. With that distinction come requirements to develop a plan, measure its overall effectiveness and have accountability to ensure its overall success. Sustainment for DoD acquisition programs is defined in a statutory Life Cycle Sustainment Plan (LCSP). The LCSP describes the resources and approach for achieving effective sustainment of the program throughout the entire life cycle of the program. The LCSP is a key component of the Acquisition Strategy. The Cybersecurity Strategy provides a similar opportunity to tell the cybersecurity "story" for an acquisition program. How effective is the newly mandated Cybersecurity Strategy in addressing cybersecurity risks in DoD acquisition programs?

Effective management and leadership of the sustainment effort on DoD programs is performed by the Product Support Manager (PSM). The PSM is a statutorily designated position for DoD acquisition programs. The PSM primarily focuses on development and execution of the LCSP. The PSM is the primary advisor to the PM on all sustainment issues. This critical position within the Program Management Office (PMO) provides the PM with a "sustainment champion" who can mitigate sustainment risk to the program across the life cycle. Is the impact and scope of cybersecurity on DoD acquisition programs significant enough to warrant a Cybersecurity champion within the PEO/PMO? If not, how can cybersecurity risks best be mitigated?

The AMRDEC CI Pilot program provides some insight into the overall effectiveness of incorporating a CI into an MDAP. This effort will continue, but initial results are enlightening!

Cyber Integrator Lessons Learned

After a yearlong pilot of the CI concept in an Acquisition Category (ACAT) ID Army Acquisition Program, the AMRDEC has learned a lot of valuable lessons. The CI concept, highlighted in an article by the authors in the September–October 2014 issue of *Defense AT&L* magazine, is an innovative approach that can assist PMs in making better investment decisions about cybersecurity. The Cyber Dashboard is a program management tool that uses program specific cybersecurity metrics to assess the effectiveness of cybersecurity across the acquisition program and life cycle. The Cyber Dashboard provides the PM with a holistic view of cybersecurity risks. The following are some key takeaways for anyone who may consider implementing the CI concept in an organization.

"I would never have given you that resumé." These were the words of the hiring manager after I recommended the individual who now successfully performs the role of CI in the AMRDEC pilot. The hiring manager was perplexed about which attributes he had missed in his screening criteria. So what makes a good CI? Hiring the CI is the single most important decision you will make when employing this concept. The natural tendency will be to look for someone with a traditional Information Technology (IT), Cybersecurity or Information Assurance (IA) background. While a strong background in IA, IT, Blue or Red Team, Systems Engineering (SE) or Cyber Test and Evaluation (T&E) is attractive, I would consider those as desirable but not required qualifications. The two primary required qualifications I looked for were:

- A proven leader able to understand technical concepts and integrate diverse teams working complex projects
- A person having the ability to communicate effectively with technical people and senior leaders through both the spoken word and development of presentation material

The required attributes of an effective integrator and communicator far surpass the advantages that a specialist brings. In fact, specialists are at a disadvantage because they almost always tend to spend undue time and attention on their area

of expertise at the expense of the other important elements of cybersecurity within the office.

"Where the CI sits matters." To be effective in a PMO, the CI must be empowered. CI empowerment. This is achieved through both verbal/written direction by senior leadership to the entire team, as well as organizationally placing the CI under either the chief engineer in the PMO or the deputy PM (DPM). Placing the CI under the lead Systems Engineer or the Systems Engineering, Integration, and Test (SEIT) lead will not send the same message to the team as putting the CI in a position with ready access to program senior leadership. Empowerment is necessary for the CI to gain access to the information needed to develop the program's Cyber Dashboard. The PM must ensure that the CI is invited to key meetings and that he or she is not viewed as outside the PMO "family." Gaining that acceptance will depend in part on the CI's relationship-building skills—but, to succeed, the CI must also have the backing and endorsement of the PM.

"Why are you here? We handle cybersecurity!" Your IA staff is not "baking in" cybersecurity for your acquisition program. The staff is only handling a portion of your cybersecurity. It is a big mistake to believe that the DoD certification and accreditation (C&A) process and cybersecurity are synonymous. IA is an important component of the overall cybersecurity effort, but cybersecurity has many other facets not adequately addressed through C&A alone. These other facets include:

- Software assurance
- Supply chain security
- Vulnerability assessments/Blue Team testing
- Others

This misconception is illustrated by the success rate of the Red Teams during Operational Test and Evaluation (OT&E) against systems that have achieved Authorities to Operate (ATOs) through the C&A process. If you want to fail at OT&E, trust all of your cybersecurity to your IA team. The recent rebranding of IA as cybersecurity in DoD policy can prove misleading to members of the acquisition community, including the PM. Currently AMRDEC has more than 30 full-time IA personnel supporting PMOs and is one of the 11 accredited Army Agents of the Certification Authority (ACAs). AMRDEC clearly understands the importance of IA as a part of cybersecurity, but AMRDEC also understands its limitations.

"Up Front, Early and Continuous." This phrase applies in two ways. First, it is best to get your CI on board as early as possible in the life cycle. The CI can make sure critical contract language is put in place, architectural decisions are made with all facets of cybersecurity in mind and can help steer limited resources to the right places at the right time in the program. The phrase "upfront and early" also applies to educating members of the PMO early. As soon as possible once the CI is on board, the PM, DPM or chief engineer should assemble subordinate leaders, engineers and staff to introduce the CI and explain why the CI has been brought onboard. The team needs to walk away understanding what cybersecurity is, how it differs from IA, who the CI is and what the CI will be doing for the PM. These actions will establish the CI as truly empowered and as a crucial member of the PMO team.

The team needs to walk away understanding what cybersecurity is, how it differs from IA, who is the CI and what the CI will be doing for the PM. These actions will establish the CI as truly empowered and a crucial member of the PMO team.

PMO employees need to know the CI is not an "extra hand" for the IA team, to be saddled with milestone documentation or C&A work. The CI's input is necessary for such tasks, but the CI must avoid the trap of going too deeply into one aspect of cybersecurity and not fulfilling the CI's mission to the PM of capturing the big picture. The CI must be able to work effectively with the team to gather the details from the experts and provide an integrated risk perspective to the PM.

The purpose of this article was to describe an emerging concept of integrating a new role into the DoD acquisition process—the CI. When implemented, the CI provides the PM a cybersecurity champion who can develop and implement an effective cybersecurity solution across the acquisition life cycle of a program or programs. This role may be best suited for only larger programs or implementation at the PEO level with one CI supporting multiple programs. The key point of this article is to present the CI concept, provide insights to date on the AMRDEC CI Pilot effort and to generate discussion on the CI concept. A key question to address is, "What is the risk of not implementing the CI Concept for select PEOs and large acquisition programs?" Please submit your questions and comments to the authors of this article. We welcome them!

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