www.dau.mil | July-August 2016

Defense AT&L
Acquisition, Technology and Logistics

A PUBLICATION OF THE DEFENSE ACQUISITION UNIVERSITY

Risk Management

SPECIAL SECTION

A Primer on Risks, Issues and Opportunities

Robust, Replicable and Defensible Risk Management
At Headquarters or the Front

Supply Chain Risk Management
An Introduction to the Credible Threat

Improving Acquisition From Within
Suggestions From Our PEOs
by the Under Secretary of Defense for Acquisition, Technology, and Logistics

CONTENTS

ALSO

Defense
AT&L

Vol XLV No. 4, DAU 251

Published by the
DEFENSE ACQUISITION UNIVERSITY

Article preparation/submission guidelines are located on the inside back cover of each issue or may be downloaded from our website at <http://www.dau.mil/pubscats/pages/defenseatl.aspx>. Inquiries concerning proposed articles can be made by e-mail to datl@dau.mil or by phone to 703-805-4282 or DSN 655-4282.

Subscribe/unsubscribe/change of address: Fill out, sign, and fax or e-mail the subscription form in the back of this issue, or download the form at <http://dau.dodlive.mil/files/2015/04/Online-Subscription.pdf>.

Privacy Act/Freedom of Information Act
If you provide us your business address, you will become part of mailing lists that are public information and may be provided to other agencies upon request. If you prefer not to be part of these lists, use your home address. Do not include your rank, grade, service, or other personal identifiers.

Defense AT&L (ISSN 1547-5476), formerly Program Manager, is published bimonthly by the DAU Press and is free to all U.S. and foreign national subscribers. Periodical postage is paid at the U.S. Postal Facility, Fort Belvoir, Va., and additional U.S. postal facilities.

POSTMASTER, send address changes to:
DEFENSE AT&L
DEFENSE ACQUISITION UNIVERSITY
ATTN DAU PRESS STE 3
9820 BELVOIR ROAD
FT BELVOIR VA 22060-5565

Improving Acquisition From Within

Suggestions From Our PEOs

Frank Kendall

This year I asked all of our Program Executive Officers (PEOs) to provide short assessments and recommendations to me directly. The result, as it was for the Program Manager Assessments I've received for the last 2 years, has been a treasure trove of observations and recommendations covering a wide range of topics. I thought it would be useful and insightful for the entire workforce to see some of these professional, and very frank, comments. I've removed most inputs that were about specific programs and edited lightly to make some of the inputs less Service specific. Arranged alphabetically by topic, and presented without comment, here is a sampling of the topics on our senior line managers' minds as they confront the many challenges we face.

Acquisition Education: Cybersecurity requirements continue to grow impacting virtually everything we do in acquisition from daily workplace activities, to Enterprise Resource Planning (ERP) system development, to weapon system development. Additionally, the Department of Defense (DoD) is required to certify audit readiness in Fiscal Year (FY) 2017. Audit readiness affects every career field in acquisition, not just financial management professionals. Ensure that the Defense Acquisition

University curriculum is updated to reflect audit readiness and cybersecurity considerations and requirements for all of the career fields.

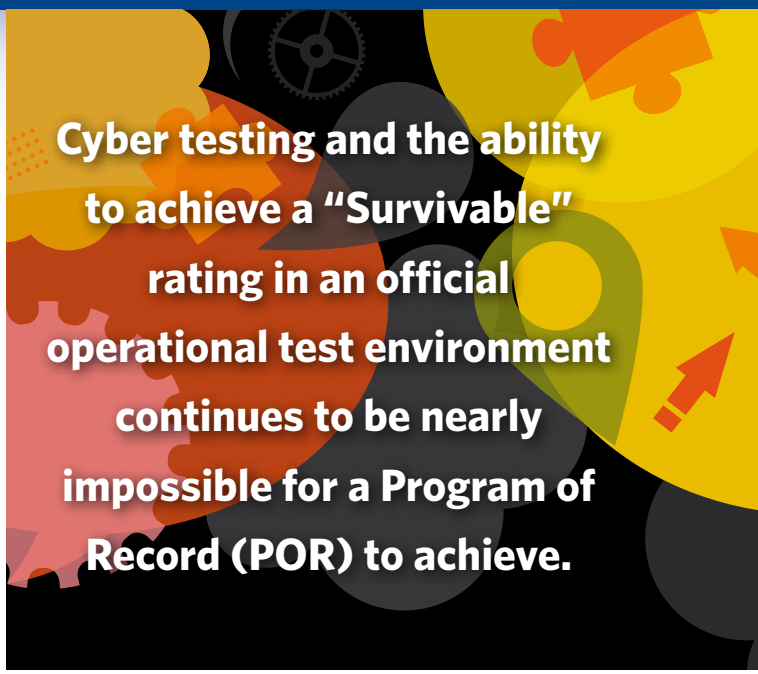
Also, an executive-level Acquisition seminar for our senior General/Flag Officers, especially those assigned in the Pentagon, would advance acquisition reform. We consistently find ourselves answering questions to our Service Chiefs and members of Congress that are far outside of acquisition responsibilities. This is a team sport, and DoD would be better served if all of our most senior leaders had a basic understanding of the Defense Acquisition process and their respective roles in it.

Business Cases and AoAs (Analysis of Alternatives): Why would we do both? There is too much complexity and lack of clarity between the Deputy Chief Management Officer and the role of the Office of Acquisition, Technology, and Logistics.

Clinger-Cohen Act (CCA) Compliance: CCA mandates the completion and approval of numerous other programmatic documents as supporting documentation before a program's CCA can be certified. The Army Chief Information Officer (CIO)/G6 estimates the staffing and approval for a program CCA compliance determination to take up to 120 days to complete. Two supporting documents required for submission for a CCA compliance determination are (1) Test and Evaluation Master Plan (TEMP) and (2) Acquisition Program Baseline (APB). Because of the potential lead time required to support a CCA determination (120 days), we recommend that draft versions of the TEMP and APB be authorized for submission for CCA compliance purposes. We also recommend that significant programmatic changes identified during documentation staffing that would alter the CCA compliance determination be presented during an abbreviated and accelerated update to allow programs to simultaneously staff critical documents without delaying program schedules.

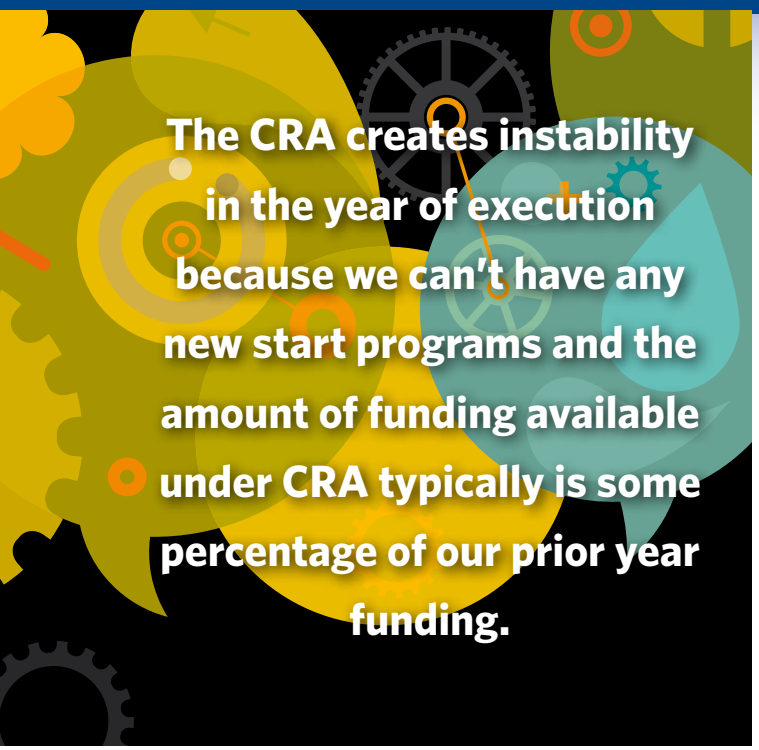
Configuration Steering Boards (CSBs) and Testing: CSBs have been especially helpful in adjusting requirements (both to provide a forum for the deliberate addition of some requirements as well as removing some requirements where they don't make sense). This process should be extended to include using the CSB process to adjust test plans and requirements as well rather than allowing independent members of the test community virtually unlimited authority to commit programs to cost and schedule of tests that the operational leaders of the Service do not believe are warranted. Similarly, it would provide a forum for those same uniformed leaders to insist on testing that might otherwise be overlooked.

COTS and NDI Acquisition: Financial Management Regulation must be clarified to provide consistent guidance on the use of procurement funds in lieu of research, development, test and evaluation (RDT&E) funds to test Commercial Off the Shelf (COTS) and Non-Developmental Items (NDI). This has tremendous impacts across my portfolio, which is heavily reliant on COTS/NDI and could mitigate additional funding stability risks if properly clarified where both the budget analysts and the lawyers agree on the flexibility to use either procurement or RDT&E to test COTS/NDI.



Cyber Security Testing: Cyber testing and the ability to achieve a "Survivable" rating in an official operational test environment continues to be nearly impossible for a Program of Record (POR) to achieve. Test criteria are not well defined and, even if requirements are met, the standards and scope is "independently" determined by the OTA or DOT&E for success. The threat portrayal often exceeds the capabilities of a Blue Force Team (i.e., nation-state threat going against a brigade-level formation), focuses more on "insider" threat of unreasonable proportions, and minimizes the importance of "defense in depth" approach. Recommend better definition for standard cyber rules of engagement at operational test, the allowance for external cyber protection teams, and that test reports focus on the program under test (not the overall "network").

Fiscal Law Constraints: It is likely pie in the sky, but to operate with a single color of money would greatly improve our efficiency and effectiveness. We spend far too much time trying to discern the gray areas that exist between the appropriations. Functioning with Operation and Maintenance dollars during periods of continuing resolutions and severe cash distribution challenges, makes continuity of support a challenge and results in all sorts of bizarre contract actions. If we operated primarily in an Other Procurement world with



narrow definition on true RDT&E (introduction of truly new functional envelopes), we would be much more efficient and effective stewards.

Funding Concerns (10 USC Section 2282): I continue to bring this up to anyone who will listen to me. This pseudo-Foreign Military Sales (FMS) funding is an excellent tool in that it allows us to deliver capability and build Combat Command (COCOM) military partnerships, particularly in countries that can't afford to invest in our weapon systems. That said, the funding is restrictive in that we need to figure out what we're going to buy, put together an acquisition strategy, and get it on contract in the year appropriated (which drives some bad acquisition behaviors). The biggest challenge is that we can only use Section 2282 funding to sustain the system for 2 years. After that, the receiving country must create/fund an FMS case or the COCOM must provide funding. Bottom line is that there is a high risk that these great capabilities will be left to rot and quickly become useless.

Funding Stability and Flexibility: For the last several years, we have started each fiscal year under Continuing Resolution Authority (CRA) for 3 to 4 months before the budget is enacted and funding begins to flow. The CRA creates instability in the year of execution because we can't have any new start programs and the amount of funding available under CRA typically is some percentage of our prior year funding. This instability is exacerbated by the fact that our funding execution is measured against the Office of the Secretary of Defense (OSD) obligation and expenditure goals that do not take into consideration the delay in receipt of funding caused by operating under a CRA. As a result of missing OSD execution goals, funding often is rephased in the out-years, which perpetuates the situation as the cycle has consistently repeated itself and is likely to do so in the future. It would be helpful if the OSD Comptroller could adjust the OSD obligation and expenditure goals to "start the 12-month clock" when the Defense budget is actually passed and not on Oct. 1, as they do now.

Hiring Authority: The agility of a PEO to support its portfolio with appropriate personnel is not adequate with the formal billeting and staffing process and needs to move to a management to budget construct that allows the hiring of additional government personnel.

Human Capital: As the military service begins to reduce force structure, similar reductions are taking place across the civilian workforce. Additionally, there is pressure from Congress to reduce the number of support contractors across DoD. My workforce is comprised of military members (4 percent), core DoD civilians (15 percent), matrixed DoD civilians—combining the traditional and product organization structure—(46 percent) and support contractors (35 percent). With all of these components being driven to reduce numbers and no relief from the mission requirements and expectations, my PEO organization will be challenged severely, even after realizing process efficiencies, to effectively perform the mission unless some portion of the workforce can be stabilized.

Innovation: In intelligence, surveillance and reconnaissance and in working with Special Operations Forces, we are working hard at giving people the tools to bring out their innovative side and give them the confidence to be creative. It is probably the most enjoyable part of my job. I have numerous examples of recent initiatives, but will mention just two of them. First, the Rapid Development and Integration Facility (RDIF) continues to grow as a place where government program managers (PMs) and engineers (sometimes in partnership with small business) are rapidly modifying everything from gunships to B-2s to helicopters. They are taking back the technical baseline, learning how to innovate and growing confidence in our government teams. Second, is the Revolutionary Acquisition Techniques Procedures and Collaboration (RATPAC) forum run jointly between the Air Force and Special Operations Command. Twice a year we select about 50 junior acquisition professionals to attend an intense week of engagement with our most innovative acquisition, warfighter and congressional thinkers. They leave RATPAC fired up to be acquisition combat enablers, and it is really special to see.

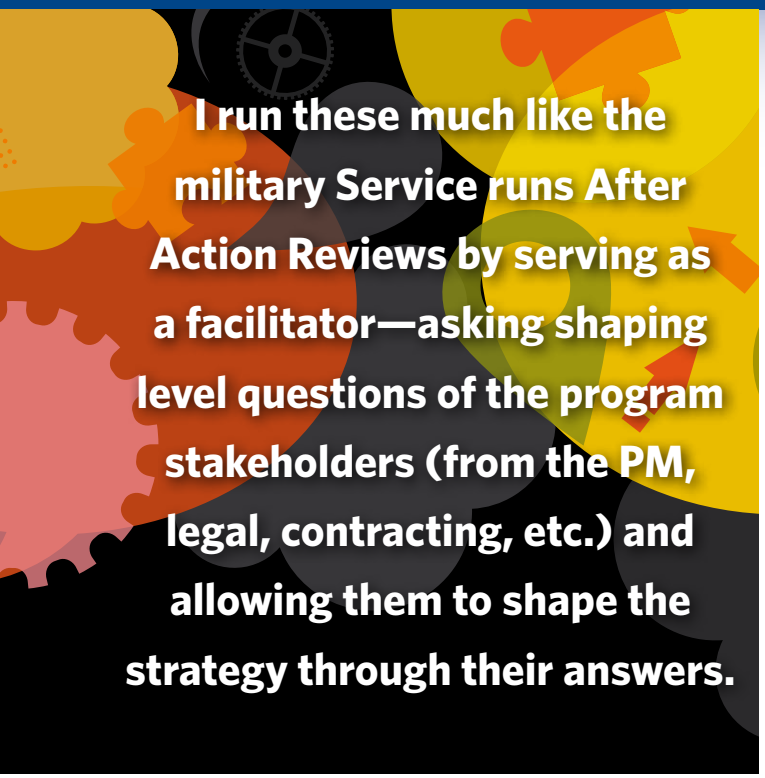
Obsolescence: We face an ever-growing challenge dealing with obsolete parts when we build on a COTS-based infrastructure. Components over the life cycle of our programs

become obsolete when supply chain providers move on to next efforts or divest in the business area. We have seen cases where we are replacing obsolete components on a system prior to fielding the initial capability. Many vendors are updating their products at an increasing rate and do not maintain or support older versions of their equipment. This is true for both software and hardware. Programs need to ensure they adequately budget for these activities and have the correct personnel to address these issues throughout the life cycle of programs. We also need to engage with vendors early to ensure we have long term sustainment strategies that may include extended lifetime buys for key components early in a program to ensure long-term supportability as well, and address the ability to upgrade at the component level to meet any potential obsolescence issues. Help is needed in supporting continuous low-level modification lines to deal with obsolescence issues.

Protests: I recommend that there be a penalty for protesting to discourage weak protests. Example: paying the DoD's legal costs, or paying some penalty for the program disruption.

Quality and Clarity of High Level Taskers: I would like to address the quality of taskers or assignments received at my level. Often a broad-based tasker is issued and, as it flows down the chain of command, it is interpreted in various ways by a number of different people to the point where nobody really understands what information is required. These taskers should be clear and concise from the beginning and follow established staffing chains to ensure that we are not wasting precious resources (time, money and people) providing data and information that does not properly respond to the issue.

Quick Reaction Capabilities: This year alone, I had 42 Quick Reaction Capabilities (QRCs) that I managed and reviewed as separate programs and resolved that 5 be closed, had 10 pending closure once 100 percent accountability of assets is resolved, 7 transitions to existing Programs of Records (PORs), and 20 that will continue to be managed as standalone QRCs. Note that no QRC comes with organic personnel resources and must be managed with allocated POR resources and the heavy use of matrix and contractor support. This is not a sustainable model. The military Service is working the requirements process that supports these transitions. However, the alignment with the Program Objectives Memorandum (POM) process inherently results in a 2-year gap that we have only been able to solve because of the availability of supplemental appropriations. If supplemental dollars did not exist, we would have been unable to transition and/or retain QRC capabilities to the degree we have successfully done to date. The delay in obtaining updated requirements documents hinders the ability to compete in the POM process and exacerbates the gap. A second issue with QRC transitions is balancing the adequacy of testing to support POR transition and milestone decisions. In many cases, these capabilities have been operated effectively for thousands of hours in combat—meeting requirements as specified for military utility, which ought to be the goal of an Operational Test event. Testing a QRC now for integration into a POR, should only verify any changes caused by modifying/integrating on platforms or needed changes to address usability/human factors of the system when we transition from contractor to green suit sustainment/operations. In many cases, we are spending extensive resources (time, money, test ranges, personnel expertise) to retest basic sensor performance on capabilities which have been operating in combat for more than 10 years as a QRC. The Service Test and Evaluation Organization, the OSD Offices of Developmental Test and Evaluation and of Operational Test and Evaluation need to adjust to a more continuous evaluation process and away from the big bang, all-inclusive testing. Finally, overall, the DoD Instruction (DoDI) 5000 series guidance does not address the process of the transition of QRCs to PORs. For example, personnel Concept Plans to support program office manning take forever, material release tailoring is all but nonexistent to deal with COTS, and timely requirements documentation and integratiion of funding into the appropriate Program Evaluation Groups/base are challenging tasks. The aforementioned conditions cause PMs to focus on near-term resourcing and not effective/efficient program management. Help is needed from an institutional perspective to take lessons learned and



update policies and provide tailoring procedures for improved transitions.

Reprogramming Authority: Another way to provide additional flexibility would be to allow greater reprogramming thresholds (this requires approval from Congress). Higher Below Threshold Reprogramming limits go hand in hand with giving PEOs/PMs greater authority to move cost savings realized from successful Better Buying Power (BBP) initiatives within our funding lines. This would also act as a strong incentive for the Defense Acquisition Workforce to inculcate BBP principles into our programs.

Requirements Process: I suggest that both the operational and acquisition communities focus serious attention at the most senior levels on implementing a simplified requirements process which better facilitates the rapid technology/threat cycles within the cyber domain.

Risk Management Framework (RMF): The construct has added time to the process with, in my opinion, no added benefit to date. This process needs quick efficiency reviews and updating. Help is needed in making the RMF more efficient and shorter.

