THE QUEST for Defense Cybersecurity

John A. Shaud ■ Michael G. Lilienthal
Scott Thompson ■ David Brown

Many of the military Services' major weapons programs, both new and legacy, have difficulty negotiating the confusing multitude of Department of Defense (DoD) and Service directives and guidance in order to develop their cybersecurity requirements and strategy. Acquisition and legacy program management, as well as Service Test and Evaluation (T&E) communities, seek methods and tools to allow for the most effective and efficient way to maximize their ability to counter cyber threats.

Let us consider a notional new weapons program, the "USS Jimmy Doolittle," to explore how programs can implement a process to comply with the requirements of Section 1647 of the 2016 National Defense Authorization Act (NDAA) to evaluate cyber vulnerabilities and develop strategies for mitigating the associated risks. A culture

Shaud *is a senior mentor for the Air Force Cyber Operations Executive Course at the Air University in Montgomery, Alabama, a senior consultant to Electronic Warfare Associates, Inc. (EWA), in Herndon, Virginia, and an active participant and mentor to the EWA Cyber Focus Group. He is a retired U.S. Air Force (USAF) general.* **Lilienthal** *is the director of Cyber and Navy Programs at EWA. He has a doctorate in Experimental Psychology from the University of Notre Dame. He served for more than 30 years as a Navy Aerospace Experimental Psychologist and worked in program management, test and evaluation (T&E), and training. He is a retired U.S. Navy captain.* **Thompson**, *a retired USAF colonel, is EWA's director of Cyber and Air Force programs. He is a graduate of the USAF Test Pilot School and holds a Master of Science in Systems Engineering from the Air Force Institute of Technology.* **Brown**, *also a retired USAF colonel, is EWA's director for Cyber Programs. He retired as a Command fighter pilot after 30 years of service in both operations and T&E.*

change also is needed for the Services to develop and execute an effective and efficient cybersecurity strategy.

Cybersecurity is "subject du jour" within DoD. It is the ubiquitous topic. Cybersecurity has the attention of senior DoD officials and the Service chiefs. It is a significant factor for policy and budgets. It affects all Services, most weapons, all command and control systems, all theaters, and all levels of war. Program managers (PMs), engineers, testers, and operators are inundated by a myriad of high-level guidance and directives. Many Service acquisition and Test and Evaluation (T&E) programs find it difficult and confusing to negotiate these policies and processes in order to develop their requirements and strategy for cybersecurity T&E. Troops are curious about cybersecurity, but have for the most part limited training other than yearly online information assurance (IA) refresher training. That IA term was formally dissolved years ago—yet remains in everyone's lexicon.

There are many DoD and Service policies, processes and programs regarding cyber and cybersecurity. But let's address what is commonly referred to as Section 1647. Or more specifically, the 2016 NDAA, Section 1647: Evaluation of Cyber Vulnerabilities of Major Weapons Systems of the DoD. Of primary interest within Section 1647 are:

- Part (a) Evaluation Required. (1) In General. "The Secretary of Defense shall, in accordance with the plan under subsection (b), complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense by not later than December 31, 2019."
- Part (d) Risk Mitigation Strategies, which states: "As part of the evaluation of cyber vulnerabilities of major weapon systems of the Department under this section, the Secretary shall develop strategies for mitigating the risks of cyber vulnerabilities identified in the course of such evaluations."

Section 1647 also addresses various additional topics, including: Exceptions, Priority in Evaluations, Integration with Other Efforts, Status on Progress, and Authorization of Appropriations, which is set at $200 million DoD-wide to fulfill the stated requirements.

This seems to be very clear guidance for both. However, if you were a DoD acquisition or legacy PM or a chief information officer, questions would remain: What do you do? How do you execute? Where do you start?