The new RMF process (which replaced the DoD Information Assurance Certification and Accreditation Process), providing for certification and accreditation of weapon systems, has been too unwieldy for the speed and agility needed in approving cybersystem solutions. Specifically, we have identified the following issues with the RMF process as applied to cyber weapon systems:

- RMF levies heavy requirements for monitoring, software updates and policy controls that are less bound by operational concerns than previous systems.
- RMF causes a large resource burden of time and manpower. With the volume of work entailed in RMF, it is difficult to make consistent progress or to develop reliable schedules to inform our operational user. Additionally, the unplanned burden on program offices to apply RMF is taking resources from fixing user issues and addressing modernization needs.
- There was little structure put into phasing the RMF requirement into weapon systems. The full requirement was mandated with less than 2 years to prepare, with limited waiver opportunities provided.
- While new systems in development can accommodate RMF during the design process, legacy systems were not designed with RMF security controls in place, so there are significant programmatic and operational impacts to meeting the RMF controls. Thus, applying RMF to currently fielded operational systems puts undue burden on the operational user.
- Control of and accountability for system cybersecurity is spread over numerous organizations and is poorly integrated, resulting in diminished accountability and unity of command and control for cybersecurity. These overlapping roles create ambiguity regarding whether the commander or the authorizing official can make the final decisions regarding risk to a mission.
- The coordination process for RMF approval packages continues to evolve. Changes in expectation, standards and formats are not communicated well, and this often creates much rework, further delaying approval and impacting program cost and schedule.
- The vast majority of our systems currently are accredited under the old structure and the RMF process does not allow previous accreditations to be easily absorbed into the new structure.
- There has been a shift in focus from simply managing risk to now ensuring all facets of system vulnerabilities are addressed. While this will improve cybersecurity, there is simply not enough manpower to adequately perform all of the required processes, specifically within the Approving Official and the Security Compliance Assessor communities.
- Approving Officials have not been issuing Plans of Actions and Milestones during this transition process, which has led to an expiration of Authority To Operate during the lengthy process.

In considering improvement opportunities since RMF has been in use and lessons learned have become available, I suggest

that the application of RMF to currently fielded cyber weapon systems be re-examined and tailored to reduce heavy RMF resource demands and impact to the operational user. In addition, as stated earlier, it is imperative that the acquisition and life-cycle management tools and processes for both new and fielded cyber weapons systems be streamlined to maximize speed and agility within reasonable levels cybersecurity risk.

Sustainment in DoDI 5000.02: I see a difference between a system in the sustainment phase and a sustainment program. Because DoDI 5000.2 is silent on sustainment programs, we sometimes treat sustainment programs the same as efforts to modernize a program in the sustainment phase, in terms of systems engineering, milestones and documentation. Modernizing a program in the sustainment phase usually fits pretty clearly into one of the "Defense Acquisition Program Models." But a sustainment program such as a Service Life Extension Program, Diminishing Manufacturing Sources Program or a Contractor Logistics Sustainment Program doesn't fit well within those models. Yet there are some nuances, best practices and common tailoring that could apply to these types of programs. I thought the "model" concept was a great addition to the DoDI 5000 series, so I think adding a model for sustainment type programs would be helpful. I have also recommended this at the military Service level to address in our documents. I see a lot of teams struggle in this area.

Tailoring: However, although you and other senior leaders continue to reinforce the importance of tailoring the acquisition process to the specific and unique characteristics of the product being acquired, the rules and policy are frequently interpreted as inflexible and prescriptive. As additional acquisition reform provisions are considered, we should look for ways to better institutionalize the expectation for tailoring, particularly as it applies to the acquisition of non-developmental or minimally modified COTS systems.

Workforce Development Ideas

Acquisition "Whiteboard" Sessions: I found that often when I received milestone packages through the staffing process, the acquisition strategies weren't tailored to the most effective approach to develop or acquire the system. In order to prevent frustration of the workforce and get the top level concepts right from the beginning, I began hosting "Whiteboard" sessions to ensure everyone had a common understanding of the strategy. I run these much like the military Service runs After Action Reviews by serving as a facilitator—asking shaping level questions of the program stakeholders (from the PM, legal, contracting, etc.) and allowing them to shape the strategy through their answers. The level of innovation and quality of the milestone packages has dramatically improved. I've received very positive feedback on the learning value of these sessions and encouraged my subordinates to replicate the process at lower levels.

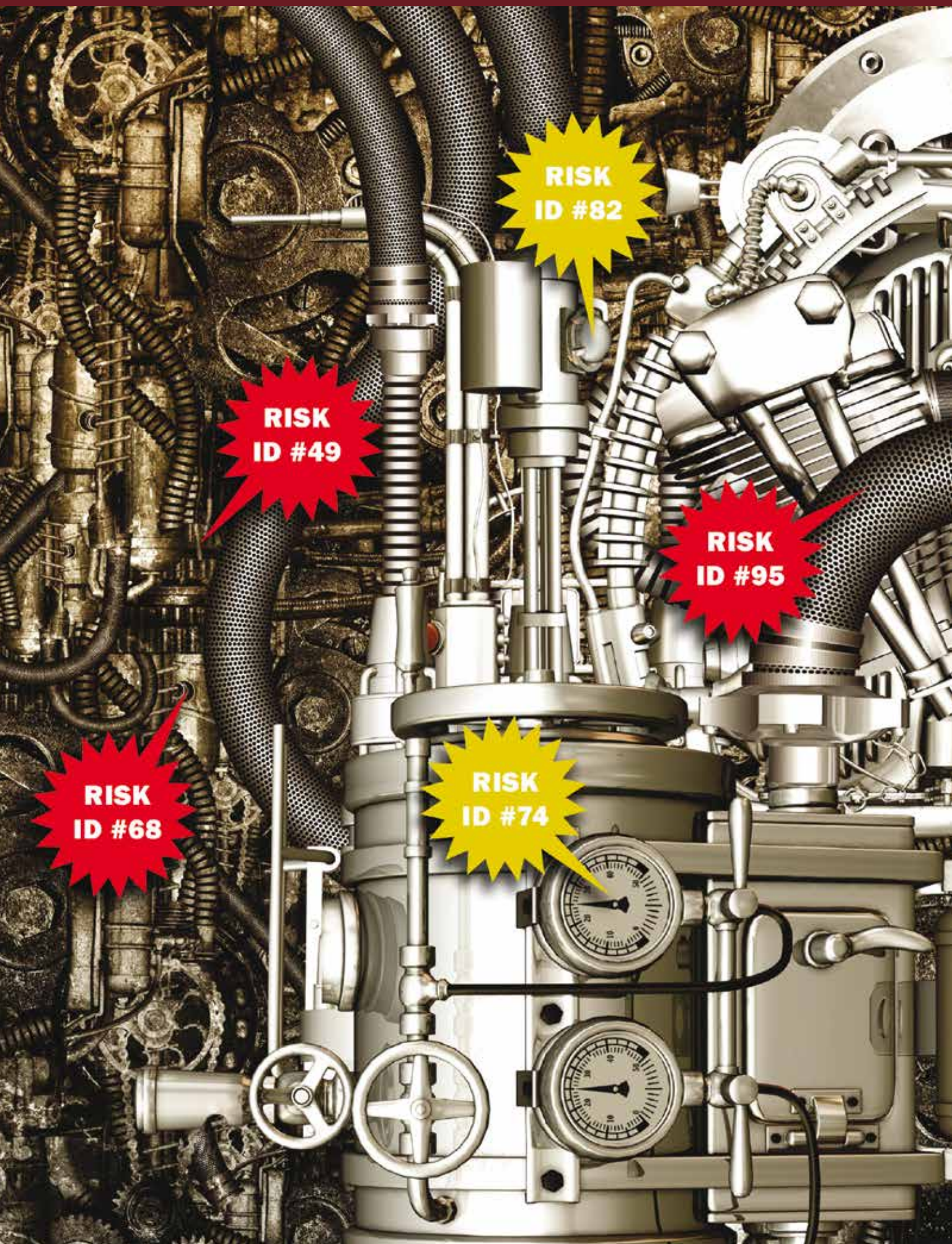
Acquisition Categories II and III Configuration Steering Boards (CSBs): Much of the equipment we acquire is commercial or commercially based. On several occasions, we received approved requirements documents that specified requirements substantially outside commercially available features. Our engineers conduct industry Requests for Information, coordinate with commercial testing facilities, and employ analytical tools to identify requirements that are driving cost and risk. We then organize a CSB with the appropriate one-star level operational community proponent, along with virtual representation from the Service staff to review the data analysis. In each case, we've been able to temper the requirements to only the critical capabilities, thereby reducing programs' costs and technical risks while allowing them to move forward without risking lost funding or schedule delays.

Junior Employee Shadowing Program: Each PM within the PEO nominates high potential GS-12/13 employees to shadow me for 2 weeks. These employees can attend all meetings that the PEO participates in and get a good sense of how to think critically about the unique facets of each program and how these considerations shape acquisition strategy, contract type, contract incentives, and source selection approaches. To date, I have had 24 shadow participants, and I have already seen evidence of grassroots movement inside their home organizations in taking more innovative approaches to acquisition strategies.

Topical Town Hall Meetings: I have held town hall meetings quarterly, and I always highlight a number of innovative accomplishments in acquisition from several of our individual PMs. As an overarching theme, I've suggested that our acquisition professionals should treat every decision they make as if it was their own money. I've continued to encourage them to challenge requirements and approaches that don't make sense based on their personal experiences both in acquisition and in their daily lives.

Conclusion

As with the Program Manager Assessments, I have responded to each of the PEOs individually. In addition, I have asked some of the writers to work on follow-up actions to explore solutions to the problems they raised, or to implement their specific suggestions. My last article and e-mail to the workforce talked about how real acquisition reform has to come from within and it has to take the form of continuous improvement on many fronts. This is one more example of what that looks like in practice.


RISK
ID #82
RISK
ID #49
RISK
ID #95
RISK
ID #74
RISK
ID #68

A Primer on Risks, Issues and Opportunities

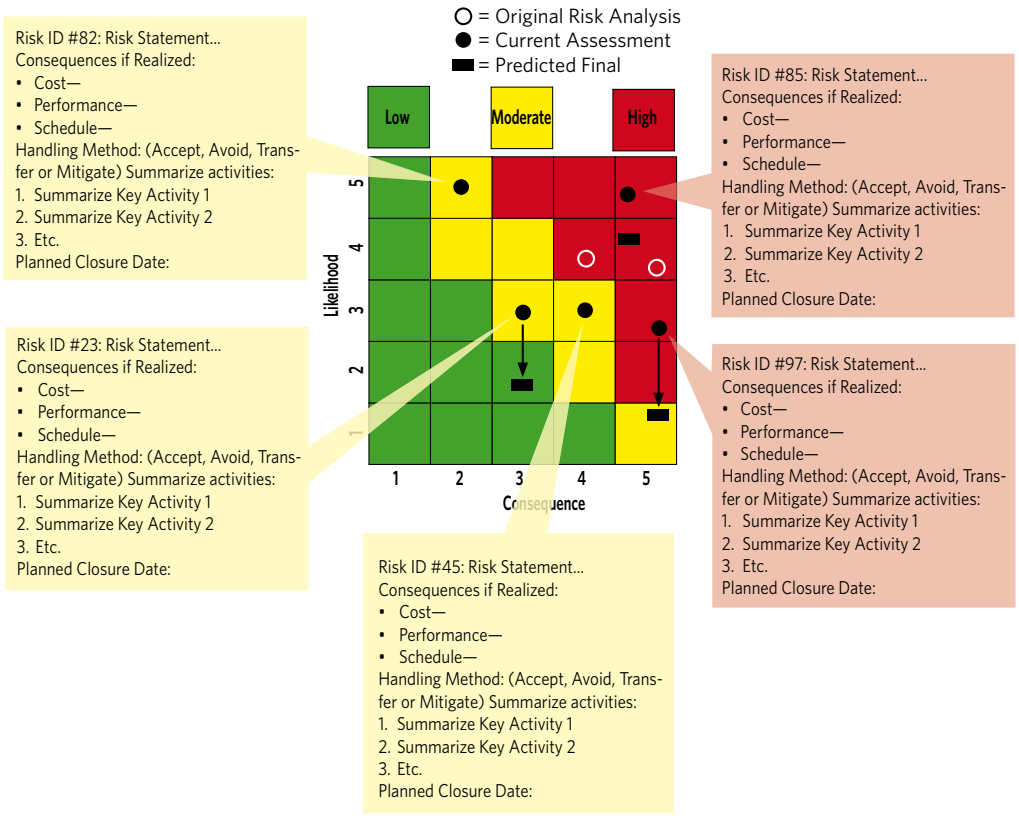
Thomas L. Conroy II, Ed.D.

Risks, issues and opportunities are programmatic hurdles for many acquisition personnel. For example, program offices deal with technical risks in the form of technologies that are not mature enough or are unable to provide the same capability in production that was achieved in development. They also deal with cost risks such as an insufficient budget or budgetary cost overruns and program efforts that take longer than scheduled due to requirements growth. The basics of risks, issues and opportunities will be tackled in this article. But, first, let's define them.

Risks are those future events that can negatively impact a program either through cost, schedule or performance. We manage risks by developing and implementing a sound, well-coordinated risk management plan and then track risks by plotting them on a 5-by-5 risk assessment matrix (see Figure 1). An important aspect of risk management is prioritizing risks to show where each additional dollar spent on mitigation would make the most sense and give the biggest return. These funds come from within the program budget and thus are extremely limited. We have several options in handling the risk in a program, and these include "buying down" risks with funds to purchase mitigation efforts that lower either likelihood or consequence. A risk has three main parts: a future root cause, a likelihood and a consequence. The future root cause is determined through root cause analysis, which is the most important part of any risk management effort.

Conroy *is a professor of Systems Engineering (Test and Evaluation) in the Capital and Northeast Region of the Defense Acquisition University at Fort Belvoir, Virginia. He holds a doctorate of education.*

Figure 1. Risk Reporting Matrix Format



Suggested Risk Reporting Format from *DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, June 2015.

Root cause analysis gets to the heart of the risk. Why does the risk exist? What is its nature? How will the risk occur? What should be done about it? All of these questions assist in identifying the root cause. Risk identification and analysis should be done early in the risk management process. In these steps, we determine what could go wrong, the likelihood of the problems, and how bad the consequences could be. The easiest way to determine the root cause of a risk is to break down the system being analyzed into lower-level components and then, based on what has happened before, ask what could go wrong with those components.

For example, let's say you are developing a previously nonexistent kind of unmanned ground vehicle (UGV). If you break it down into its components, you will find that you have a lot of background information for performing analysis based on the individual components and their histories. If the UGV has armor, you can analyze the armor type and material to determine what types of risks might be caused. If the UGV has a remote control, you can analyze the radio transmitter and receiver components and user input and control functions to determine the risks associated with those types of subsystems and components.

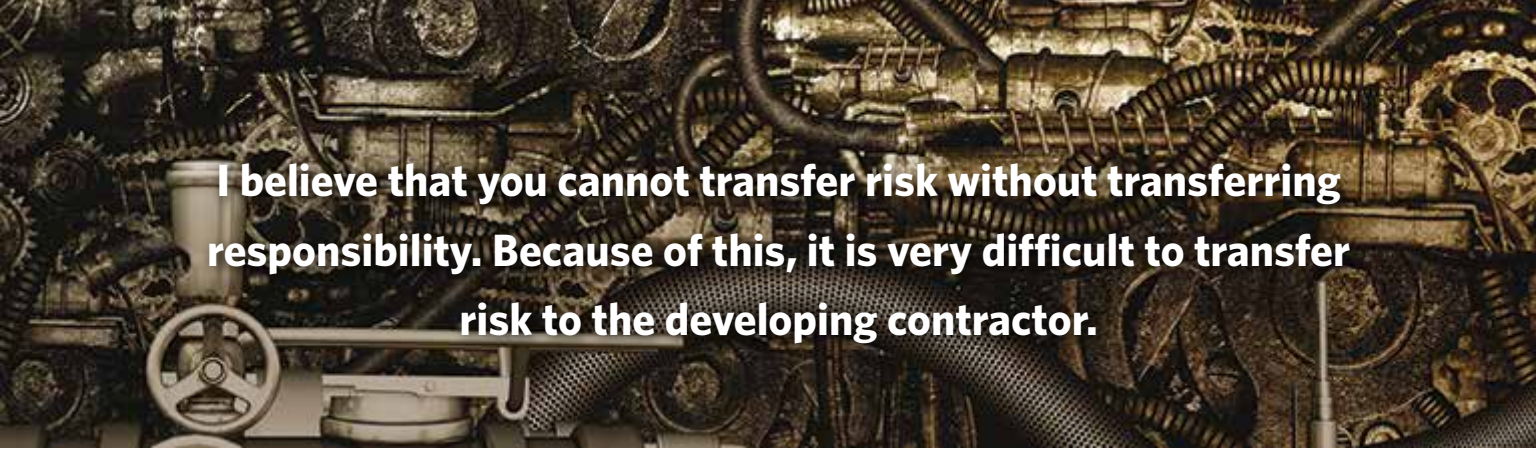
Root cause analysis is about predicting the future likelihood and consequences of a particular cause based on the data that exist about previous, similar cause-and-effect relationships. If there have been similar, earlier causes with similar consequences, we can use various statistical and cause-and-effect analyses to determine the likelihood of those causes recurring and producing a similar effect. This is why gathering data about the performance of a system and its components is so important throughout a system's life cycle.

Issues are simply risks that have a likelihood of 100 percent. They are no more or less important than risks. This is important because, once it is understood, you can treat risks and issues in similar fashion and prioritize them using the same criteria rather than arguing over whether a risk is an issue or vice versa. For example, you may have a risk that has a 50 percent likelihood based on past years in which your budget was cut by 15 percent. Based on the June 2015 *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, this would be a red, or high, risk with a likelihood rating of 3 and a consequence rating of 5. On the other hand, if you had an issue that meant your schedule definitely will slip by 2 weeks, this would be a green, or low, issue because it would rate a likelihood rating of 5 (for 100 percent likelihood) and a consequence rating of 1. Based on this situation's analysis, it would make more sense to spend time and money mitigating the budget risk instead of the schedule issue.

Handling Risks and Issues

There are four approaches to risks and issues. They are: avoid, assume, transfer and mitigate. Of these, the most common form is mitigation.

Avoiding a risk or issue involves avoiding the root cause of the risk or issue. For example, if using a certain type of fuel has toxicity risks, then redesigning the engine so that particular fuel type would not be used would avoid the root cause and thus the risk. This is most common when a risk has an extremely high consequence and/or high likelihood.



Assuming the risk or issue involves allowing the potential risk or issue to occur because most likely the consequence is low or acceptable. For example, it would make more sense to assume a risk of which the consequence was $1,000 and the mitigation would cost $50,000. It does not make sense to spend $50,000 to save $1,000.

Transferring the risk or issue involves shifting the consequence to another party or component by shifting the root cause to that party or component. For example, if you had a very high-risk requirement due to a low technical maturity of the components needed to achieve that requirement, you could shift the requirement to the next increment of development to allow time for the technology to mature. There are caveats about transferring risks and issues, in my opinion. I believe that you cannot transfer risk without transferring responsibility. Because of this, it is very difficult to transfer risk to the developing contractor. I believe you can share risk with the developing contractor through contract incentives and warranties. But without transferring the responsibility, you cannot fully transfer the risk.

Mitigation of risk or issue is the method I have seen most often used to handle risks and issues. For mitigation, we take funding from the program and use it to produce opportunities to counteract the root cause of the risk or issue. It is most important that the mitigation counters the root cause and not the symptom of the risk or issue. Otherwise you will be spending funds to plug one hole in a sieve. Mitigation is important to tackle throughout a program's life and requires being proactive with risk management early in the system life cycle. Mitigation can be used to "buy down" the risk to a lower level such as red to yellow and then possibly green. It is important to try to lower and not try to negate the risk with mitigation.

It also is important to ensure that your mitigation has time to succeed. For example, if you usually leave for work at 7:30 a.m. to arrive at work by 8 a.m., but your car often fails, you may use the bus to mitigate lack of a ride to work (as opposed to servicing your vehicle). If the bus that would get you to work by 8 a.m. leaves at 7:10 a.m., you would need to prepare to drive to work by 7 a.m. to allow enough time to catch the bus if your car fails—not prepare to leave at 7:30 as you would if the car were dependable. You need to plan and schedule for your mitigation strategy to allow it time to succeed.

Opportunities

Let's now discuss opportunities, which are the positive view of planning whereas risks and issues constitute the negative view. Opportunities are dealt with in a similar fashion to risks: We still use root cause analysis to plan for them. We look at opportunities for positive events to occur and the root causes of those future positive events and prioritize them on a 5-by-5 matrix focusing on likelihood and benefits (instead of consequences). The opportunity matrix allows for prioritization of opportunities so that they can also be handled for future potential benefits.

Opportunities are handled through three main ways: pursue, reject, and re-evaluate. These are the types of possible action for each opportunity. Pursuit of an opportunity means that you accept that the potential for a future benefit is likely enough to warrant spending funds to achieve it.

Rejecting an opportunity means that you have analyzed the return on investment potential for the future benefit and found that it does not warrant the expenditure. This could mean either that the return on investment or that the likelihood of success is too low. Either way, it would be a bad investment.

Re-evaluating an opportunity requires focusing on continually evaluating the potential for success over time. It means allowing more data to be gathered and allowing the likelihood for success to grow over time until the return on investment looks worthy of funding and success seems achievable.

Summary

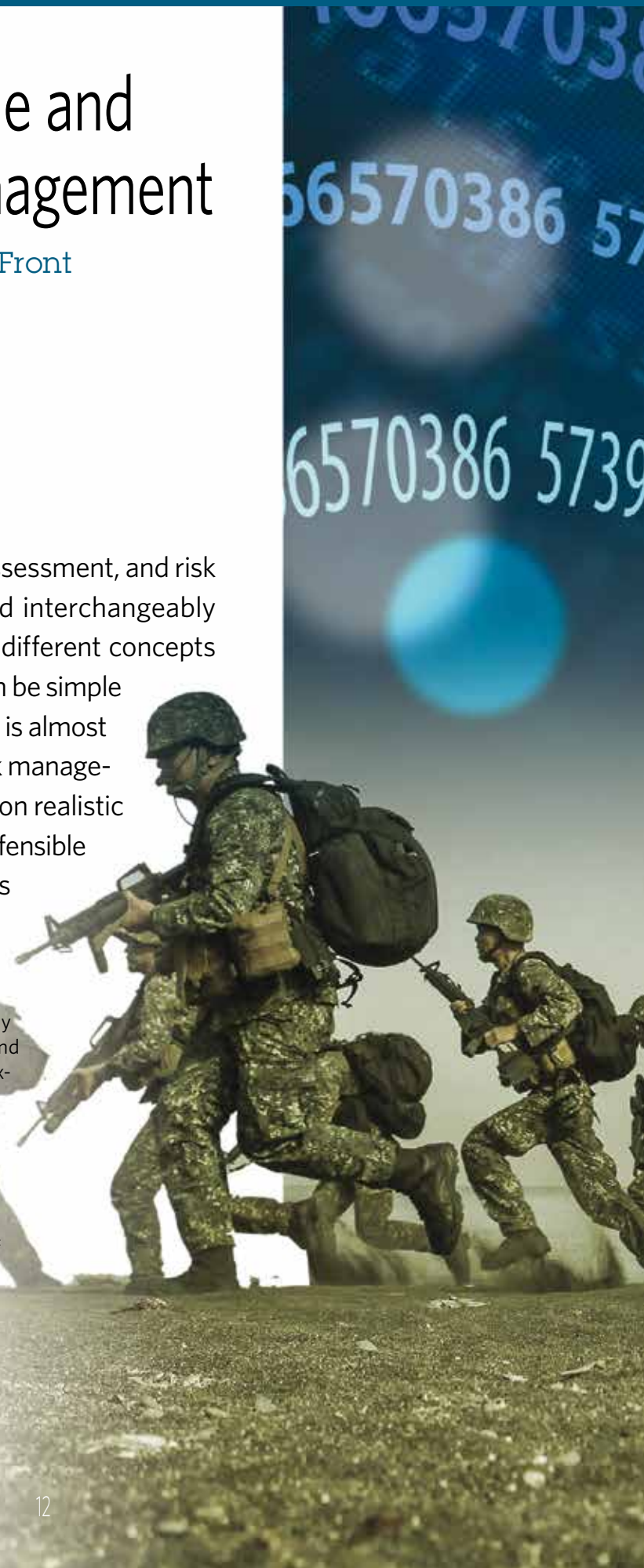
I think there are many exciting ways to deal with risks, issues and opportunities for programs today. The methods are sound when approached responsibly. It is up to every member of a program office to support the risk, issue and opportunity management processes and learn from the *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs,* as well as the best practices and lessons learned in other programs.

The author can be contacted at **tom.conroy@dau.mil**.

Robust, Replicable and Defensible Risk Management

At Headquarters or the Front

Eugene A. Razzetti



Terms like risk analysis, risk assessment, and risk management often are used interchangeably and can include a variety of different concepts or strategies. Approaches can be simple or complex, although simpler is almost always better. Properly conducted risk management permits decision making based on realistic scenario assumptions and provides defensible justification, before limited resources are committed.

The risk management model described in the pages that follow is based on what I like to call "disciplined subjectivity." Risk planners can use it to subjectively identify and assess mission threats, criticalities and vulnerabilities—applying the best knowledge and experience available. The discipline comes when they assign consistent, replicable, numerical values to them in accordance with established criteria. (I do not recommend that planners do risk management either in their heads or by themselves.)

I have used this model with clients both in and out of the military for more than 10 years.

Razzetti, *a retired U.S. Navy captain, is a management consultant and military analyst. He is the author of five management books and has served on the advisory boards of two business schools.*


86 40003755 98309363
67 40003755 98309363
755 98309363
73967 40003755 98309363
967 40003755 98309363

Table 1. The Criteria

Level	Scale	Threat Criteria	Criticality Criteria	Vulnerability Criteria
Lowest	1, 2	Never occurred before—unlikely; minimally effective due to physical area/environment; not a significant source of disruption	Minimally disruptive to mission if used	Minimally vulnerable to attack, due to own tactics, equipment, physical surroundings
Low	3, 4	Has occurred before—possible; effective in physical area for short period; potential source of disruption	Disruptive to mission if used; minor mission degradation	Susceptible to attack, but history and physical surroundings make attack unlikely
Medium	5, 6	Occurs periodically and predictably; likely to encounter; disruptive when occurring	Mission degraded, but can continue if attacked; some casualties	Highly vulnerable to attack, due to own tactical limitations and physical surroundings
High	7, 8	Occurs often; enemy has expertise; utility in area against missions; expect to encounter; highly disruptive	Mission seriously degraded, but can continue marginally if attacked; significant casualties possible	Extremely vulnerable due to tactical and equipment limitations and physical surroundings
Highest	9, 10	High probability of use; enemy proficient in use; unlimited utility and effectiveness against most missions; catastrophic if used	Mission failure; much disruption likely	Imminent danger, due to nature of operations, plus equipment limitations

I. In General

Risk = Criticality × Vulnerability × Threat

A spreadsheet model consisting of a set of connected worksheets can be a priceless management tool for the program manager (PM), enabling him or her to identify major potential threats to the mission of the organization and prioritize them, by assigning a numerical value to each. The PM also could assess the criticality of each threat to the mission expressed as a numerical value, and the vulnerability of the mission or organization to the threats expressed as a numerical value.

Then (and unlike other risk models) this model also helps to predict the impact on risk of one or more external or environmental factors, and the change to the risk if a selected course of action (COA) is implemented. With this last step, risk assessment becomes risk management.

II. In the Headquarters

Creating Criteria

For risk assessments to be consistent and reports to be uniform among reporting subordinates, the model requires an established set of numerical values or "criteria." The criteria Table 1 uses numerical values from 1 to 10 and describes each in terms of threat, criticality and vulnerability (to a mission).

Step 1. Developing the Threat Assessment Matrix

PMs and staffs identify the threats, and then assign numbers based on their knowledge and experience. The spreadsheet automatically computes the total and the average threat. The model uses average threats in all the calculations. This is a simple way to quantify threats in a "multi-threat" scenario. You may have another way, but you must be consistent in whatever method you use. Some variations may prove misleading or self-defeating (such as assigning zeros). The shaded columns are computed and posted automatically by the software.

Table 2. Threat Assessment Matrix

Program Management	Terrorist Attack	Utility Loss	Hacker or Cyber Attack	Industrial Espionage	Strike	Contractor Default	Natural Disaster	Falsified Reporting	Total	Average
Concept Design	9	4	9	9	3	5	8	8	55	7
Systems Engineering	4	4	9	9	3	5	8	8	50	6
Reliability & Maintainability	9	9	9	5	3	5	8	8	56	7
Manufacturing & Logistics	9	4	9	5	6	5	8	8	54	7
Environmental Planning	9	4	6	5	6	5	8	8	51	7
Safety/Security Plan	6	4	6	5	3	5	8	8	45	6
Software Engineering Plan	4	4	6	5	3	5	8	8	43	5
Quality Engineering	4	4	7	5	3	5	8	8	44	6

Table 3. Computing Basic Risk, Environmental Adjustment and Adjusted Risk

(Criticality × Vulnerability × Threat)

Program Management	Criticality	Vulnerability	Threat	Risk	Environment Adjustment	Adj Risk (1)	Revised Vulnerability	Adj. Risk (2) (COA)
Concept Design	8	6	7	330	0.9	297	5	248
Systems Engineering	8	5	6	250	0.2	50	4	40
Reliability & Maintainability	8	5	7	280	0.4	112	3	67
Manufacturing & Logistics	8	4	7	216	0.5	108	2	54
Environmental Planning	5	5	6	159	0.3	48	2	19
Safety/Security Plan	7	6	6	236	0.7	155	4	110
Software Engineering Plan	4	7	5	151	0.9	135	4	77

Table 2 is a threat assessment matrix. This matrix (worksheet) is the basis for all subsequent computations. There is an abbreviated list of program management tasks on the vertical axis and identified potential threats along the horizontal axis. It remains only to assign subjective numerical values from the criteria table.

Step 2. Computing Basic or "Unadjusted" Risk

The next worksheet (see Table 3) automatically copies the computed average threat from Table 2 for each program management sub-category. Planners then compute unadjusted (i.e., basic) risk according to the formula:

Risk = Criticality × Vulnerability × Threat

Planners assign numerical values from the (same) criteria table for the criticality of the threat incident or adverse event (if it happened) to the specific mission task and the resultant vulnerability of the mission.

When planners update the spreadsheet model displayed in Table 3 they automatically revise its associated graph shown in Figure 1. The first bar in Figure 1 (automatically formed by the spreadsheet software) displays basic or "unadjusted" risk. This often is the final step in risk assessment, but it is only the beginning of risk management, as shown in the last four columns on the right-hand side of Table 3. The reader will need to refer to Table 3 periodically as the risk management picture develops.

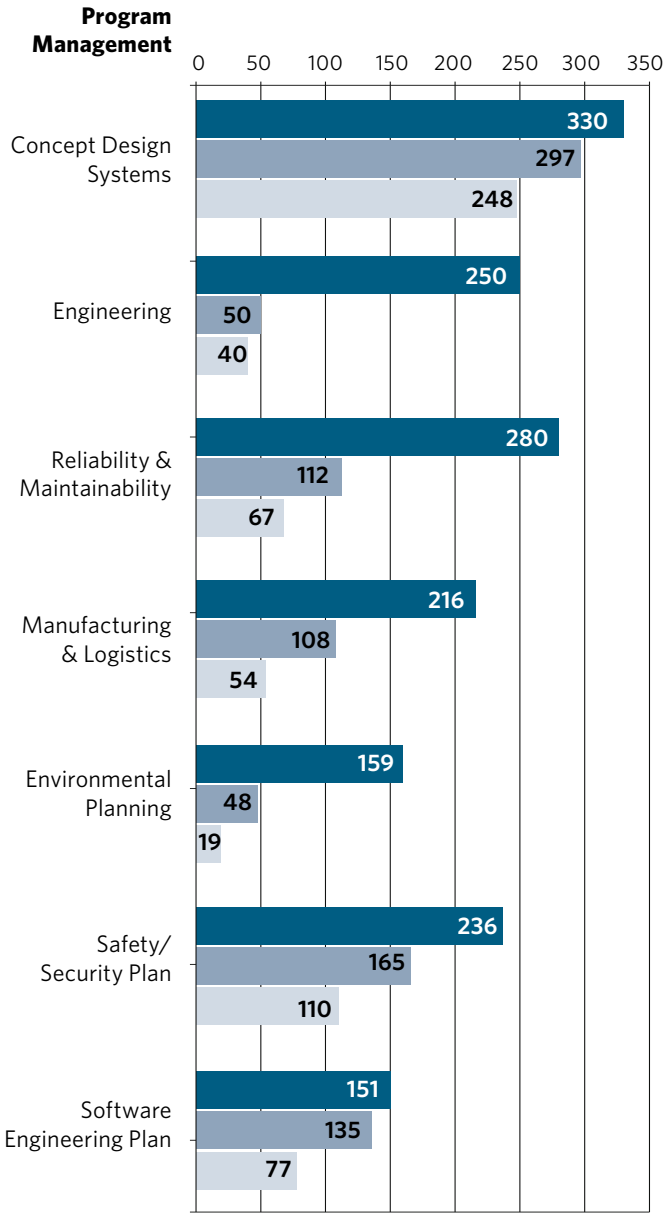
Step 3. Assessing Impact of the External Environment

Risk = Criticality × Vulnerability × Threat × Environmental Adjustment

The next step in the modeling process assesses the impact of external factors over which planners may have little or no control, such as host nation support of logistical operations in theater. In some cases, host nation support and/or involvement is invaluable, as in assigning interpreters or counterparts.

Figure 1. The Total Risk Management Picture for the Headquarters

(Composite Risk and Adjusted Risks From Table 3)



Risk assessment becomes risk management when the PM goes beyond what he has just completed, to identify and evaluate potential courses corrective COAs before expending any time or funding.

In other cases, (e.g., corrupt bureaucracies), U.S. Forces are often better left alone.

Planners wanting to separately reflect external variables on risk can add this step to assess (among other variables):

- Foreign country support (receipt, transportation, customs, etc.)
- Supply chain security
- Outsourcing (foreign or domestic)
- Special laws, regulations or protocols
- Anything else you want to separate from the internal processes but feel must be included in the overall risk assessment process.

For example, if the addition of a certain procedure or custom in the country where your operations are based cuts the risk in half, you multiply the risk figure by ".5." If the practice makes no appreciable difference, multiply the risk by "1" (no change). If a procedure makes it half again as difficult or risky, multiply by "1.5." Again, this will not corrupt or hinder your computations, as long as you apply it consistently. Planners not wishing to go through this step may either remove the "Environmental Adjustment column from the spreadsheet or leave it in and place the number "1" in each row.

Graphing Unadjusted and Adjusted Risk

Thus far, we have quantified (1) the unadjusted risk and (2) the impact of the environmental factors, providing a more realistic assessment of the actual risk. The second bar in Figure 1 displays the change (for better or worse) brought about by external factors.

Step 4. Identifying and Assessing Potential Actions

Reduce Risk by Reducing Vulnerability. Identifying threats, criticalities and vulnerabilities in accordance with a standard set of numerical values to provide a "snapshot" of operations normally is the extent of risk assessment as currently practiced.

However, risk assessment becomes risk management when the PM goes beyond what he has just completed, to identify and evaluate potential corrective COAs before expending any time or funding.

Identifying potential COAs and modeling them in the spreadsheet can show one of the following:

- Measurable potential reductions of risk in one or more mission areas if implemented (good)
- Small or insignificant potential changes of risk if implemented (neither good nor bad; not worth the time or expense)
- A measurable increase in risk to another part of the mission if implemented (bad)

Implementing a new course of action for an existing mission, operation or project does not change the threat to the mission. Neither does it change the criticality of the mission. It does (or should), however, measurably reduce the vulnerability of the mission. For example, posting extra security personnel or adding alarm systems can decrease an organization's vulnerability to a break-in. The alarm systems have not decreased the threat of a break-in, or the criticality of a break-in—only the vulnerability.

Accordingly, you reduce risk by reducing vulnerability. Recognizing this fact and using it to predict changes in risk is an indispensable to program management in general and risk management in particular.

The following formula computes the impact of the COA on the risk computed earlier:

Risk = Threat × Criticality × Revised Vulnerability × Environmental Adjustment

The third bar in Figure 3 displays the application of the revised vulnerability and, accordingly, the revised risk resulting from implementing a (notional) course of action. The graph displays at a glance:

- The unadjusted (basic) risk assessment
- The impact of the external environment
- The impact of a notional course of action, which is the result of revising the numerical value for vulnerability.

We have not only a realistic snapshot of the present, but our best possible prediction (albeit subjective) of the future, if we were to implement specific courses of action.

Revisions that reflect changing situations and the immediate feedback provided by the graphs make the model a dynamic management tool for evaluation, prioritization

Table 4. Threat Matrix Closer to the Front

Program Management	Terrorist Attack	Utility Loss	Hacker/ Cyber Attack	Industrial Espionage	Strike	Contractor Default	Natural Disaster	Falsified Reporting	Total	Average
Security/Surveillance										
Detecting/Identifying unauthorized movement-personnel	9	4	9	9	3	5	8	8	55	7
Detecting/Identifying unauthorized movement-vehicles	9	4	9	9	3	5	8	8	55	7
Surveillance of restricted areas	4	4	9	9	3	5	8	8	50	6
Securing Incident Sites	9	9	9	5	3	5	8	8	56	7
Detection of unauthorized material	9	4	6	5	6	5	8	8	54	7
Surveillance of access points	9	4	6	5	6	5	8	8	51	6
Harbor Surveillance	6	4	6	5	3	5	8	8	45	6
Automatic Security Systems	4	4	6	5	3	5	8	8	43	5

and presentation, as well as a timely, stand-alone report to higher authority.

It is not unusual to discover that modeling potential courses of action (i.e., "gaming" them) predicts only small or insignificant changes. Modeling can show PMs in advance that certain courses of action simply may not be worth expending limited resources.

III. Risk Management at the Front

This includes identifying (as appropriate):

- Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action
- Operational threats and risks, including the control of security, human factors and other activities that affect the organization's performance, condition or safety
- Environmental or cultural aspects that may either enhance or impair operations
- Factors outside of the commander's control, such as failures in externally supplied (e.g., host nation) equipment and services
- Contractor and host nation challenges, such as local regulatory requirements
- Facilities and equipment, including information, data and communications management systems
- Any other threats to the continuity of operations

Commanders and planners closer to the front can use the model and approach to assess actual operations.

Table 4 contains a threat matrix for a key mission set of a (notional) deployed unit: "Security/Surveillance." A corresponding risk table and graph are not shown, due to space constraints.

Summary

Properly conducted risk assessments based on lifelike scenario assumptions lead PMs to either justify or preclude commitments of time and funding in making their decisions.

There are many approaches to meaningful risk management. This model provides risk planners with a simple but comprehensive management tool for identifying mission threats, criticalities and vulnerabilities. It can help identify and assess potentially mitigating courses of action.

Regardless of where the assessment leads, completing this model will provide a rigorous and structured process to help PMs and commanders arrive at logical and defensible conclusions.

The author can be contacted at **generazz@aol.com**.