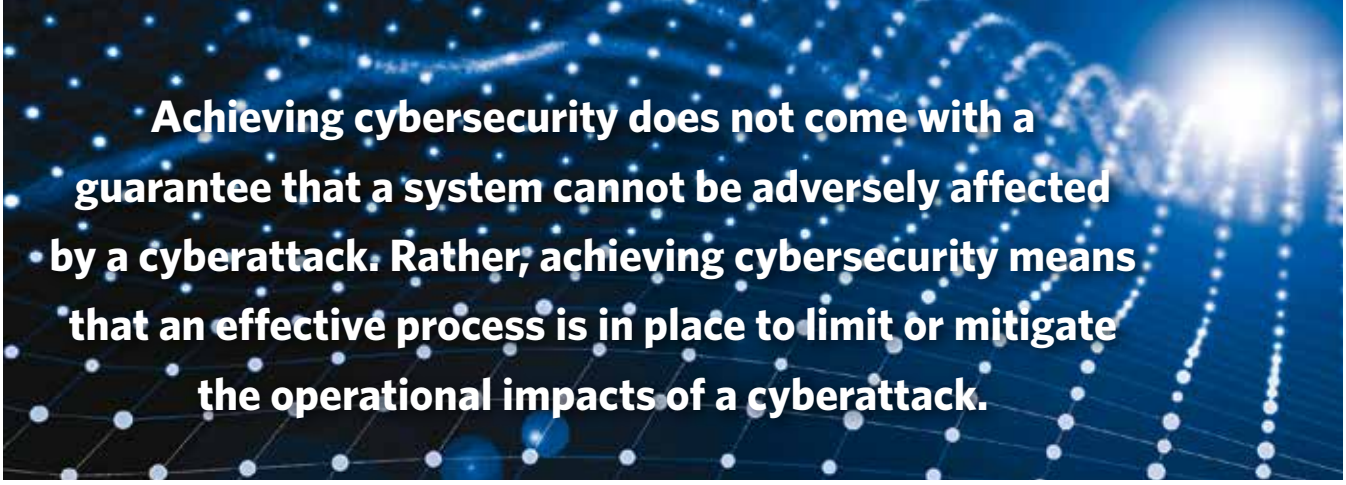
What Is Cybersecurity?

According to DoD Instruction (DoDI) 8500.01 (Cybersecurity), it is the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." A 2015 RAND Corporation report on Air Force cybersecurity referenced DoDI 8500.01 definition above, adding that cybersecurity is "limiting adversary intelligence exploitation to an acceptable level and ensuring an acceptable level of operational functionality (survivability) even when attacked offensively through cyberspace." Cybersecurity should not be viewed as an end state. Achieving cybersecurity does not come with a guarantee that a system cannot be adversely affected by a cyberattack. Rather, achieving cybersecurity means that an effective process is in place to limit or mitigate the operational impacts of a cyberattack.

Cyber resilience is an important component to cybersecurity and is relevant to any effort regarding Section 1647. A recent Navy (OPNAV [Office of the Joint Chief of Naval Operations] N2/N6) presentation defined cyber resiliency as "continued operations in a contested cyber environment." The Navy's CYBERSAFE program strives to "provide maximum reasonable assurance of survivability and resiliency of mission critical information technology, in a contested cyber environment in order to maintain mission capabilities." However, cyber resilience is not a term unique to the DoD. Cyber resilience, as defined by Presidential Policy Directive 21, is the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." Wikipedia states that, "The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously at all times. This means even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms."

Cybersecurity and cyber resilience are linked by an emphasis on mission effectiveness. Achieving cybersecurity means designing and fielding new and legacy systems capable of carrying out operational missions despite opposition in the cyber domain—not just attempting to prevent intrusions. To achieve cybersecurity, designers and planners must incorporate cybersecurity concepts into the initial development of new systems and sub-systems. T&E must be based on potential vulnerabilities identified early in the acqusition cycle to ensure the most efficient use of limited T&E resources. Operational influence must be fully engaged in this process, and operators must have input into all phases of the acquistion process—from initial concept through design and engineering along with doctrine, organization, training, materiel, leadership and education, personnel and facilities.

But how does all this affect the requirements of Section 1647 to "complete an evaluation of the cyber vulnerabilities of each major weapon system" and "develop strategies for mitigating the risks of (identified) cyber vulnerabilities"? Each DoD major



weapon system is a complex System-of-Systems (SoS), and Section 1647 does not discriminate between new and legacy programs. This is a very complex problem and the questions still remain: What do you do? How do you execute? Where do you start?

Looking at Our Theoretical Example

Before we address these questions, we need to introduce the imagined "USS Jimmy Doolittle." The Jimmy Doolittle is a notional complex major weapons system that can serve an example of how to achieve cybersecurity. The Jimmy Doolittle is presented as a contrived new class of aircraft carrier: 1,156 feet long, with a beam of 150 feet at the water line and displacing well more than 101,000 tons. The Jimmy Doolittle's mission is power projection and combat. Specific tasks include air, surface, and antisubmarine warfare, command, control, and communications (C3), command and control warfare (C2W), intelligence, mine warfare, and strike warfare. All that is in addition to the ship performing fleet support operations, logistics, non-combat operations and naval special warfare.