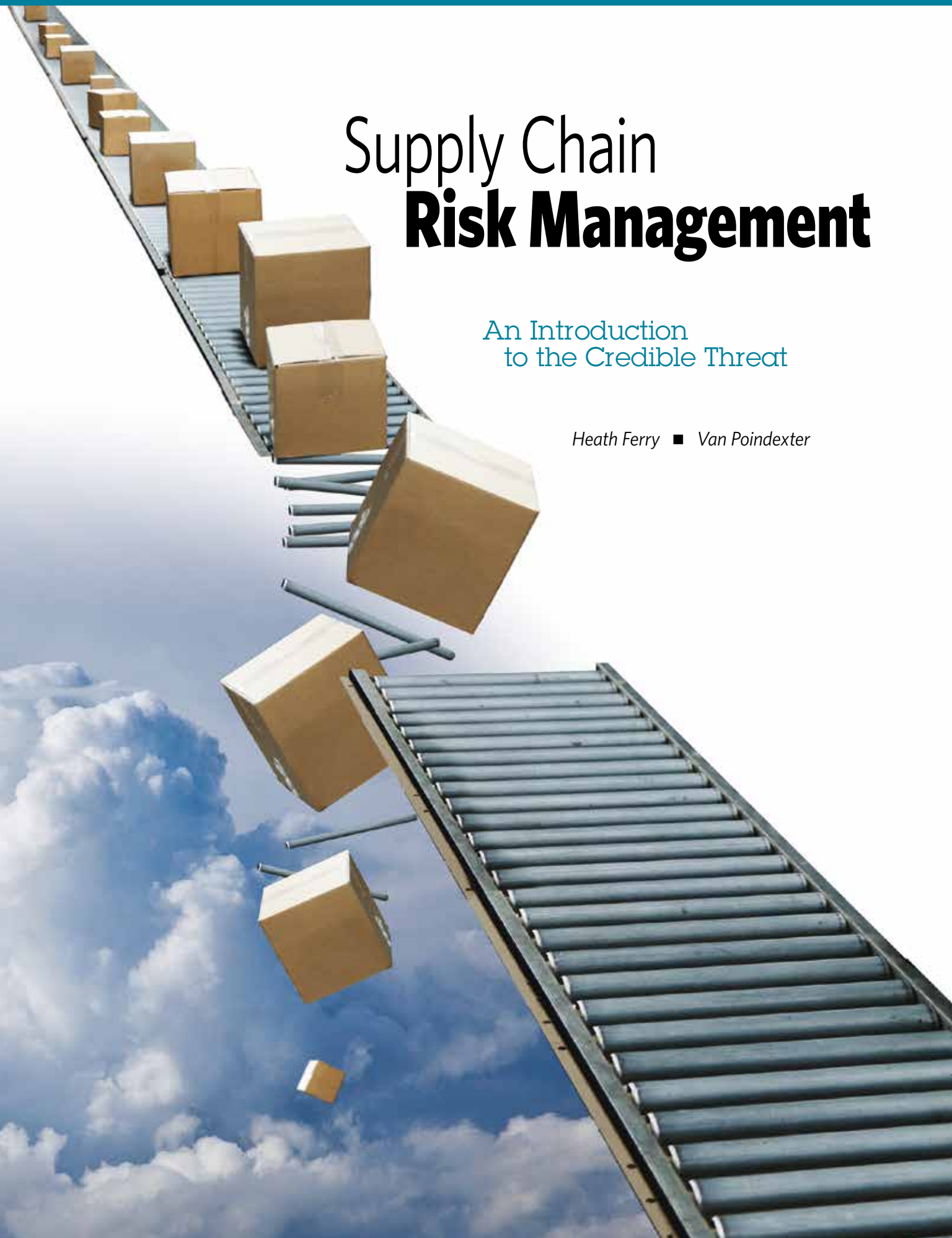
MDAP/MAIS Program Manager Changes

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 March and April 2016.

Navy/Marine Corps

CAPT Todd St. Laurent relieved **CAPT Leon R. Bacon** as Program Manager for the T-6B Joint Primary Aircraft Training System (JPATS) program (PMA 273) on March 4.

Patrick Fitzgerald relieved **Laura Knight** as program manager for the Sea Warrior program (PMW 240) on April 1.



Supply Chain **Risk Management**

An Introduction to the Credible Threat

Heath Ferry ■ *Van Poindexter*

We live in a wonderful world of instant information, and everything is connected. All we have to do is pull out our phones, tablets, laptops or any other similar device and get the information we need virtually instantaneously.

While all this advanced communications technology constitutes one of the greatest things about living in a technologically advanced world, it also exposes us to one of the biggest threats. How can we be sure that any and all of these devices were made to strict manufacturing standards and weren't designed with the flaws built in or downloaded? Some of the same tools that make our lives easier also could leave us wide open to a cybersecurity breach. This article examines the elements of supply chain risk management, the national security risks associated with exploitation, and the concerns for the Department of Defense (DoD).

According to the November 2012 DoD Instruction (DoDI) 5200.44, Supply Chain Risk Management (SCRM) is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the product and its subcomponents or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation and disposal).

So what does all of this mean to the government and the overall acquisition life cycle? SCRM is a credible inside threat every bit as much as a malicious insider, counterfeiters, terrorists or industrial espionage agents. Is SCRM just a cyber issue? An intelligence issue? An acquisition issue? Honestly, it is all the same and should be treated as such. A concerted effort should be made, across all levels and domains, to address it at every step of the acquisition life cycle.

The DoD, military, business and intelligence operations—including communications and command and control—rely heavily on trusted networked systems, devices and platforms. All of these components support the ever-increasing number of capabilities that support the DoD's missions. Every component is designed, manufactured, packaged and delivered to end users, and global supply chains provide multiple attack vectors that increase a program's cybersecurity risk. The supply chain is a globally distributed and interconnected web of people, processes, technology, information and resources that creates and delivers a product or service. Global supply chains are dynamic, multilayered and complex. Lack of visibility and traceability through all of the diverse layers of the supply chain create security challenges because each component has its own supply chain that provides multiple opportunities for an adversary to sabotage the raw materials, manufacturing processes, packaging and even shipping. All of these can collect information on DoD systems and lead to either industrial or traditional espionage.

Ferry *is one of the newest cybersecurity professors at the Defense Acquisition University (DAU) South Region in Huntsville, Alabama. He currently provides Mission Assistance, curriculum development, and support to all segments of the Defense Acquisition Workforce. He holds a master's degree in cybersecurity and has multiple cybersecurity certifications.* **Poindexter** *is a professor at DAU South Region. He currently is involved in enhancing the awareness and proactive involvement of support managers and logisticians in identifying and mitigating risks in the Department of Defense supply chain. He is working on his doctorate in education.*

Figure 1. The Four Aspects of Supply Chain Risk Management

- **Security** provides the confidentiality, integrity and availability of information.
- **Integrity** focuses on ensuring that the products or services in the supply chain are genuine and contain no unwanted functionality.
- **Resilience** focuses on ensuring that the supply chain provides required products and services under stress.
- **Quality** focuses on reducing unintentional vulnerabilities that may provide opportunities for exploitation.

Source: National Institute of Standards and Technology (NIST) Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015, Page 4.

Supply chain risk, by definition, is any risk that an adversary may use in order to sabotage, exfiltrate information, maliciously introduce unwanted function or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a system so as to surveil, deny, disrupt or otherwise degrade the function, use, or operation of that system. Other risks include the insertion of counterfeits, unauthorized production, tampering, insertion of malicious software, loss of confidential government information, and poor manufacturing and development practices in the supply chain. Counterfeit components have the potential to degrade performance, but they often are introduced into the supply chain for financial rather than malicious purposes. Counterfeits can contain intentional modifications for the purpose of sabotage or exfiltration of information. SCRM focuses more on identifying the potential impacts of threats from malicious actors, rather than counterfeits. Supply chain weaknesses and vulnerabilities offer adversaries attack vectors for cyber exploitation and manipulation.

The Need to Manage the Supply Chain

Everything is interconnected today, and one component in a system or network can have an impact on one system or on multiple systems at the same time. Therefore, risk must be considered for each component before it is purchased or integrated into a system. The more critical the mission, the system and the component, the more diligent we must be in managing risk. Risk management decisions require that the decision maker consider three factors (cost, schedule and performance) and consider the impact of his or her decision about the desired or needed level of performance (in this case, cybersecurity) in the context of the impact of performance criteria on cost and schedule.

A May 2012, Senate Armed Services Committee inquiry report stated that China was found to be the dominant source country for counterfeit electronic parts, a major vulnerability in the supply chain. The Chinese government has failed to take steps to stop counterfeiting operations, which means DoD must step up its efforts to manage and mitigate the counterfeit threat. Unfortunately, DoD lacks knowledge of the sheer scope and impact of counterfeit parts on critical defense systems. This lack of knowledge can compromise performance, reliability of defense systems and can even risk the safety of military personnel. The defense industry's reliance on unvetted independent distributors and the weaknesses in their testing regime for electronic parts creates unacceptable risks and vulnerabilities. The defense industry routinely failed to report cases of suspect counterfeit parts. This has to stop.

SCRM traditionally refers to managing risks in the manufacturing and delivery supply chains. Globalization requires that SCRM include the process of identifying critical components and functions; identifying supply chain threats, vulnerabilities, and risks; determining likelihood (susceptibility) and the impact of those risks; and developing strategies in response. All of these supply chain exploitation risks should be assessed at each stage of the life cycle.

How to Manage It

One solution might be to buy only U.S.-made products, but this usually is difficult and could carry a higher cost, with the exception of certain very critical components. Trusted Suppliers (including Trusted Foundries) have been accredited by the Defense Microelectronics Activity to provide secure design, manufacturing, packaging and testing services. These suppliers also provide foundry capability, prototyping, testing and packaging services. Producing chips or other microelectronics through a Trusted Supplier can be more expensive than purchasing chips from commercial sources.

The Trusted Foundry program was started in 2004 to ensure that mission-critical national defense systems had access to microelectronics from secure, domestic sources. This program identifies Trusted Foundries for contract semiconductor manufacturing at features sizes down to 22 nanometers. Although most SCRM focuses on the tactical end—protecting

There is growing concern that counterfeit parts—generally the misrepresentation of a part's identity or pedigree—can seriously disrupt the DoD supply chain, harm weapon systems integrity, and endanger troops' lives. Additionally, with many manufacturing steps being performed offshore, sophisticated adversaries have the opportunity to inject vulnerabilities that introduce kill switches, back doors or Trojan viruses to render systems ineffective upon command or to leak sensitive information.

Source: "Trusted State-of-the-Art Microelectronics Strategy Study," July 2015, Potomac Institute for Policy Studies report.

components from sabotage or espionage—the trusted process is a response to a strategic SCRM issue: that companies are increasingly moving their semiconductor fabrication facilities overseas. As with the other Trusted Suppliers, purchasing components from entities with accredited trusted processes can be more expensive than purchasing them from commercial suppliers, which limits the use of this option for reducing risk. Even when components are purchased from trusted sources, continuous configuration control and parts management remains necessary.

Component Testing

Testing can provide an effective method to help detect counterfeit parts and identify unintentional design flaws rather than find that potential malicious alterations, particularly latent functionality that could be triggered well after a component or software code is already installed in a system. Normal test protocols operate under the assumption that the test process will expose all of a component's possible behaviors. Testing can help verify whether a component works according to the design specifications, but testing has its limitations. Malicious functionality can remain hidden or dormant during normal testing and is difficult to discover. Investigating the supply chain of each critical component begins with determining its source and possible attack vectors along the supply chain.

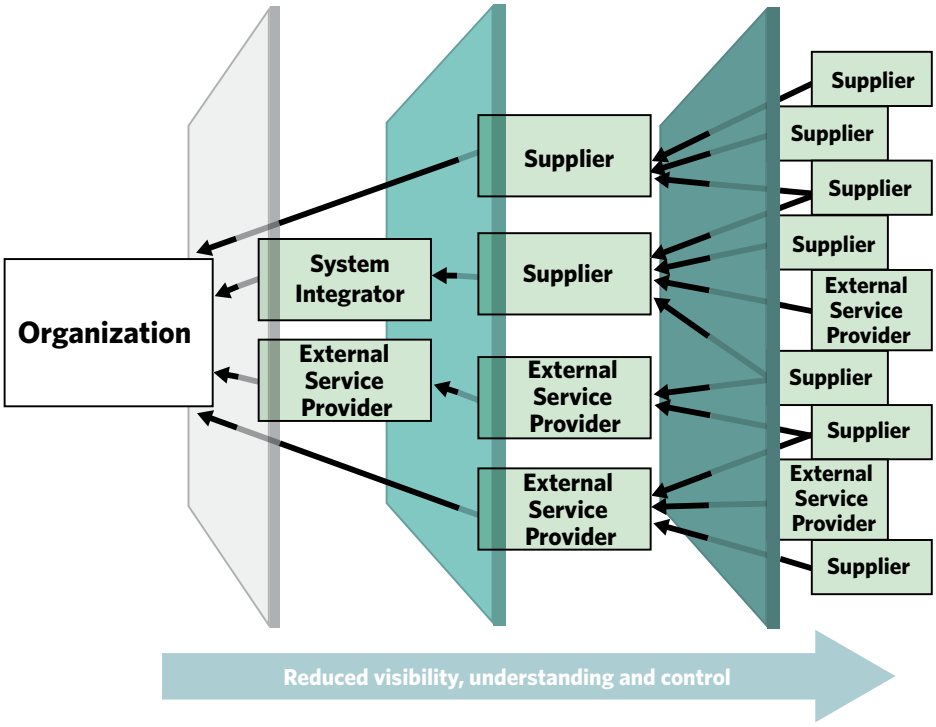
Responses to Risk

It is impossible to eliminate all risks associated with the supply chain, especially when it comes to the use of electronics, computers and other computerized components. The attempt to remove or mitigate risks can be extremely expensive and time consuming. Applying countermeasures and mitigations will lessen the consequence of a compromised component or system by incorporating risk management strategies throughout a component's or system's life cycle. There are four basic ways to address identified risk:

- **Treat it**: Employ protective measures (countermeasures and mitigations) that may either reduce the consequence or likelihood of a threat exploiting or triggering a vulnerability, or remove the threat or vulnerability that generates the risk.
- **Transfer it**: Allocate some or all of the responsibility for risk mitigation to another organization and/or phase of life cycle by passing the risk along.
- **Tolerate it**: Make a conscious decision to continue with the activity (or acquisition) despite the identified risk.
- **Terminate it**: Eliminate the likelihood of a threat, susceptibility to a vulnerability or impact of exploitation by not continuing with the activity or acquisition.

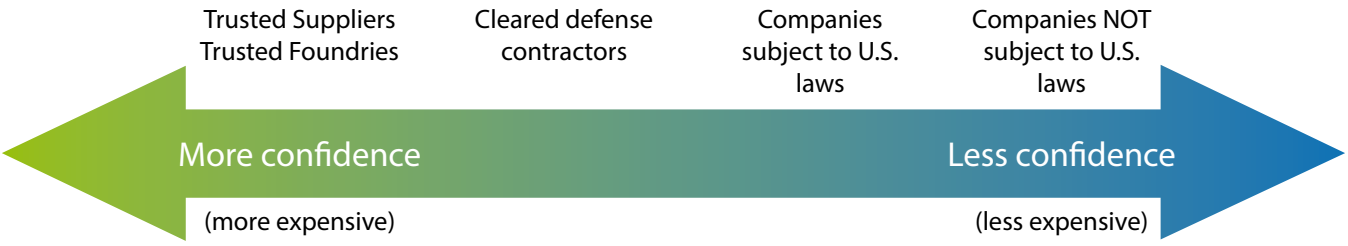
The options to consider in response to identified risks associated with a component range from doing nothing (usually not

Figure 2. An Organization's Visibility, Understanding and Control of Its Information Technology Supply Chain



Source: N*IST Special Publication 800-161, SCRM,* April 2015, Page 8.

Figure 3. Trusted Suppliers



Source: "Managing Information Communications Technology Global Supply Chain Risk Awareness Module 2014," Institute for Defense Analyses (IDA), Page 33.

an option) to redesigning a system to avoid using a component that does not have acceptable risk mitigation options. Risk mitigation requires significant effort and could have a significant effect on cost and schedule.

Choosing an option that requires less effort will save upfront costs but often will result in greater costs later in the system's life cycle. Vulnerabilities identified early in a system's design often can be significantly lessened or eliminated with simple design changes or procurement constraints at relatively low cost. It is much less expensive to design in cybersecurity from the very inception of the project rather than to implement cybersecurity fixes throughout a system's life cycle.

Conclusion

Supply chain risk management is not a simple one-time, one-solution scenario. All of those in the acquisition field need to understand the need and implications of poor practices that can easily lead to cost overruns and, even worse, a security incident where DoD information is stolen. The acquisition workforce needs to institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions, address cybersecurity in relevant and meaningful training, include a requirement to purchase from original equipment manufacturers, their authorized resellers or other trusted sources whenever available and increase government accountability for cyber risk management. The Defense Acquisition University is working closely with Supply Chain Risk experts from the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) Cyber Campus to present the most up-to-date information and integrate it into the curriculum. Later articles will discuss further the threats, vulnerabilities and policy associated with the supply chain and the DoD path forward.

The authors can be reached at **heath.ferry@dau.mil** *and at* **van.poindexter@dau.mil**.

Intellectual Innovation

A Paradigm Shift in Workforce Development

Michael Cook

Every organization struggles with recruiting and retaining the quality personnel needed to meet the ever-evolving requirements of the mission. Today's workforce complexity adds a unique challenge. As every manager and supervisor knows, the required work becomes more challenging over time, not less so.

Technology and innovation drive the challenge, forcing organizations to recruit and retain employees who can respond to the organizations' missions or operational requirements.

Here lies the challenge. How can organizations find, develop and keep employees in this dynamic and complex environment that constantly forces those who operate within it to question how to achieve continuous improvements? Perhaps a paradigm shift is needed in how we do this.

Cook *works at the 412th Range Squadron at Edwards Air Force Base in California. He is Project Management Professional certified and has a master's degree from the University of Management and Technology.*

The Challenge

Innovation drives everything we do. In developing and delivering complex weapons systems to the warfighter or logistically maintaining the systems or training personnel to operate them safely and effectively, innovation is never far from the overarching acquisition process. The paradigm has been to enable technology to meet the innovative challenge of developing the workforce. Faster computers, interactive simulation software, Web-based training sites and Web-enabling technologies are just a few ways in which technology has been the focus of innovative training, education and professional development.

At times, technology can become a crutch that prevents an organization from seeking better ways to deliver the training and provide the professional development opportunities that employees need in order to excel.

Although it is readily presented as important in workforce development, technology all too often has become synonymous with innovation in the minds of managers and supervisors trying to develop their respective employees so they can meet their unique workforce requirements. But employing existing technology or seeking to employ emerging technologies actually may not provide the innovation needed to meet current challenges. Although technological advances have provided huge benefits to a number of different fields over the years, technology is neither the only answer nor the only way to innovate. At times, technology can become a crutch that prevents an organization from seeking better ways to deliver the training and provide the professional development opportunities that employees need in order to excel.

Innovation evolves from necessity and successful utilization of available resources. In other words, take what is available and find new and improved ways to employ it. Technology often has been the resource readily at hand and has shaped the paradigm many now operate within. In the case of many training and educational methods used to develop the workforce, the paradigm can and should shift. We should focus on the resources at hand and develop training and development initiatives that incorporate a holistic approach to developing the workforce.

Technology need not and should not be totally disregarded. However, to succeed in austere times in which many research and development budgets are shrinking, we must all take a new and different look at the assumptions and standard ways of doing things. The challenge is for managers and supervisors to realize this in order to change the paradigm. The benefit may be a better and cheaper method of developing the workforce and meeting operational requirements.

The First Step

Among the most commonly overlooked resources of organizations are their current employees. Every organization has abundant experience, education, knowledge, skills and abilities that remain dormant because they never are utilized. However, these resources often are not captured by management, and therefore their existence remains unknown. These intellectual resources in essence are wasted.

The first step in shifting the personnel development paradigm is to capture and understand the abilities of current employees and try to share them across the organization. This is done easily through resumé and records reviews as well as personal interviews with employees. Documenting the intangible resources of knowledge and experience is an important first step. Supervisors and managers identify educational programs completed, years in the current career field, specific training received, unique assignments and a number of other important facts that become organizational resources that can be used.

There are two indirect but crucial benefits of this first step. First, it allows the employees an opportunity to discuss their contributions to the team and opens dialog on how to improve the organization. Many employees truly want to perform well, help those around them and improve the organization in order to achieve success. Employees also want to know that managers and supervisors value and respect their contributions, and open collaboration between managers and employees makes that awareness possible.

Any organization may allocate funds for employee training. Sometimes this is necessary, such as for certifications or the successful completion of exams. However, it often is not necessary. The organization could save time and money by employing the one-time common practice of on-the-job training (OJT). An OJT program matches new employees up with experienced employees to share the experience, education, knowledge, skills and abilities. This offers a win-win opportunity. The new employee benefits from gaining knowledge and insight from the experienced employee. The experienced employee gains the satisfaction of sharing his or her

knowledge and insight in order to improve the organization. An OJT program also provides team-building opportunities, creates camaraderie and develops a sense of ownership on the part of experienced employees.

The second indirect benefit is the development and sharing of ideas on how to improve employee training. Not only do experienced employees have a wealth of knowledge and experience, but they also have an abundance of ideas. In many cases, employees are likelier to remain in an organization that values their input. On the central focus of innovation, they may have previously undiscussed ideas on how to better train the workforce. Perhaps it is an idea on areas of training that could be eliminated, or perhaps the need to alter the sequence of training in order to improve understanding. We must come to realize that innovation need not consist of groundbreaking discoveries. Sometimes simple changes produce huge benefits and change how we think about things.