The Jimmy Doolittle is a very complex SoS. Beyond the systems required to perform the previously listed missions and tasks, it requires a secure command, control, communications, computers, and intelligence (C4I) system, enclaves for unclassified, coalition, secret, and for special compartmented information (SCI) environments. To be effective, it must have a common computer domain for conducting command, control, intelligence, business, maintenance, supply and aircraft. In addition, the Jimmy Doolittle must communicate with a great many support and sub-systems. A significant number of these are legacy systems. Many were not designed for cyberattack, and all of these systems and sub-systems are subject to routine software and firmware upgrades. This makes the USS Doolittle a good example of how to negotiate the Section 1647 requirements.

What are the vulnerabilities of this very complex weapons system? Even in peacetime, the ship can expect routine cyberattacks on its communications pathways. In wartime, successful cyberattacks on its C4I, mission planning or other communications links could render this SoS ineffective or nonsurvivable. How can relevant vulnerabilities be identified? How should any identified vulnerabilities be prioritized? What can be done to mitigate these vulnerabilities to provide the Jimmy Doolittle with cyber-resiliency?

Achieving cybersecurity requires an iterative process that ensures cybersecurity and cyber resilience are planned for, developed, tested, implemented, evaluated, and made integral to operational employment in order that expected cyberattacks are so mitigated that mission accomplishment is not jeapordized. The PMs for the Jimmy Doolittle knew they had to design, build, test and then begin shipboard operations with cyber resilience embedded into the culture across the entire program.