Determine Knowledge and Experience Gaps

Once supervisors have performed the background due diligence for organization members, the next step is to identify employee gaps in knowledge and experience. Typically, organizations ignore the training or knowledge shortfalls of the more experienced employees. This is a mistake. Although experienced employees need less training than new employees, eliminating training often results in occupational apathy.

Experienced employees may feel that, since they receive no training opportunities, they have reached the limit of their professional development. This is not conducive to the development of innovative ideas for improving the organization. It also may impede knowledge-sharing for newer employees if the more experienced employees have no incentive to train others who may compete with them for future career advancement or opportunities. Both scenarios are potentially damaging, not only to the organizational growth and development but potentially to effective job performance.

Once the gaps in knowledge and experience have been identified for all employees, a strategy can be developed that benefits everyone. Two key components to the strategy for innovatively developing a well-trained workforce are mentorship and tailored training programs. Each component can play a unique and vital role in applying innovative strategies and not just technological strategies.

Develop a Mentorship Program

As with any program or initiative, it is only as good as the buy-in from the organization and should be supported from the top down. Leadership-supported mentorship programs can play a critical role in the knowledge transfer between experienced and new employees. Mentorship programs help indoctrinate new employees, transfer knowledge, create a more adhesive workforce and encourage the sharing of ideas across all levels of an organization.

Mentors interact and communicate with new employees, and vice versa. Mentors also share their thoughts with management on the progress and capabilities of new employees. Mentors discuss mentorship techniques and challenges with peers and share ideas on how to be better mentors. Good mentors also take ownership of the process and prove to be exceptional stewards for the organization; they make the extra effort to improve the organization and freely share ideas on how to do so.

This open communication across the entire organization and the contributions of mentors creates and fosters idea-sharing and the possibility for innovative ideas to take root. For many organizations, the best benefit is that this results in no cost to the organization's budget and may actually save money in the long run. The benefits associated with cost-avoidance and cost savings have a pivotal role in today's operational environment.

Developing Tailored Training Plans

The problem with most training plans is that the approach taken all too often is to develop a one-size fits all plan. The cookie-cutter approach leads itself to fast creation of a plan—however, not a very good plan. Supervisors need a paradigm shift away from the generic and toward the tailored training plan that takes into account the individual employee and includes assignment of a mentor to the new employees. In many organizations, this can be seen as an innovative approach.

Every employee comes with unique education, knowledge, experience and abilities. Instead of trying to train everyone according to a prepackaged set of training courses or objectives, organizations should develop a tailored plan that focuses on what each employee needs to learn. Time and effort are saved by focusing on the knowledge and skill gaps instead of a list of courses or objectives, some of which may not be needed if the employee already developed has the skillset associated with the training.

Although experienced employees need less training than new employees, eliminating training often results in occupational apathy.

Another key aspect of the tailored training plan is the realization that each employee learns in a different way, which can include the use of visual and/or audible as well as the hands-on method of instruction. Employees also have varying learning abilities and disabilities, and require varying lengths of time to learn and

retain new things. There is an associated completion date in an overwhelming percentage of training plans. It is important to understand that not every employee can retain the knowledge and gain the experience and proficiency to compete a training plan within a month, or 6 months or even a year.

Tailored training must emphasize collaboration between the supervisor and the employee in developing a plan and a timeline that the employee can complete. The plan should look at the holistic approach. Some employees may need significant formal classroom training. Others may find OJT or online courses better suited to them, or possibly a combination OJT, online and classroom learning. The key is for the plan to be tailored to the individual and not to the job being performed.

Mentors play a critical role in helping the new employees achieve their training objectives. In many cases, the mentor has been in the shoes of the new employee and understands how to gain the knowledge and training to do the job. To assist the employees, mentors bring many tools to the table—including lessons learned, information on degree and certification programs, and pitfalls to avoid during a career.

Conclusion

Although this article is centered on innovation, nothing here is groundbreaking. Many of these concepts and practices have been around for generations. However, the author does feel that seeking ways to solve the workforce development through nontechnological methods can lead to innovative breakthroughs. Every supervisor and manager must make it a priority to recruit the best employees possible, develop every employee the best way possible, value the contributions they make and challenge them so that they want to stay within the organization.

Before we look to new technology to solve our workforce development issues, let's look at the intellectual resources already available within the organization. The rewards and benefits of employee development and retention are enormous. In today's technological environment, any avenue that leads to attainment of these goals is truly innovative, whether technology is used or not.

The author can be reached at **cookm49@hotmail.com**.

Defense ARJ and AT&L have become online-only publications for Individual Subscribers

If you would like to start or continue a subscription for Defense ARJ or AT&L, you must register a valid e-mail address in our LISTSERV.

NEW

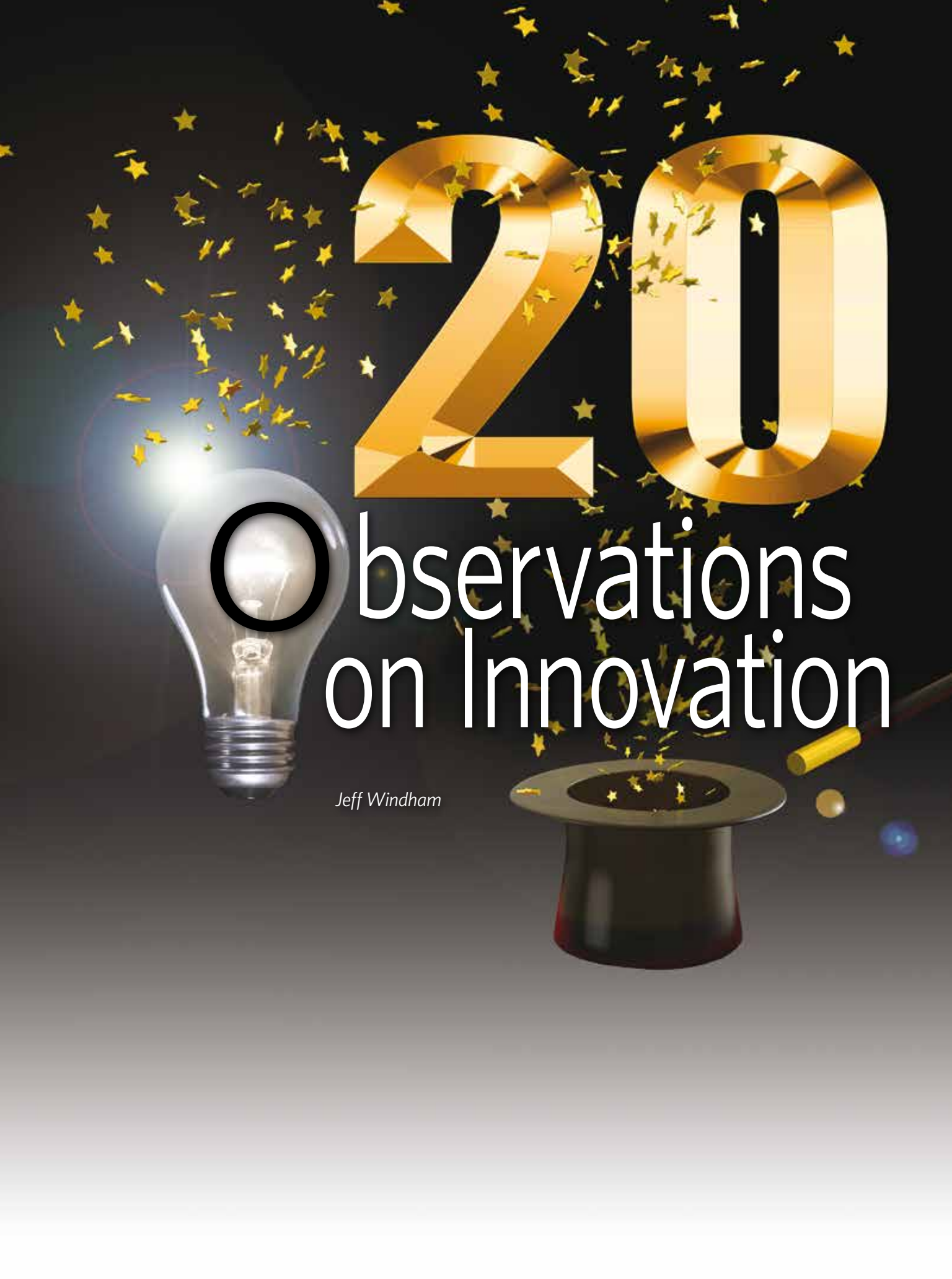
Online Presence for Easier Use on Mobile and Desktop Devices: http://dau.dodlive.mil

ALL READERS: Please subscribe or resubscribe so you will not miss out on accessing future publications.

Send an e-mail to darjonline@dau.mil and/or datlonline@dau.mil, giving the e-mail address you want us to use to notify you when a new issue is posted.

Please type "Add to LISTSERV" in the subject line.

Please also use this address to notify us if you change your e-mail address.



Observations on Innovation

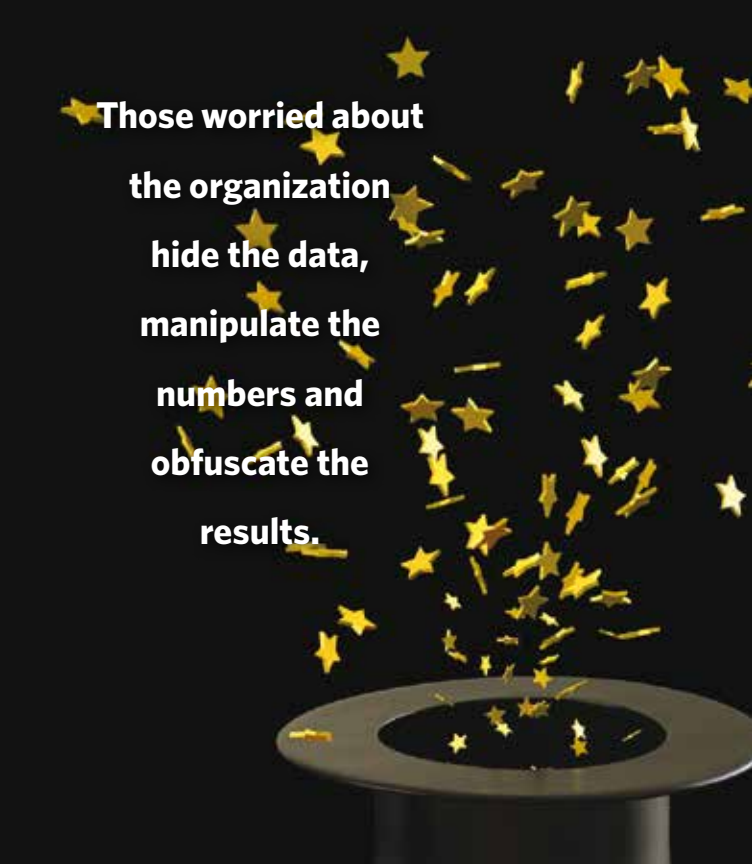
Jeff Windham

Defense Secretary Ashton Carter issued a challenge to the defense establishment to think "outside the five-sided box" and apply innovative solutions to today's national security challenges. Innovation in the Department of Defense (DoD) isn't easy. It's harder to innovate in the government than in the private sector; that's just the way it is. It's not easy, but it can be done. For those leaders and innovators who work inside the DoD acquisition system, here are some observations:

1 **Innovation is not a product; it's a byproduct.** You can't create innovative ideas by trying to innovate. Innovation isn't a product created at will, it's a byproduct of something else. Innovation occurs when organizations solve difficult problems in an environment that encourages experimentation, risk taking and allows for short-term failure. The Bell X-1 flown by Chuck Yeager had a single design requirement: Break the sound barrier. It wasn't intended to do 100 things, or 10 things or be multi-role or modular. It addressed just one simple, single, hard problem. Solving that one problem led to many downstream innovations. If you want innovation, identify a few hard problems and challenge your organization to fix them.

2 **Lack of funding is no excuse**. If you think the first step to innovation is for someone to give you a big bag of money, you've already failed. Col. John Boyd's Energy-Maneuverability theory (E-M) revolutionized fighter aircraft design in the 1960s. Boyd had no money to develop his idea and no official backing. He developed his E-M equations by sneaking into the computer room at night at Eglin Air Force Base in Florida. To Col. Boyd, lack of funding

Windham *is chief of the Configuration Management Division's Small Caliber Systems Branch at the Army Armament Research, Development and Engineering Center in Rock Island, Illinois.*



was not an excuse. This leads to the most important assumption you must accept if you want an innovative organization:

3 **In the DoD, we don't lack resources, we lack resourcefulness**. What John Boyd lacked in resources, he made up with ingenuity. Wherever you are in your innovation quest, I guarantee there is something you can do that doesn't require a big bag of money. Start with the assumption that you don't lack resources to innovate, you lack resourcefulness. Start with that assumption, and I guarantee you will get better results.

4 **Worry about advancing your goals, not your organization**. There are two types of people in an organization: Those who protect and advance the *organization,* and those who protect and advance the *goals* of the organization. For example, a teacher who worries about educating kids, looks for better ways to educate kids and stays up nights worrying about educating kids, is advancing the goals of the organization. A school administrator who worries about increasing budgets, reducing classroom sizes and protecting teacher tenure is protecting and advancing the organization. In most situations, these two people will be in agreement. Reducing classroom size helps both advance the organization and the goals of the organization. But occasionally these two philosophies will diverge. For example, what to do with a poor performing teacher? If you support the goals of the organization, you will say that teacher needs to be fired. If you are protecting the organization, you will say that teacher needs to stay.

Another example is the wait-list scandal in the Veterans Administration (VA). The VA realized the long wait times made the organization look bad, so little by little they shaved the numbers and made many small adjustments to hide a problem and protect the organization. It wasn't one big decision; it was many little decisions. They were so worried about the protecting the VA that they lost sight of the goals of the VA.

One way to tell if someone supports the organization or the goals of the organization is how they react to bad data: a bad fitness report, bad customer survey or a bad metric of any type. Those who support the goals of the organization will publicize the bad data so problems can be corrected. Those worried about the organization hide the data, manipulate the numbers and obfuscate the results.

Why does this matter? If you want to have an innovative organization, worry about your goals more than you worry your organization. And when you find bad news about your organization, embrace it, publicize it and then work to make the bad news better.

5 **Be a problem solver, not a problem hider**. The VA wait list scandal is a great illustration of what can happen when there is an aversion to problems becoming known to the outside world. This is the "don't air our dirty laundry" mantra. But this approach leads to many negative outcomes. For problems to be fixed they must be discussed openly. If you want to be an innovator, make sure problems are not hidden. Be a problem solver, not a problem hider.

6 **Solution versus workarounds**: There's a difference between a solution and a workaround. A workaround alleviates a symptom of a problem, a solution cures the problem.

For example, in the DoD, we have a supply system that provides spare parts to keep equipment operational. The DoD supply system is not very good. As a rough metric, it has about an 80 percent chance of delivering a part within 60 days. That means 1 part in 5 takes more than 2 months to arrive where needed. I use an online retailer and, if I order before 10 a.m. today, there is a 95 percent chance the box will be on my doorstep tomorrow. A 95 percent chance of next-day delivery—now that is a supply system. OK, but in the DoD it is 80 percent within 60 days. That lack of responsiveness is a root cause of many downstream problems. Field units create all kinds of workarounds: they cannibalize parts, keep an unauthorized inventory of spares, order nonstandard parts using a credit card, or use parts long after they should be replaced. Every workaround creates its own new set of problems. I'm not saying don't do workarounds—sometimes they are necessary. An individual field unit isn't going to fix the DoD supply system, so it does what is necessary to achieve the mission. But, as you address problems in your organization, if you understand whether you are doing a workaround or fixing the root cause, you will create a better solution regardless.

7 **Have you found the root cause**? Root causes are simple to express: "The DoD supply system is too slow." That's an easy problem to express. Not an easy problem to fix but easy to articulate the problem once you've drilled to the true root cause. If someone gives a long complex explanation of their problem, they are describing a symptom, not the root cause.

8 **Don't overestimate senior leaders' power**. Some think the way to implement an innovative idea is go to the head of the organization, convince that person of the merits of your idea, and—bam!—it will happen. It doesn't work that way. Every senior leader has 100 problems on his or her plate and only enough time and resources to deal with three of them. The chances of an innovative idea making it to the top of the list are remote. Keep senior leaders informed, but don't think selling the head of an organization on an idea will make it happen. Leaders can't order innovation to *occur.* They can be champions and help clear roadblocks, but, in general, senior leaders are not the driving force in innovation.

9 **Passion drives innovation—not rank, power or position.** The person who drives innovation is rarely the highest-ranking, smartest or best-educated person in the room. Those who drive innovation are the people who are the most passionate about the idea.

10 **Don't underestimate the power of passion in a junior leader**. An enlisted person, noncommissioned or junior officer, civilian or contractor who is passionate about an idea can accomplish far more than that person's rank would otherwise indicate.

11 **Innovation is not a committee function**. Committees can be useful venues for reviewing ideas and providing feedback but cannot develop innovative solutions to problems. Don't even try to innovate by committee.

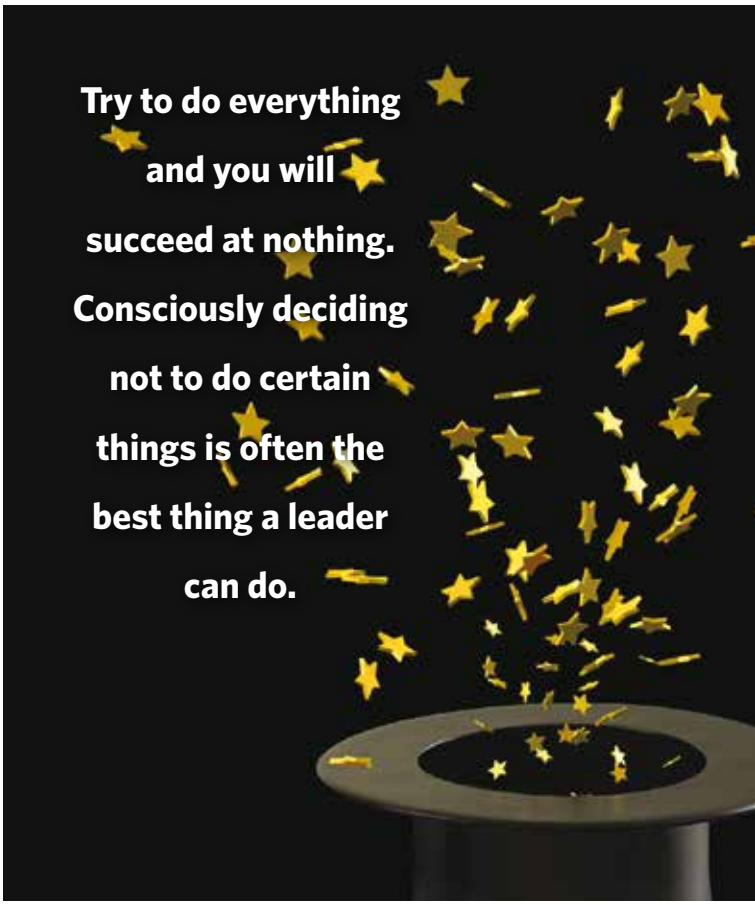
12 **Innovators are a small minority**. Less than 1 percent of the people within DoD are innovators. You may not like this statistic and you may wish it weren't so, but you must accept it. Identify the 1 percent in your organization and empower them in any way you can.

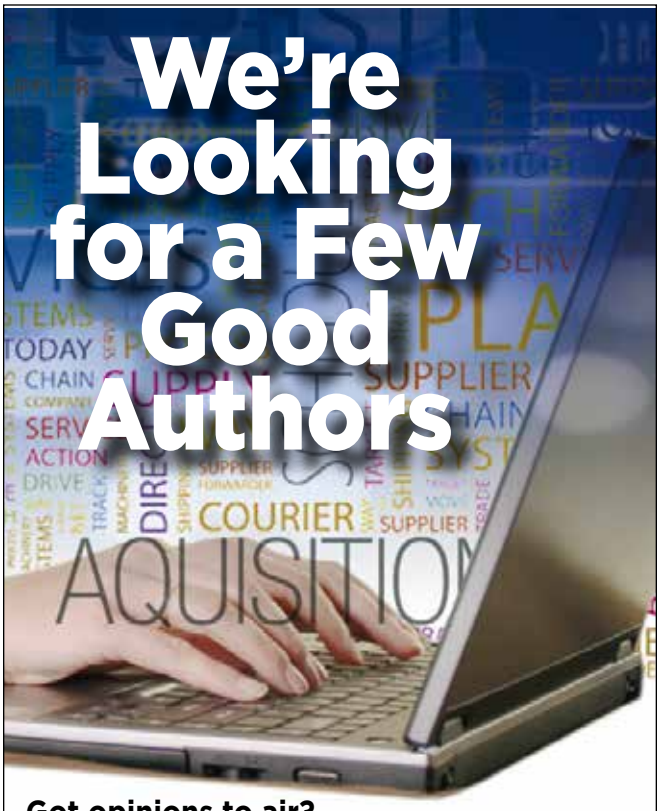
13 **You can't do everything**. Try to do everything and you will succeed at nothing. Consciously deciding not to do certain things is often the best thing a leader can do. When Steve Jobs returned to Apple Computer in 1997, the company was on the verge of bankruptcy. Its employees were disillusioned, unfocused and unmotivated. Apple had many projects in development and Jobs canceled 70 percent of them. Many of those canceled projects could have been successful, but Jobs understood that management and innovative bandwidth are limited commodities; spread them too thin and they are ineffective. When a leader consciously decides not to do certain things, he sends a powerful message to focus only on a few things and accomplish those few things well.

14 **Large organizations and the pitfalls of complexity**. Task a bureaucracy with solving a problem, and the solution it develops usually will add complexity—complexity to the process, to the organization, to reporting requirements or to the product. This is almost always wrong. Complexity is the enemy of innovation. Develop a disdain for complexity and constantly and forever simplify your processes, simplify your organization and simplify the products you provide.

15 **A bad solution written down is better than no solution**. If you have a problem and you don't know what to do, don't just commiserate about the problem and do nothing. Nothing gets fixed without a plan, and a plan has to start somewhere. Come up with a solution, no matter how bad, write it down and start a conversation.

16 **Ignore the naysayers**. The path to every successful idea is lined with people who say "you can't do it," "you shouldn't do it," "it's not necessary" and "you're doing it wrong anyway." The naysayers will wear you down. Ignore them. Perseverance is your most valuable commodity.





Got opinions to air?

Interested in passing on lessons learned from your project or program?

Willing to share your expertise with the acquisition community?

Want to help change the way DoD does business?

Write an article (1,500 to 2,500 words) and *Defense AT&L* will consider it for publication. Our readers are interested in real-life, hands-on experiences that will help them expand their knowledge and do their jobs better.

What's In It for You?

First off, seeing your name in print is quite a kick. But more than that, publishing in *Defense AT&L* can help advance your career. One of our authors has even been offered jobs on the basis of articles written for the magazine.

Now we can't promise you a new job, but many of our authors:

- Earn continuous learning points
- Gain recognition as subject-matter experts
- Are invited to speak at conferences or symposia
- Get promoted or rewarded

For more information and advice on how to submit your manuscript, check the writer's guidelines at http://www.dau.mil/publications/ATLdocs/Writer's%20Guidelines.pdf or contact the managing editor at datl@dau.mil.

17 **The soft sell works better**. When selling an innovative idea, the soft sell works better than the hard sell, especially when you introduce the idea. Sit back in a room and watch when any new idea gets proposed. People's thoughts immediately jump to "how can this new idea harm me?" It's easy for members of a group to talk themselves out of a good idea before they fully digest it. Soft sell the idea to get the group exposed to it. If you encounter resistance, back off and bring it up later. If you hard sell and people dig in their heels, nothing you say after that will matter. No new information will persuade them, because it's no longer about the idea; it's about the argument. Try to not let it get to that point. Patience and persistence are key.

18 **Prototype, prototype, prototype**. The first prototype is a sketch on a bar napkin. From that moment on, continually prototype as many iterations as possible, making them increasingly more developed. Use whatever means possible—cut and paste, flow charts, computer-aided design, 3D printing, whatever. This will help develop the idea and transition the vision from your head into the minds of others. Constantly prototype your idea in any way you can.

19 **Forget about unanimous consent**. In the DoD, we like consensus. This is the belief that we must achieve unanimous consent, and only then will we have the best idea. When it comes to innovation, this is a false belief. To quote Silicon Valley guru Guy Kawasaki, "innovative ideas polarize people." Innovative ideas are by nature new, untried, provocative, controversial and, therefore, divisive. Try to achieve consensus and you will do two things:

- Waste time (months and years in some cases).
- Turn innovative ideas into pabulum.

Wide-area review is a good thing, but complete consensus is neither healthy nor desired.

20 **Don't check your common sense at the door**. Anyone who works for the government can attest, we swim in a sea of rules, regulations and contradictory guidance. These rules probably made sense when they were established. But over time, piled one on top of the other, they can make doing the right, logical thing impossible. Regardless of this, blindly following the rules can't be an excuse for not doing the right thing. You can't check your common sense at the door. Understand the rule and why it was put in place, but at the end of the day do what is best for the warfighter and taxpayer. A word of caution: Understand the difference in bending a rule and breaking the law. Never break the law. But if you want to be an innovator, sometimes you have to follow the spirit of the rule more than the letter of the rule. Never check your common sense at the door.

The author can be contacted at **james.j.windham.civ@mail.mil**.

What's Your **Acquisition EQ**?

Owen Gadeken

At the Defense Acquisition University (DAU), we teach acquisition professionals the policies, processes and tools of the acquisition profession. We use a variety of learning strategies to enhance the "Intelligence Quotient (IQ)" of the acquisition workforce.

Often missing is the human element. Where are the human performance tools and best practices that can improve acquisition outcomes? DAU recently incorporated a new emotional intelligence tool with

Gadeken *is a professor at the Defense Acquisition University at Fort Belvoir, Virginia. His current interest centers on helping program managers become effective leaders. Gadeken received his doctorate in engineering management from the George Washington University.*

Table 1. Elements of Emotional Intelligence (EQ-i 2.0)®

Self-Perception	Self-Expression	Interpersonal Skills	Decision Making	Stress Management
Self-Regard	Emotional Expression	Interpersonal Relationships	Problem Solving	Flexibility
Self-Actualization	Assertiveness	Empathy	Reality Testing	Stress Tolerance
Emotional Self-Awareness	Independence	Social Responsibility	Impulse Control	Optimism

Note: The EQ-i 2.0 is a registered trademark of Multi-Health Systems, Inc. Table adapted by author.

the goal of enhancing the "Emotional Quotient (EQ)" of our workforce. This tool is the EQ-i 2.0® (Emotional Quotient Inventory, Version 2.0).

The concept of emotional intelligence goes back to 1983 when Howard Gardner at Harvard University advanced his theory of multiple intelligences, which included social intelligence. Interest skyrocketed when Daniel Goleman, a science writer for the *New York Times*, published his book *Emotional Intelligence: Why It Can Matter More Than IQ* in 1995. Several instruments have been created to assess emotional intelligence, and among them is the EQ-i developed by Multi-Health Systems in Toronto, Canada.

The current version of this assessment, EQ-i 2.0®, is illustrated in Table 1. It is composed of five categories with three elements (behaviors) in each category. An additional element of well-being (happiness) was added as the final component of the model.

While measures of intelligence (such as IQ) and even personality (such as the Myers-Briggs Type Indicator®, or MBTI) are thought to test inborn traits, emotional intelligence elements are considered skills that can be learned and further developed. The implication for acquisition professionals is that growing your emotional intelligence can provide a lever or springboard for improving the use of your acquisition intelligence and achieving better workplace results.

According to Dr. Travis Bradbury of TalentSmart, 90 percent of the top performers studied also had high emotional intelligence. On the flip side, just 20 percent of the bottom performers had high emotional intelligence. By using the EQ-i 2.0® as a development tool, you can measure, and then work to improve, your emotional intelligence.

Before embarking on the quest to assess and develop your EQ, we need to look for evidence that such effort will pay dividends in the defense acquisition environment. Fortunately, the evidence is readily available. In the early 1990s, DAU embarked on a major research study of program manager (PM) competencies. Twenty PMs from each Service (for a total of 60) were nominated by their program executive leadership to be interviewed by DAU. The interviews were based on critical incidents that each PM faced and were recorded and analyzed to develop the competency model in Table 2. Independent of the interviews, the PMs were divided into two groups (top versus good performers) based on assessments provided by their senior leadership as well as their direct reports.

When the research data then were analyzed to determine which competencies differentiated the top performers, the six competencies displayed in bold type in Table 2 emerged. Looking at these competencies, the four in italics clearly embody emotional intelligence: political awareness, relationship development, strategic influence and interpersonal assessment. Here is a more detailed look at these four competencies along with a quote for each from the interview transcripts.

Political Awareness. This competency enables a PM to know who the influential players are, what they want and how best to work with them.
"I really had to be sensitive to everybody's little piece of the pie. The operational community traditionally doesn't want to get involved with the development community. So you have to handle it with kid gloves to make sure you're not stepping on anyone's turf."

Table 2. PM DoD Competency Model (1990s)

(The six in bold type differentiate top-performing PMs)

Sense of Ownership/Mission ***Political Awareness*** ***Relationship Development*** ***Strategic Influence*** ***Interpersonal Assessment*** **Action Orientation**	
Decision-Making Competencies: - Critical Inquiry - Proactive Information Gathering - Systems Thinking - Optimizing - Results Orientation	Other Competencies: - Managerial Orientation - Long-term Perspective - Focus on Excellence - Innovativeness/Initiative - Assertiveness

Source: Defense Acquisition University.

Relationship Development. Time and energy are spent getting to know program sponsors, users and contractors.
"I made a trip to Scotland as a damage-control effort. I tried to restore our credibility. We really did want to help them out. I think they were surprised to see a four-striped Captain come all the way from Washington DC to talk about their problems."

Strategic Influence. This competency enables the building of coalitions and orchestration of situations to overcome obstacles and obtain support.
"I finally recognized that I needed heavy hitters with more influence and authority than I had, so I set up a meeting with the program executive office, the head of procurement, my staff, an attorney adviser and the Army's contract policy expert. In other words, I had to go in there and literally stack the deck in terms of influence and independent representatives who would vouch for what I had said."

Interpersonal Assessment. This competency enables a PM to identify the specific interests, motivations, strengths and weaknesses of others.
"I had one guy, a commander, who was really good, not so much on the technical side, so I had him work with me to pull this thing together. Interestingly enough, he was one of the best leaders I had ever run across, so I could use him to inspire people. A great manager, but not good enough to be captain."

While decision-making skills are part of the competency model in Table 2, none of these skills differentiated the top performers. Another way of explaining this finding is that the interview population of experienced PMs had all developed decision-making skills. But, except for the top performers, they had not developed their emotional intelligence skills.

A more personal example of this focus on emotional intelligence is provided by Capt. Mark Vandroff, PM for Arleigh Burke class destroyers. Here are excerpts from his October 2015 *U.S. Naval Institute Proceedings* article, "Confessions of a Major Program Manager":

- Most Navy Major Program Managers (MPMs) have graduate degrees in a technical field such as engineering or physics and then spend their tours practicing *organizational psychology*.
- The single most important skill an MPM can bring to the job is the ability to *convince a stakeholder* with limited accountability for program success to support a program like his or her life depended on it.
- The most important thing an MPM can build throughout his or her career is *relationships*.
- The Navy's senior leaders must choose MPMs who have a *passion* for their product.

The same focus on emotional intelligence also is found in the commercial sector. In 2012, Google launched a major internal study (as reported in a Feb. 25, 2016, *New York Times* article by Charles Duhigg) codenamed Project Aristotle to investigate why some of their teams achieved dramatic successes while many others did not.

As a data-driven organization, Google gathered extensive data from hundreds of its teams. At the top level, they found that teams that did well on one project usually did well on all their projects. Teams that performed poorly on one task often underperformed on their other tasks.

The research revealed that what distinguished the top performing teams was how team members treated each other. The researchers characterized this difference in terms of group norms. Top performing teams were found to share two specific norms not found in the less successful teams:

Taking turns in conversations. When everyone on the team had a chance to talk, the team did well. But if one person or a small number of members dominated the group discussion, the team was less effective.

Social sensitivity. This relates to team members' skill in "reading" each other. Top performing teams were skilled in telling how each other felt based on their facial expressions, tone of voice and nonverbal cues.

The Google researchers linked their findings to the concept of psychological safety. Teams thrived when members felt safe to openly share their ideas and feelings. These group norms also illustrate the impact of emotional intelligence. By demonstrating these two relationship behaviors, teams at Google were able to dramatically improve their business results.

The above research makes it clear that expert knowledge alone will not always result in successful acquisition outcomes. Acquisition work depends heavily on cross-functional teams. So, in addition to teaching the knowledge base of defense acquisition disciplines, DAU is beginning to offer team assessments and team-based tools. One of these tools is the emotional intelligence EQ-i 2.0® assessment. This assessment offers our acquisition professionals the opportunity to leverage their knowledge and experiences and apply them more effectively in their team-based environment to achieve significantly improved results.

Summary

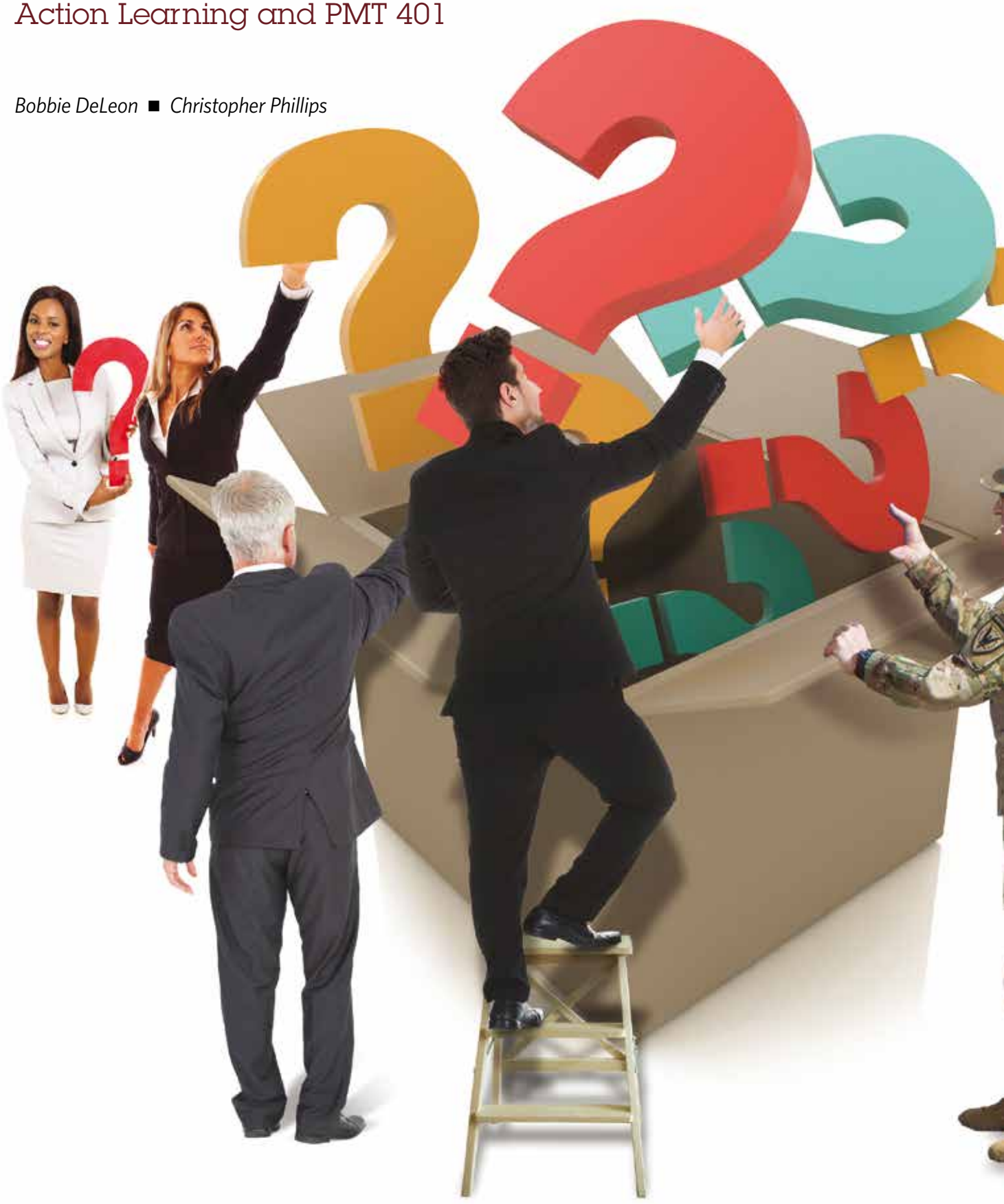
Success in the complex world of defense acquisition requires that acquisition professionals possess a broad range of knowledge, skills and abilities. But acquisition intelligence (IQ) can only go so far in delivering outcomes for the warfighter. Working to improve your emotional intelligence (EQ) promises dramatic improvement of your personal effectiveness in the near term and significantly improved acquisition results in the far term.

The author can be contacted at **owen.gadeken@dau.mil**.

Asking the **Right Questions**

Action Learning and PMT 401

Bobbie DeLeon ■ *Christopher Phillips*



Six students form a rough circle seated in a seminar room at the Defense Acquisition University's Fort Belvoir, Virginia, campus. They lean forward, engaged in animated give-and-take.

The students are enrolled in the Program Manager's Course (PMT 401), an intensive case-based, 10-week program aimed at improving leadership, critical thinking, problem solving and decision-making skills. Participants in this rigorous, in-residence program hail primarily from the military Services, defense agencies and the defense industry. Although most are program managers (PMs), their experience encompasses a wide a variety of acquisition communities including, engineering, logistics and testing. A trained coach is on hand to focus on the learning, and steers clear of direct involvement in the problem-solving discussion. The coach makes sure, among other things, that the questions broached are open-ended and that all students actively take part and are committed to arriving at a consensus. This maximizes opportunities for learning and development.

Students are charged with identifying the problem and the next steps in resolving a dilemma that a PM would face in the life of an acquisition program. It is an issue or situation in which they are not the subject-matter experts and do not have extensive personal experience with the specific program. They must nevertheless identify a path forward, seeking to find the optimal solution.

Here is a typical question-centered problem that PMT 401 students scrutinize and seek to resolve: The PM has just received new data that suggest an in-flight failure may occur. The technical experts do not agree on the nature of the problem and first flight is scheduled for today. The PM has to decide whether to continue or to delay first flight, given the cost, schedule and performance ramifications of each course of action.

By bringing their unique experience, perspectives and insights to the question, the students are able to shine new light on it. Meanwhile, their coach listens intently, observing the group dynamics and enforcing the rule requiring the statements be made only in response to questions (see Figure 1). She deftly inserts herself when appropriate with a timely query: Do we have consensus on the problem? What is the quality of our questioning? What question are you answering? What are we doing well as a team in terms of problem solving? What can we improve on? Each session concludes with a review of the next steps in resolving the problem as well as a discussion of best practices to improve both team and individual performance.

DeLeon *and* **Phillips** *are professors at the Defense Acquisition University, Defense Systems Management College at Fort Belvoir, Virginia.*

Figure 1. Two Ground Rules

1. Statements only in response to questions
2. The Action Learning coach has authority to intervene to improve the performance and learning of the group.

Needless to say, this is not your typical instructional approach for simulated real-world problem solving—a group of people with no particular proficiency in the specific problem under examination offering valuable insights that can lead to novel and effective solutions.

Welcome to Action Learning.