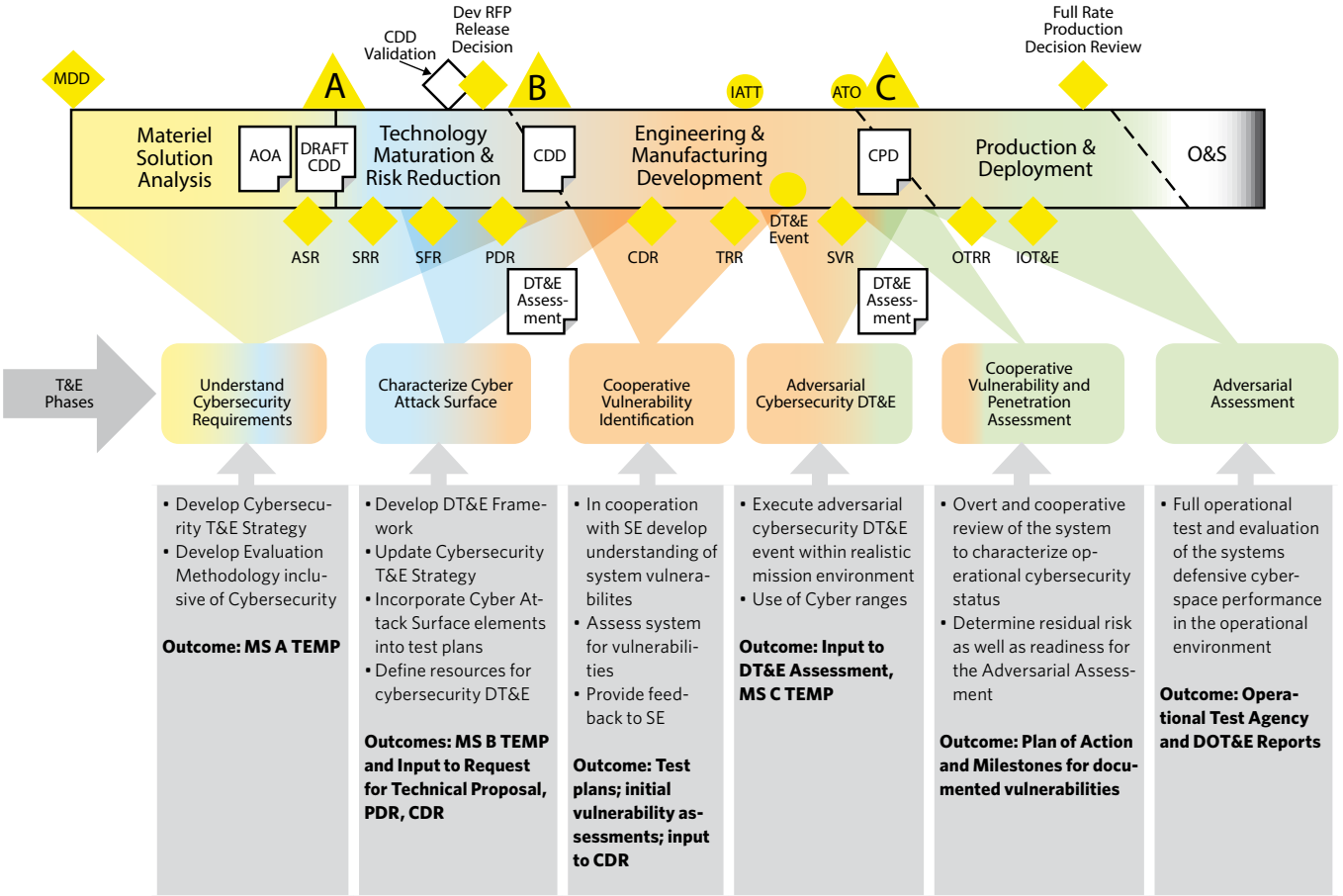
First Main Focus: Start Early

There were two primary focus areas to implement this process for cybersecurity.

First of all, they understood that cybersecurity starts early with concept development and systems engineering. DoDI 8500.01 (Cybersecurity) states: "Cybersecurity must be fully integrated into system life cycles and will be a visible element of organizational, joint, and DoD Component IT [information technology] portfolios." However, mere reliance on DoD and Service compliance activities will not ensure success. Cybersecurity became an integral part of the design and cultural process of the notional example of the USS Doolittle. It focused on resiliency and mitigating cyberattacks. In our example, early in the design phase the PMs began a disciplined and iterative process they termed a cyber operational vulnerability assessment (COVA) for cybersecurity. The Doolittle COVA is a rigorous process leveraging "tabletop" wargaming principals focused on developing an understanding of (1) how personnel actually use and maintain a system to carry out a specific mission, (2) how successful cyberattacks degrade or prevent operational mission success, and (3) how potential actions or workarounds might prevent or minimize cyber effects. The COVA process developed and used by the Doolittle Program Office is intended to be used throughout the life cycle of the Doolittle program—from concept development thru operational deployment and sustainment.

COVA is a low-cost, intellectually intensive, and interactive data collection and analysis process that introduces and

Figure 1. Six-Phase Process for Cybersecurity T&E in Accordance With the DoD Guidebook



For a more complete review, see the *Cybersecurity Test and Evaluation Guidebook Guidebook*, Chapter 3.

Key to Abbreviations Used in Figure 1

AoA = analysis of alternatives; CDD = Capability Development Document; CDR = critical design review; ASR = alternative systems review; DT&E = developmental test and evaluation; ATO = authorization to operate; CDR = critical design review; CPD = Capabilities Product Document; IOT&E = initial operational test and evaluation; MDD = materiel development decision; MS = Milestone (A,B,C); OTA = Operational Test Agency; PO&S = operations and sustainment; OTRR = operational test readiness review; POA&M = Plan of Action and Milestones; PDR = preliminary design review; RFP = Request for Proposal; RFTP = Request for Technical Proposal; SE = systems engineering; SVR = systems verification review; T&E = test and evaluation; TEMP = test and evaluation master plan; TRR = test readiness review.

explores the effects of cyber-offensive operations on an SoS capability to execute a mission. It was designed to help identify, size and scope the test effort in the cybersecurity focus area and to identify potential threat vectors, the risks associated with threat vectors, and potential threats from boundary systems (e.g., programs outside of the PM's control). A COVA produces a prioritized list of actionable recommendations for making tradeoffs in a fiscally constrained environment. Leveraging the COVA results, the USS Doolittle managers ensured the engineers and cybersecurity personnel worked with those with active duty experience so both would have a deep understanding of the technological capabilities of the new system(s). They also were able to incorporate a cyber awareness into the ship's operators and aviators that would permeate into all shipboard operations.

At the same time, the managers demanded all shipboard disciplines work as one team to understand potential cyber effects and mission consequences. Because they participated in a COVA, the Doolittle's cyber warriors now understood the mission and the operational environment and how it might be affected by their controls and protections. The operators (aviators, maintainers, supply officers, ship drivers, etc.) now understand the potential for cyber affects—that is, they understood the controls and protections needed for their own mission success. Together, these two communities were able to effectively communicate to PMs the risks, costs, limitations, and alternatives of protections and controls.