A Unique Approach

Action Learning's origins can be traced back to the 1940s, when Reginald Revans, a Cambridge University scientist, was asked to help improve productivity in the United Kingdom's coal mining industry. While industry executives expected Revans to use a traditional problem-solving approach—in which the managers would take the lead—he instead insisted on meeting with those who worked on the frontlines in coal mining. Revans believed that, if the viewpoints of those involved in mining were solicited, if their combined brainstorming power was harnessed, and—most important—if they had real decision-making authority in solving their most intractable problems, this would prove the most productive way to devise and carry out an effective solution (see Figure 2). That was the genesis of the Active Learning approach.

Figure 2. How Action Learning Differs from Other Problem-Solving Groups

- Questions precede answers; dialogue over discussion and debate
- Learning and team development as important as solving the problem
- Membership not reserved to experts or involved people
- Coach works learning opportunities
- Consensus on problem
- Skill Development
- Urgent and complex problems requiring unique systems thinking
- Groups charged with implementing the solution as well as solving the problems

Fast forward to today. The current version of Action Learning was developed by Dr. Michael J. Marquardt, Advisory Board chairman of the World Institute for Action Learning and professor of Human Resource Development and International Affairs at George Washington University. Marquardt has seen to it that Action Learning's core tenets from its very beginning—the use of insightful and reflective questioning in tandem with careful listening and immersive problem solving by small multidisciplinary teams—have remained distinctive elements.

Action Learning now is used the world over by business and organizations of all sorts, in the public and private sectors, and makes significant contributions to the most pressing organizational issues: problem solving, organizational learning, team building, leadership development, and professional growth and career development. Its five core components:

- A problem or project challenge
- An action learning group or team
- A process of probing questioning and reflective listening
- A specific response, developed by consensus, on the assigned problem or dilemma
- A shared commitment to learning that contributes to the development of more effective and equipped leaders, teams and organizations

In the PMT 401 instructional approach that incorporates the Action Learning method and ethos, one key distinguishing feature is that students do not start out with a preconceived problem. Rather, they begin with a situation or issue that is described in a PMT 401 case study. It can be posed as a problem, but the students themselves decide whether this is in fact the problem they're solving or whether it's a symptom. They must first arrive at consensus on this dilemma before proceeding. This focus on better defining and discovering the problem at the outset sets apart Action Learning from other approaches, and makes it an effective complement to PMT 401.

Action Learning and PMT 401

Action Learning in PMT 401 began as a pilot in 2011, undertaken by Dr. Bobbie DeLeon, professor of Acquisition Management, who was exploring the impact of Action Learning on the

critical thinking development of professionals taking part in the 10-week course. The initial feedback from the students was mixed: Some found the structure too restrictive, while others appreciated the participatory and inclusive approach. They particularly lauded how Action Learning helped improve and hone their listening and questioning skills.

Since then, Action Learning has become a mainstay of PMT 401 at Fort Belvoir. It has been further refined over the years, with students now undertaking case dilemmas in three Action Learning sessions (see Figure 3). The PMT 401 enterprise faculty received training to ensure that the "learning by doing" experience is as meaningful as possible for all involved, and that the Action Learning paradigm meshes with the program's best practices for learning.

Figure 3. Action Learning Team

- Small group (4-8 participants)
  - Problem Presenter
  - Team Members
- Learning Coach
- Focus on Individual Skill Development
  - Each member uses questions from critical thinking model
  - Other members note demonstrated skill
- Focus on Group Learning
  - Reflect on actions to improve future sessions
  - Reflect on learning to identify insights

Most curricula that aim to enhance leadership capacities for professionals tend to lump together problem-solving and decision-making skills. Not so for PMT 401. Its emphasis is on taking a step back and first zeroing in on key foundational questions: "Am I solving the right problem?" "What do I need to make a decision?" "Have I framed it the right way?" This learning paradigm, which places primacy on framing and exploring the right questions, can generate more fruitful options and more effective outcomes for decision makers.

The emphasis in the initial part of any given Action Learning module offered at PMT 401 is on arriving at consensus on the problem that students seek to solve. This doesn't mean that there is universal agreement that there is one way to solve the problem, but students have come to a meeting of minds on an approach and how to move forward with this particular approach. This in turn helps them better answer that question of questions: "Am I solving the right problem?"

The Primacy of Questions

Action Learning is comparable in many ways to the Socratic Method, in that questions are considered more important than answers. Or at least, the operating premise with both approaches to inquiry is that the most advantageous answers—ones that (in the case of Action Learning) lead to beneficial knowledge for impactful problem-solving—cannot be arrived at until and unless significant attention and effort are initially placed on coming up with the most potent question or set of questions. The result is that, rather than spurring PMT 401 students to engage in a debate in which someone wins and someone else loses, the emphasis is on open-ended, methodical and reflective inquiry promoting the discovery of common ground in which all the participants "win."

Clearly, this puts Action Learning into alignment with PMT 401, with its emphasis on cooperative and experiential learning and with facilitated discourse that stresses student-centered questioning and reflective engagement on real-world problems that a senior manager would face. Students gain considerable practice in exploring questions that lead them to engage in shared problem-solving rather than in advancing a particular agenda. This is at the heart of leadership development, critical thinking-based problem solving and sound decision making.

PMT 401 students also come to a keener understanding of when it's best to talk and when it's the best time to listen. Action Learning stresses that what you say, how you say it and encouraging others to share their own insights, make all the difference in cultivating leadership and problem-solving skills. This is where becoming a more astute questioner enters the picture. The best leaders know that the quality of the questions that they and their team come up with are paramount (see Figure 4). All those involved must become more expert at understanding the purpose of their questions, their underlying assumptions, the problem they're trying to solve, the concepts that everyone needs to understand, and who the stakeholders are. Leaders must model this approach.

Figure 4. Attributes of Great Questions

- Do not have a preconceived answer in mind
- Are fresh questions to evaluate the same data in new ways
- Are supportive, insightful and challenging
- Create clarity—open doors in the mind and get people to think more deeply
- Challenge and test assumptions—explore why and how
- Are open-ended

A hallmark of Action Learning is the promotion of this guiding tenet: Leaders ask questions, actively listen and encourage those working with them to do the same. By employing precepts of the Action Learning method, such as reflective questioning, those taking part in PMT 401 become even more proficient at its collaborative problem-solving approach in a rapidly changing environment. That is the crux of the program.

The authors can be contacted at **bobbie.deleon@dau.mil** *and at* **christopher.phillips@dau.mil**.


DEPARTMENT OF DEFENSE

Turning **Words** Into **Action**

Confronting Acquisition Challenges

Maj. Jamie J. Johnson, USAF, Ph.D.

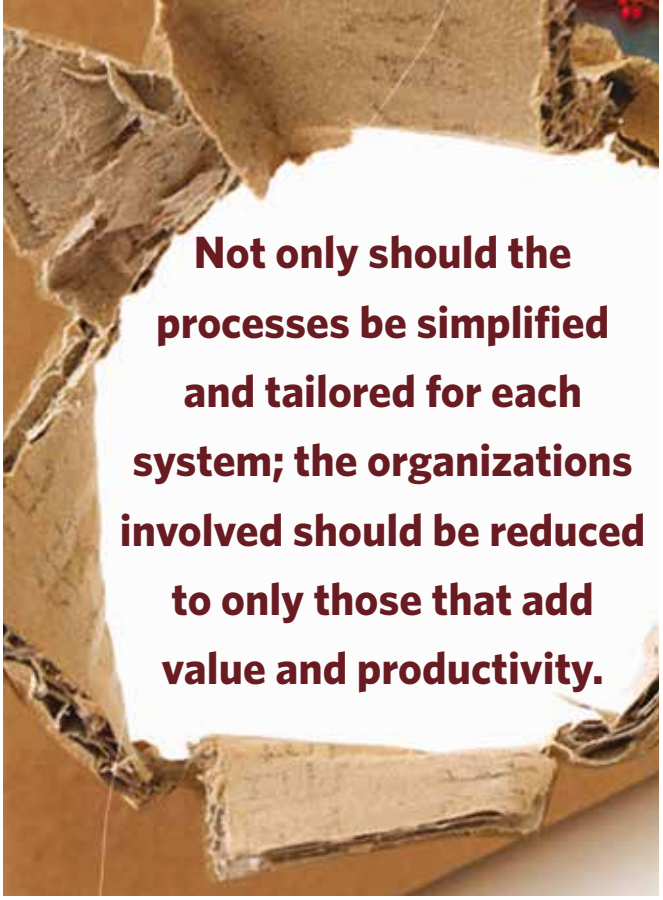
The 2014 U.S. Air Force policy document *A Call to the Future* boldly stated that the military of today and the future faces a new threat, a new environment, and urged that our force be prepared to respond appropriately. Its message was and is a call to accept a coming change that we cannot control, be prepared to fight new evolving threats, and begin thinking differently about how to execute our mission.

The Secretary of the Air Force asked that we eschew any "stay the course" mentality, while our Chief of Staff stressed that we "continue to adapt and respond faster than our potential adversaries." It noted that we must be a strategically agile force, with flexibility and consciousness of the strategic implications of changes. Change is very much a theme, as the report emphasizes "changing those things that stand between us and our ability to rapidly adapt."

The section that addresses acquisitions was titled "Capability Development." One reads that "the system is cumbersome, as the cost and complexity of these large programs draw additional layers of oversight and scrutiny," and that agility must be designed into the system being acquired. It suggests an acquisition process that uses "pivot points" designed to change or abandon elements of a program that have become too costly or that are underperforming. Rapid prototyping is suggested to reduce resources needed to bring new ideas online and to make technology insertion more efficient. It promises that regulations and policies will be changed so we can smartly go from "complex programs rife with crippling interdependencies to programs with simple, severable components, open architectures, and more distributed participation."

Transitions between full-time and part-time work are to be entertained for the acquisition workforce, with the goal of "flatter and more agile organizations that minimize administrative drag." For the foreseeable future, the pace of acquisitions will be driven by technology.

Johnson *is a selectee for the new Department of Defense career intermission program. He has 14 years' experience in technical program management and systems engineering working with space control, spacelift, aircraft, and propulsion systems. Johnson earned his Ph.D. at the Air Force Institute of Technology.*



This "is central to maintaining the asymmetric our Air Force has always provided the nation." This also in line with the latest National Security Strategy that directs us to "safeguard our science and technology base to keep our edge in the capabilities needed to prevail against any adversary."

The warfighters—those who operate the systems we field—continue finding new uses that designers never originally imagined. This "feedback loop" is critical and must be made stronger, as it helps "rapidly validate operating concepts ... and disseminate them force-wide." But modern challenges remain that must be confronted.

Meeting the Call: People

Current challenges for the workforce involve how we think, how we organize and how we are developed. If we want more agile acquisitions that effectively implement program pivot points and allow faster decisions, then our people will need to change too. Leading troops is one thing; leading a sea of people with master's degrees and making them feel empowered is another. The challenge to address is:

Our not-for-profit workforce must earn respect as entrepreneurs and be prepared to take risks based on educated trade-offs.

Often when an organization begins a major acquisition, norms are set that may cause groupthink or other phenomena that could cause problems. One type of groupthink involves overestimations regarding acquisition guidelines and rules, that they must all be followed by the book—every milestone, every piece of documentation, and every step in the staffing process must be met. Another type involves pressure toward uniformity and not questioning the organization's direction.

For example, an organization may hold on to a key performance parameter that through years of analysis and technology development, has been found to be very unrealistic. And this may be held onto despite the group's best efforts to start with tangible and testable requirements.

Major cost-benefit questions should not be ignored, regardless of the momentum or smoothness of the current program execution. Air Force leaders now recognize and want to incentivize "smart risk-taking" and reward "constructive failure" to knock down barriers to new ideas.

Another barrier arises when a group collectively decides on a course of action that is not in line with the preferences of many or all group members. This is the well-known Abilene Paradox. Many of us have had the pleasure of experiencing this phenomenon, in which a strong personality may push for something and the rest of the group internally disagrees but no one will speak out because they all mistakenly believe everyone else agrees with the plan.

It is difficult to predict the future—however, time should be given early to testing unpopular thoughts and courses of action. All members—from managers all the way down to the worker bees—should be heard from and insights sought from all direct and indirect stakeholder organizations. All should have the courage to make a change or cancel unnecessary activities if things do not turn out as planned. This approach provides a lower chance of going from the Abilene Paradox to dumping money into a never-ending, never-achieving, and worst of all, never-delivering acquisition program.

How we organize is important because it determines levels of empowerment, authority, responsibility and the size of the project we can handle. For very large projects, bureaucracy can be a necessary burden and works best if planned for early. For smaller projects, smaller groups can handle the load with less bureaucracy. Large projects typically are run by "hierarchical" organizations, while smaller projects can be run by "intermingling" organizations.

Col. "Lee" Battle led an intermingling organization when he suggested looking to "keep the program office small and quick reacting at all cost," which would later become one of "Battle's Laws." Smaller groups can give taxpayers a warm fuzzy feeling that we are maximizing return on investment, yet this does not mean hierarchical organizations do not achieve success as often. The challenge is to ensure the program office is the right size for the program and that unnecessary bureaucracy does not slow its pace. At the end of the day, to meet the goals set by our leadership, our workforce must be empowered and measure up to the employees of the most established corporations and most innovative start-ups.

Meeting the Call: Speed and Agility

A Call to the Future notes that rapidly emerging technological breakthroughs will result in more opportunities for global game-changers and that rapid change is the new norm. The effect to the warfighter is that we enjoy shorter durations of operational advantage. Speed and agility pertain directly to technology and our ability to harness it during its useful life. Therefore, this section recognizes the second major challenge:

Technology timescales are much less than our traditional and deliberate acquisition timescales.

Imagine if new models of smartphones and automobiles were developed and delivered to customers in the time it takes for typical defense acquisitions. Those companies would be out of business. Sure, the Air Force makes more than just smartphones, but most electronics companies offer many models and devices. Then these companies distribute these products to millions, sometimes billions, of people. That is quite a feat. To pile on, they provide a product that most people are satisfied with.

What sets the Air Force apart is that we often deal with cutting-edge secret technology combined with highly complex systems. Then we add requirements that make it more complex. And we deliver only a few hundred or sometimes just a handful of these items. Too often we do not know the true satisfaction level of the receiver of the product.

Last, this all costs a ton of money. Technology cycles will only decrease with time. Unless we make great leaps, this challenge only gets worse.

The pace of traditional acquisitions is greatly affected by the regulations that govern it, the processes, the organizations and the staffing. The Integrated Life Cycle Management System chart has been the standard for acquisitions processes for the last 10 years. Thankfully, this monster is now defunct and has been replaced by the Generic Acquisition Process Wall Chart, which debuted in December 2014. We smartly realized that "we must empower, encourage, and train our workforce to think—not dictate a cookbook that workforce members blindly follow," as Frank Kendall, Under Secretary of Defense for Acquisition, Technology, and Logistics, noted in the *2014 Annual Report on the Performance of the Defense Acquisition System*.

The new life cycle chart is intentionally less detailed in order to be less prescriptive and to encourage tailoring of the acquisition process as outlined in Better Buying Power (BBP) 3.0. Regardless of which process is used, we must ask ourselves, "To what degree are our adversaries holding themselves to the same high levels of bureaucracy, and is it worth the risk?"

In order to reduce acquisition cycle times, process cycle times must be addressed. Sure, mechanisms exist to speed the process based on urgency. We have joint and component-level urgent and emergent needs. However, these are not funded with the same "color" of money as most deliberate acquisitions reported in national news for having technical issues or delays. For the majority of programs which go through the Defense Acquisition System (DAS) sequence, there are other tools in the toolbox. Department of Defense Instruction (DoDI) 5000.02 offers an Accelerated Acquisition Program model when an adversary creates a technological surprise. This model can be used where the need is very urgent, in which case it becomes a Rapid Acquisition Activity (RAA). The concept of RAAs popped up in late 2013 and unlike joint urgent operational needs, use highly accelerated phases and milestones to support fielding within just 2 years.

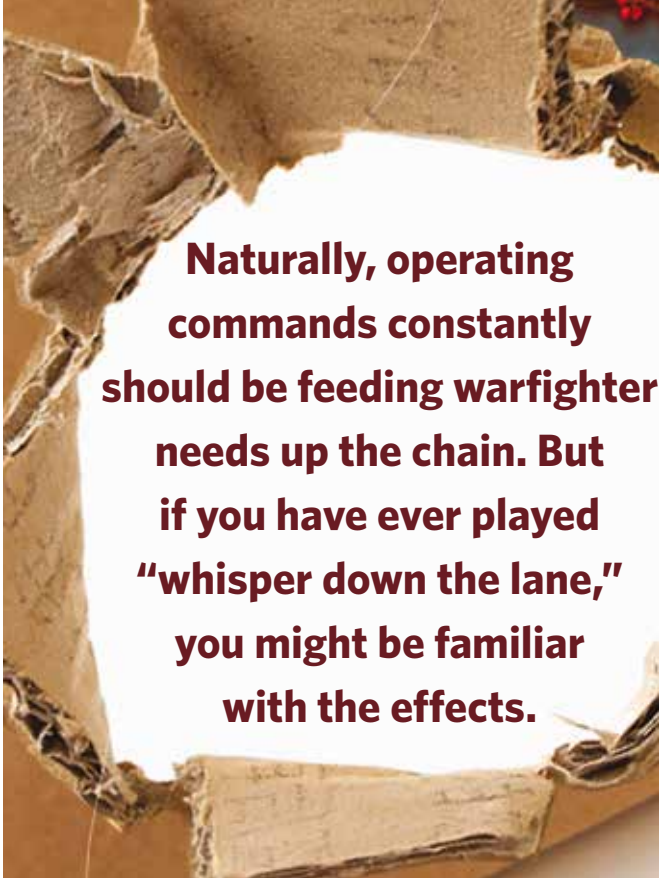
Programs can also use novel methods of contracting, such as rapid technology prototyping, milestone-based competitions and incentive prizes. Examples can be found in the *2014 White House Report on Innovative Contracting Studies*.

One notable form of contracting is Fast, Inexpensive, Restrained, and Elegant, which puts hard limits of time, money, complexity and size to ensure the right product results at the right time. There also is traditional contracting that uses schedule or performance incentives, award fees or fixed prices to put the burden on the contractor. Finally, there is Lowest Price Technically Acceptable contracts for simple services and systems with well-defined requirement sets. Ultimately, it is imperative that traditional system acquisitions are delivered to the warfighter in a timely manner before they lose relevance, utility and effectiveness against a future threat.

Not only should the processes be simplified and tailored for each system; the organizations involved should be reduced to only those that add value and productivity. This means that any organization that performs unnecessary oversight or funding pass-through should be considered for elimination. This would enhance delegation of authority and responsibility commensurate with the program manager (PM) position. Holding PMs accountable with less oversight or dependency on other organizations ensures efficient division of labor within the command chain.

Along with standard operation and organizations, our definition of staffing requires attention. We are all familiar with the analogy of the clock on the wall in the meeting room ticking away with all the dollars over the length of the meeting at the combined hourly rate of everyone in the room. Meeting costs add up quickly. This argument has driven forward-thinking companies to minimize duration of and attendance to meetings, as well as conduct them as stand-ups, where no one has the opportunity to sit. This has proven to make meetings more efficient with no detriment to the quality of the decisions.

Now imagine a clock on the wall ticking away, adding dollar after dollar, while everyone in your organization waits for key authorities to staff key documents, waits for leader's and adviser's calendars to clear up, and waits for other organizations to approve coordination of program documents. This is



an early acquisition schedule risk that is unaccounted for in most planning and acquisition strategies—in the meantime, the warfighter waits.

Often program milestone documents, especially for higher acquisition categories, go through multiple iterations within the major command, then within the Service component, then within the DoD. Now, we're really talking a lot of money on the staffing clock. Per BBP 3.0, action is being taken to address this, as the Assistant Secretary of Defense for Acquisition was charged with drafting a plan in 2015 to streamline staffing for document reviews. We all know time is money, and this should be kept in mind when we execute acquisition staffing functions.