Capitalizing on this relationship, potential "workarounds" or engineering options were developed and evaluated

continuously throughout the acqusition and development process. Operators, maintainers, systems engineers and cyber experts were brought together to not take the approach of compliance with current checklist directives and policies but to approach the design, operation and maintenance of the USS Doolittle from the mission viewpoint. They assumed they would be operating in a cyber-contested environment; that cyber hackers would find new and innovative ways to penetrate vulnerabilities and weaknesses; that all software and firmware were flawed; and that personnel who operated the USS Doolittle would make mistakes that would allow for a cyberattack. They looked at designs and design tradeoffs early with that in mind. As system design progressed, they continued the iterative COVA process to include the more mature versions of systems and added additional systems to the process to ensure operational relevance. Eventually, due to the complexity of the Doolittle, individual systems were broken out and a similar process was completed, with a focus on assessing access pathways for the attack, command and control of malware, and the effects of a successful attack on a system.

Second Main Focus: Test and Evaluation

The second primary focus area of the USS Doolittle's cybersecurity was T&E. As the Doolittle began to mature and approached the testing phases, program management already had an eye for developing an effective and efficient T&E program. The six-phase process for cybersecurity T&E is outlined in the *Cybersecurity Test and Evaluation Guidebook* and has been adopted as the DoD standard. A key feature of this process is an early and iterative involvement in test planning and execution (Figure 1).

The T&E community seeks to understand the procedures, methods, test ranges and tools necessary to address the six-phase process. At the same time, many programs and T&E professionals are having difficulty deciphering the multitude of DoD and Service directives and guidance in order to develop a cybersecurity T&E strategy. For example, although there are six phases for cybersecurity use throughout the acquisition life cycle, there is anecdotal information that many programs and T&E efforts enter directly with a Red Team penetration assessment and then consider themselves to be in compliance with DoD directives.

For effective and efficient T&E, the T&E community needs to take the correct steps early in understanding the threats and the vulnerabilities. These threats and vulnerabilities can be part of the system design or can be introduced through other programs of record that make up many of the complex systems fielded by the DoD.

The Doolittle COVA process directly supported the first three phases of the six-phase cybersecurity testing process: Understanding cybersecurity requirements; characterizing cyberattack surfaces; and identifying cooperative vulnerability. However, the results of the COVA also provided actionable and credible inputs to the fourth phase: Adversarial cybersecurity developmental T&E.

Finally, an established COVA process furnished Doolittle T&E planners with inputs to the fifth phase (cooperative vulnerability and penetration assessment), and it provided valuable insights to the final phase: Adversarial assessment. Almost as important, the COVA process has been a cultural change mechanism to move the Doolittle Program from a checklist information assurance strategy to a proactive iterative risk management process aimed at ensuring personnel can still carry out the mission even in the face of successful cyberattacks.

The USS Doolittle has many attack surfaces and pathways. For example, in addition to the myriad systems and sub-systems, PMs knew their young crew would bring onboard personal computers and mobile devices that can be plugged into the ship's network. The presence of the latest virtual reality devices and Internet of Things (IoT) has exploded in the private sector and become part of the way of life for much of the crew. Maintenance devices are becoming wireless connecting via the next generation Bluetooth, and software patches reveal vulnerabilities of the Doolittle operating systems, etc. Even our fictitious USS Doolittle, as large an acquisition program as it was supposed to be, lacked the time and funding to test all communication pathways and entry points.

Three actionable recommendation categories for the T&E community were produced by the Doolittle's COVA process:

- Recommend the cyber weakness/vulnerability is an acceptable risk due to the difficulty of the cyber attack succeeding and/or the minor effect of a successful attack on the mission.
- Recommend further analysis because there is insufficient understanding of the system under development to determine the degree of vulnerability or the degree of cyber effect.
- Recommend testing due to the mission criticality and the likelihood of a successful cyberattack on mission success.

Once identified, vulnerabilities were sorted into risk initial assessments. The Doolittle planners knew that they simply couldn't test to every cyber eventuality. The results of the risk assessments were used to design and plan an efficient T&E strategy. This iterative process, begun early, allowed multiple legacy systems and sub-systems onboard the USS Doolittle to be tested in an expected operational environment with the results focused on mitigating mission impact.

As the Doolittle continued to mature and progress through the acquisition cycle, the PMs emphasized the slogan of "one team, one fight!" This required Service-certified Blue and Red Teams to become more involved in the correction of found vulnerabilities. The first step was to move beyond the "we got in" mentality. Cyber teams, both Blue and Red, engaged with the

systems engineers and operators by helping them understand not only that they got into the system (a "gotcha" approach does not instill team cohesion) but how to fix and prevent such intrusions. Both Red and Blue Teams worked early and continuously in the acquisition process as partners with the design and engineering teams, as well as operators.

The Doolittle's COVA process also revealed that Electronic Warfare (EW) needs to be considered in tandem with cyber warfare. The use of the Electromagnetic Spectrum (EMS) can be affected or disrupted by cyber or EW. The EMS is critical for communications, command and control, blue force tracking, precision attack, and, to a certain extent, most warfighting capabilities. Current adversaries certainly understand how the United States uses and depends upon EMS, and they will contest our military's access to it. Leadership cannot deal with cyber and EW separately; for cybersecurity, they must be viewed as a complement to each other.

MDAP/MAIS Program Manager Changes

With the assistance of the Office of the Secretary of Defense, *Defense AT&L* magazine publishes the names of incoming and outgoing program managers for major defense acquisition programs (MDAPs) and major automated information system (MAIS) programs. This announcement lists all such changes of leadership, for both civilian and military program managers for July-August 2017.

Army

COL Francisco J. Lozano relieved **COL John M. Eggert** as project manager for lower tier on July 12.

Navy/Marine Corps

COL Matthew Kelly relieved **COL Daniel Robinson** as program manager for V-22 OSPREY Joint Advanced Vertical Lift Aircraft (PMA-275) on July 5.

CAPT Philip Malone relieved **CAPT Douglas Oglesby** as program manager for GERALD R. FORD CLASS Nuclear Aircraft Carrier (CVN 79) (PMS-379) on July 21.

CAPT Michael Taylor relieved **CAPT Thomas Anderson** as program manager for Littoral Combat Ship (PMS-501) on July 31.

Air Force

Col Todd D. Darrah relieved **Col Darien J. Hammett** as program manager for the Global Hawk Unmanned Aerial Vehicle Program on July 1.

Col Darien J. Hammett relieved **Col Anthony W. Genatempo** as program manager for the F-22 Modernization Increment 3.2B Program on July 1.

Summary and Conclusion

Successful implementation of the evaluation of the cyber vulnerabilities and developing strategies for mitigating the risks required by Section 1647 requires a culture change on how cybersecurity is addressed for legacy as well as for new systems. Achieving cybersecurity focuses on mission accomplishment by aiming to minimize mission impact of successful cyberattacks. While the USS Doolittle is a fictitious program, the solutions discussed to implement Section 1647 for new and legacy programs are not fictitious and can work in the real world. The COVA described in this article was developed on the foundation of a cyber "tabletop" process that the U.S. Naval Air Systems Command (NAVAIR) has adopted as a standard work package for determining cyber vulnerabilities and requirements. The cyber tabletop process was recognized by NAVAIR as an important tool in an operational threat risk assessment as well as a catalyst for intellectual change. A senior NAVAIR director offered the following assessment following a recent cyber tabletop exercise:

"The event was a 'game changer' in that it not only helped identify vulnerabilities but it tied them to mission risk and also helped with the culture change necessary to get our entire workforce behind this important topic. Getting our engineers, fleet, and program offices to understand exactly what a potential adversary could do to a ship's ability to safely and efficiently launch and recover aircraft was worth it alone. We will be using the results from this event to drive POM [Program Objective Memorandum] requests, recommend technical fixes, plan further analysis/testing, as well as change some of our internal processes."—By permission, June 12, 2017, Kathleen P. Donnelly, Senior Executive Service, NAVAIR 4.8, director, Support Equipment and Aircraft Launch and Recovery Equipment.

To succeed with Section 1647, programs must implement a low-cost, intellectually intensive, data collection and analysis process that introduces and explores the threat that offensive cyber operations pose to mission impact. This process identifies credible cyber vulnerabilities, potential threat vectors, risks to the mission, and potential threats from boundary (e.g., legacy) systems as early as possible. This process must be iterative, expeditious and readily understandable to the operators and maintainers. It should be implemented early and continuously across the acquisition life cycle to ensure continued cybersecurity. The process must provide actionable information to correctly size and scope cybersecurity T&E efforts. Furthermore, the culture of cyber awareness must permeate into all facets of weapons systems acquisition, training, maintenance and operations.

The key to achieving cybersecurity is development of a process for embedding cybersecurity across the life cycle of acquisition design, development, testing, and employment life cycle. It's past time we got started.

The authors can be contacted at **JShaud@afa.org**; **MLilienthal@ewa.com**; **SThompson@ewa.com**; *and* **DBrown@ewa.com**.