Meeting the Call: Including the Warfighter

The cyber domain is on the leading edge where the lines are blurred between development, test, operations and sustainment, as all of these processes can be done through a keyboard. Other systems in other domains will begin to blur these boundaries as well, especially as technology timescales decrease. As our leaders call for a more integrated operator feedback loop, we need to address the following challenge:

The user warfighter requires more say in the acquisition process.

Acquisition professionals are collectively called "idea fairies" for a reason. Because we swoop in once every couple of years and tell the operators what they're going to get and how we have a grand scheme to deploy a new system with our great ideas founded on all of our master's degrees. Then we run off to design and build our widget and don't see them for another 2 or 3 years.

Sure, warfighters are involved in the process. However, there are two types of warfighters. There is the warfighter who spent the majority of a career on operations with a ton of experience at the Pentagon and who can help inform requirements and future planning. Then there is the operator or user who actually will receive and use the system. The latter of the two, the "user-warfighter," requires more say in the defense acquisition process.

The latest *Joint Capabilities Integration and Development System Manual* outlines who the primary equities are for key program documents during pre-program activities. Nothing is listed about user-warfighters. Naturally, operating commands constantly should be feeding warfighter needs up the chain. But if you have ever played "whisper down the lane," you might be familiar with the effects. Compounding this effect, you have very senior advisers who are excited to do their job well and add their own inputs. These advisers do great things informing Capabilities Based Assessments and Initial Capability Documents. Still the user-warfighter needs to be more involved in some capacity early in the DAS process and be a voting member for milestone reviews.

DoDI 5000.02 includes little content regarding the required attendees to program milestone reviews. Nowhere on the new DAS process chart does it have markers for "warfighter input." Upon searching the term "user" in DoDI 5000.02, one will find few instances of the term until you get to the sections about developmental and operational test. Regarding selection of PMs, the document mandates that they have a "deep understanding of user needs." How can PMs deeply understand user-warfighter needs if they do not begin to talk to each other until after Milestone C?

Meeting the Call to the Future

With the latest acquisition guidelines and a sampling of modern acquisition challenges, one can better turn words into action. And with an acquisition expert, Defense Secretary Ashton Carter, at the helm of the department, we can be sure that the challenges noted in *A Call to the Future* will be taken seriously and the continued implementation of initiatives followed closely. Acquisition leaders should be held accountable for the actions given and resulting changes outlined in key acquisition guidance—most of which was refreshed in 2015.

We should ensure that those not familiar with these changes are educated and continue to change their way of thinking. With a conscious and critical awareness of how we do business, why we do business as we do, and most important for whom we perform acquisitions, I expect we can and will continue to have the advantage over potential adversaries.

The author can be contacted at **jamiejayjohnson@yahoo.com**.

Improving **Competition**

Reforming the Requirements Process

Roy Wood, Ph.D.

Typical acquisition reform efforts have been focused in the margins, achieving marginal results. The evidence of decades of acquisition reform indicates that the marginal reforms typically taken are not making the fundamental changes needed by the Department of Defense (DoD). Legislative changes made since 2009 and several years of Better Buying Power refinements have incrementally improved acquisition practice, but many would argue that more change is needed.

Real competition is the single most powerful tool available to the Department to drive productivity.

—Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics' Better Buying Power Web portal.

http://www.acq.osd.mil/fo/docs/USD_ATL_Guidance_Memo_September_14_2010_FINAL.PDF

Wood *is the Acting Vice President of the Defense Acquisition University and former Principal Assistant Deputy Under Secretary of Defense. He is a retired naval officer and acquisition professional.*

Losing a single large procurement for ships or aircraft could force a company out of the business, leaving the government with a single monopolistic provider in a significant sector.

The simple, but revolutionary reform idea presented here is based on the author's research for the paper and presentation titled "Three 'Big Ideas' for Reforming Acquisition," delivered to the 12th Annual Acquisition Research Symposium in Monterey, California, on May 13, 2015.

The Problem With Competition

Full and open competition is the Holy Grail of defense acquisitions. Competition is believed to lower costs to the customers, incentivize productivity and efficiency, and spur innovation among competitors. To win a competitive contract, a defense company must provide a responsive proposal for a product or system at an affordable price that meets the military requirement.

To position itself to win a competitive procurement, a company must continually assess its capability to produce technical and innovative solutions to meet government needs while keeping its cost structures lean and competitive to produce these goods at more attractive prices than its competitors. Again and again, the government has seen evidence that competition encourages this behavior in the defense industry and has gone to great lengths to sustain a viable industrial base where competition can flourish. In short, competition is good, and more is better.

Yet, since the mid-1990s, the defense industrial base has shrunk and consolidated to an unprecedented level. With fewer businesses in the industry, it has become increasingly hard for government to encourage fierce head-to-head competition for many of its products and systems. This has been exacerbated by the reduction in new program starts, with the result that losing a single large procurement for ships or aircraft could force a company out of the business, leaving the government with a single monopolistic provider in a significant sector. Under these conditions, government source selections must be concerned with dueling priorities of sustaining the industrial base while getting the best deal.

In an effort to mitigate the situation, government buyers have sometimes attempted to create pseudo-competitive solicitations among the prime contractors or find ways to encourage competition at the subcontractor level. Workarounds, like dual-sourcing, split buys and leader-follower procurements have propped up the industrial base, but sub-optimized some of the cost benefits of real competition among the primes.

Encouraging competition at the subcontractor level has been more difficult. Privity of contract has deterred direct government intervention and influence on subcontractor selection and behavior. Another approach is sometimes used where the government contracts directly with lower-tier vendors and provides subsystems as government furnished equipment (GFE). Many government organizations are hesitant to use this GFE strategy because it risks placing the government in the proxy role of system integrator.

Given the challenges that a shrinking industrial base poses to competition, and the limited ability of government to engender competition among subcontractors, options to maintain a cost-competitive environment seem extremely limited. If competition at and below the primes is less an option then, what about competition above the prime?

Competing the Requirement

In theory, when capability gaps are identified, a full range of potential solutions is analyzed through a rigorous Analysis of Alternatives (AoA or AOA) process. Unfortunately, Service-centric solutions often emerge from the process, sometimes cutting off more innovative solutions. The Government Accountability Office noted in 2009 that "while AOAs are supposed to provide a reliable and objective assessment of viable weapon solutions, we found that Service sponsors sometimes identify a preferred solution or a narrow range of solutions early on, before an AOA is conducted."

A more robust and objective process might be to "compete" Initial Capabilities Documents (ICDs) among the Services and let each of the "bidders" conduct its own competing AoA to provide the capability. Rather than have only the predictable replacement of an Air Force bomber capability with another bomber, for example, perhaps more novel and affordable solutions would emerge from the Navy or the Army.

Competitive AoAs of this sort would become more rigorous, with both technical solutions and cost estimates coming under greater cross-Service scrutiny. The winning AoA, as judged by the Combatant Command and Joint Requirements Oversight Council (JROC), would then be "awarded" to the Service to manage through the conventional acquisition process. Armed with a more thoroughly scrutinized and complete AoA, the government would be better equipped

With increased incentive for one Service to call the bluff of another, overestimated claims of performance or underestimated cost estimates would not go unchallenged.

to negotiate with industry for a capability the joint forces require and have a much better understanding of the cost of such a system.

Adding this extra layer of competition could help address a number of current shortfalls and issues. First, it would force the Combatant Commanders and JROC to write ICDs that are focused on warfighting capabilities rather than tailored to telegraphing a proposed Service-centric solution.

For example, a generically written capability for destroying targets at long ranges could be accomplished with manned or unmanned bombers; cruise or ballistic missiles launched from aircraft, ships, submarines or land sites; rocket-assisted shipboard or ground artillery; or potentially other more innovative solutions. One can imagine the Navy and Air Force going head-to-head with aircraft and missile alternatives and the Army and Navy competing on missiles or artillery and all of the solutions competing on affordability.

Second, creating an environment of Service competition for real resources would incentivize each of the Services to ask hard questions about solutions the other Services put forward and to be better prepared to answer questions about their own proposals. This would force—and enforce—a cross-Service competitive rigor that does not exist today. With increased incentive for one Service to call the bluff of another, overestimated claims of performance or underestimated cost estimates would not go unchallenged.

Advantages of Internal Competition

In "Strategies for Managing Internal Competition," J. Birkinshaw points out three advantages to internal competition: first, it increases flexibility; second, it challenges the status quo; and third, it motivates greater effort. Each of these three advantages would accrue to the DoD through use of inter-Service competition.

Flexibility is critical at this time of rapid changes in potential threats as well as opportunities presented by new technologies. As militaries are wont to assume that the next war will be like the last one, it is critical to create an environment that produces a more flexible and responsive military. Competing requirements at the Service level would encourage innovation and flexibility and prevent the DoD from being stuck with proposals for the usual stuff from the usual players.

Similar to the first point, creating a competition among Services would help break the status quo. The Services are quite comfortable in their mission stovepipes, each continuing to receive about an equal 30 percent of the annual defense budget. Large organizations can become victims of their success. The inertia can stifle innovation and crush new ideas that seek to violate the way things have always been done. Indeed, most new systems are simply incremental improvements over previous ones, becoming one-for-one mission replacements of aircraft carriers, bombers and ground vehicles.

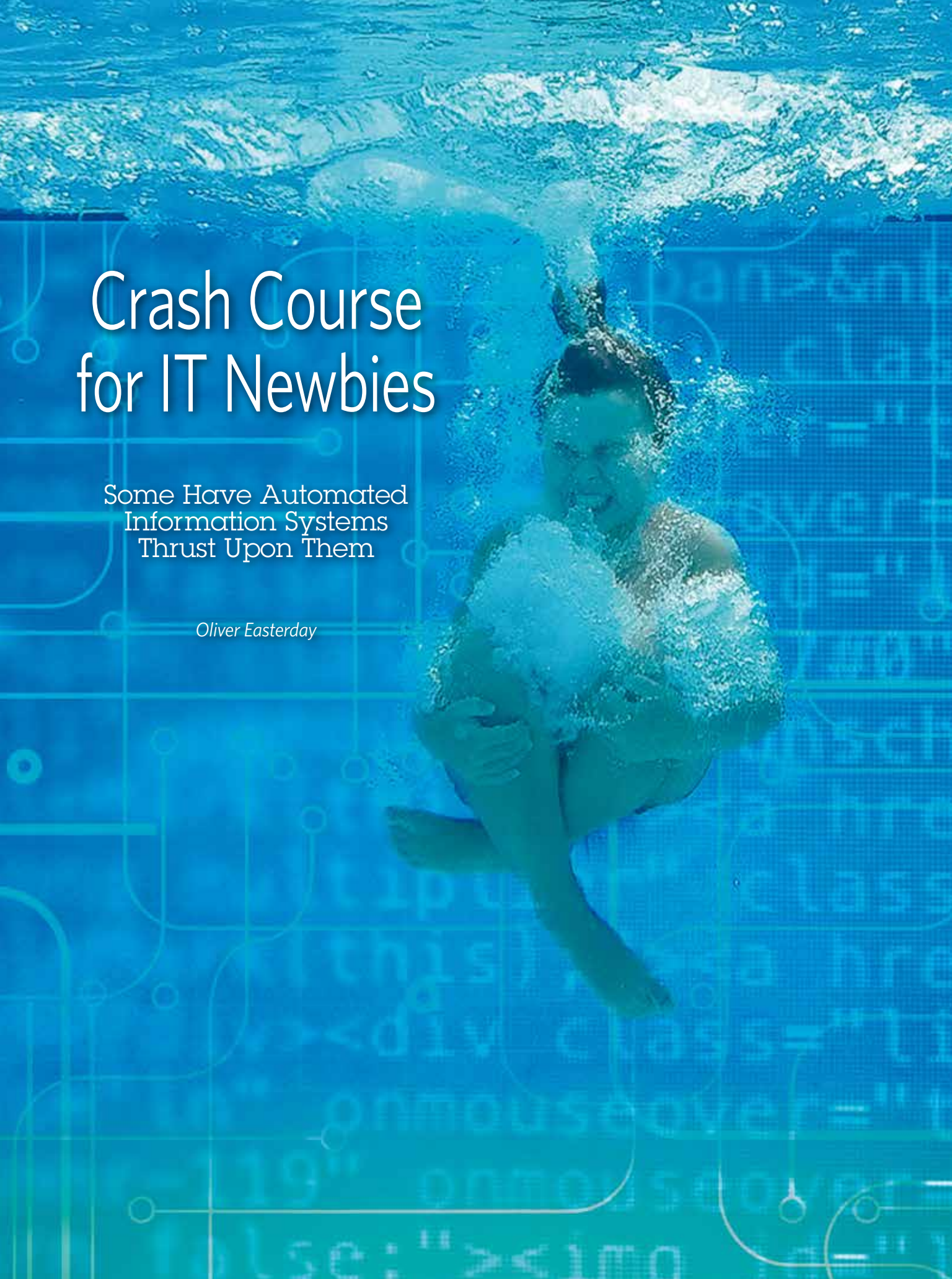
In 2004, the Joint Defense Capabilities Study noted that "Alternative ways to provide ... capability are not adequately considered—especially if the alternative solutions are resident in a different Service or Defense Agency." Instilling competition across the Services would challenge the status quo in ways not seen before.

The third point is that competition motivates greater effort. In an internally competitive environment, Services could be expected to be more aggressive, innovative and forward-leaning when faced with a direct threat to budgets and resources. One might imagine, for example, that a more thorough and lively discussion of the mix of sealift versus airlift capability would be brought forward by the Navy and Air Force if the results could change the resource and mission mix of each Service. Similarly, each of the Services might scrutinize quite differently the output of their various laboratories and warfare centers if they were forced to compete with each other on superior technology and innovation.

What Now?

The idea of internal competition above the prime contractor level is an attractive option to offset the difficulties of controlling costs through competition in a shrinking industrial base. Competing requirements among Services could help inspire innovation and break the status quo. It would reduce costs by allowing the warfighters to select the best-value solution to meet the need, not simply be tethered to a single Service's traditional alternative. Even with these potential benefits, the idea of competing requirements undoubtedly will meet resistance from those who seek to protect the status quo. The question is: Are we ready for real acquisition reform?

The author can be contacted at **roy.wood@dau.mil**.



Crash Course for IT Newbies

Some Have Automated Information Systems Thrust Upon Them

Oliver Easterday

Congratulations! Since you wrote code in the past, you're now designated as a software program manager for automated information systems (AISs) and information technology (IT). Don't forget, you developed embedded digital engine control code or perhaps published vehicle dynamics modeling software, and so human resources now deems you as "in-the-know" about all matters IT, AIS and/or Defense Business Systems (DBS) technology. You have now been assigned to start managing one of the Department of Defense (DoD) IT/AIS programs somewhere in the system's engineering process—perhaps in requirements or functional analysis and allocation or in synthesis.

During the 1990s' dot.com boom, and continuing in today's "post-personal computer era," the DoD has had trouble retaining cyber experts due to the lure of the private sector. Since losses are unlikely to be stanched anytime soon, a great deal of technically savvy, but not IT-specialized, folks are being shunted into IT/AIS/DBS program management. This happens because the domain of science and technology (S&T), which includes AIS/IT, is not well understood by many decision makers. "The needs of the Service" prevail, which raises the question of what hardware-centric acquisitions experts need to unlearn to avoid unwittingly injecting cost, schedule or capability slippage into their programs. Well, it's time to learn quickly that AIS/IT/DBS and software have some important fundamental differences where your experience can lead you astray. So what are the top things you need to unlearn? Here are some lessons learned the hard way:

- In scheduling out your program, realize software tech state-of-the-art is blazingly fast-paced. For example, one generation of gas turbine technology development encompasses almost 10 generations of software development and three to four generations of AIS/IT hardware. Fourth-generation fighters like the F-16 and F-15 have been around for 40 years and finally were eclipsed about a decade ago. In that same period, IT hardware evolved from minicom-

Easterday *is deputy branch chief of the Sustainment Branch at the Air Operations Center, U.S. Air Force C2 Requirements Division, Headquarters Air Combat Command, in Hampton, Virginia. He is an Air Force developmental engineer with 7 years of experience in turbine engine Science and Testing development and 4 years in depot sustainment of airframe line replaceable units.*

puters (PDP-8), through 8- to 64-bit personal computers, single-core to eight-core, and onward to the handheld device. When your system is being designed, keep a wary eye on not only the hardware obsolescence but also that of the software components. Press hard for mitigation strategies and a loosely coupled architecture. Remember when that F-16 fleet was just nearing initial operating capability back in the early 1980s? How much luck will you have opening on today's nonclassified network computer the Fielding Plan that was written in Word Perfect for DOS v5.0? Similarly, will your mission-critical database migrate across the iron to new operating systems? Be a futurist and think through on what data standards for exchange, formatting and transmission this future event will rely? Get familiar with the Joint Capabilities Integration and Development System ITBox process if you're working requirements.

■ Recognize that software configuration management is perhaps even more critical than that for hardware systems. There is a compulsion to keep tweaking code, thereby succumbing to requirements creep and "gold plating" with the attendant risk of completely losing configuration control. This is due to the perceived malleability of code. The key word here is "perceived," because tracking software changes and their introduction of second-order effects can be more tedious than actually making the changes. It is perhaps telling that Linus Torvalds, founder of the Linux operating system, seems to have felt that his greater contribution was the source version control system Git, which was developed to track versions of and allow scaling up his first contribution. It is also revealing that the Capability Maturity Model Integration concentrates more on software management than on the software product itself.

When costing unit production costs in Engineering, Manufacturing and Design, it is best to dump your hardware-centric thinking. Once code is written, debugged, passed through Developmental and Operational testing and the first compact disc is pressed, the unit cost to scale up is minuscule. The rare exception is software components that are commercial-off-the shelf (COTS) items for which per-processor and/or annual licensing, and/or software as a service costs may apply. By the way, direct licensing costs and avoidance of the recurring management burden to deal with them, not to mention baked-in data rights, are excellent reasons to explore the 2009 DoD Chief Information Officer memorandum on (free and) open source software to be deemed a commercially viable industry competitor. Know that hardware components are nearly always COTS and that a full technical data package may be hard to source. You may be further constrained by DoD IT equipment and software enterprise buys for many of your components. And while grousing about this loss of agility, admit that it does have an upside, such as leveraging enterprise bulk buys and helping to ensure parts traceability back to the foundry (per Open Trusted Technology Provider Standard of the International Organization for Standardization and the International Electrotechnical Commission). The latter benefit is not to be underestimated in this age of pressing cybersecurity concerns.

■ To comply with security, safety and privacy imperatives for Command, Control, Communications, Computers and Intelligence systems, weapon systems, and DBS, respectively, in this post StuxNet world, the aforementioned supply chain integrity is important for software, firmware and hardware. It's not just Windows 10 being the "bad boy" phoning home as mentioned in the lay press; Cisco routers have been found with "backdoor" code in their firmware that presents potential opportunities for espionage, or worse, sabotage. As a non-cyber acquisitions subject-matter expert, recognize that if it's on the DoD Information Network—and even if it's not—but merely executes binary code (e.g., "pushes 1's and 0's"), that, by definition, it is not behind the base fence but is out there in the public square and vulnerable to attack. From Day One of your program's architecting within DoD Architecture Framework Version 2, cybersecurity needs to be baked into your design and not bolted on. In a similar vein, net-centricity and utilization of open standards are critical capabilities and provide a major hedge against obsolescence. So while at, dust off that copy of DoD Instruction 5000.02 (*Operation of the Defense Acquisition System*) and give it another read through; this time dwell heavily on Enclosures 11 and 12, which are focused on pressing topics in defense software systems acquisition.

■ Unlike hardware components (gears, pistons and bearings), defense information and software systems do not fail on a Weibull or "Bathtub" curve. Outside of a select few components, like muffin fans, hard disk drive bearings and switching power supply transistors, bits and bytes do not wear out with duty cycling over their service life. Software stack components do undergo a high-velocity of capability upgrades and bug fixes, thanks yet again to that malleable nature of software. Data exchange standards evolve, application programming interfaces morph, and portions of the software stack get patched and modernized and so introduce second- and third-order changes. This leads to the fifth point and that is ...

■ Recognize that data rights are as critical, if not even more so, than protected rights in hardware systems. Reverse engineering by software decompilation often is prohibited by End User License Agreements (EULAs), is a more arcane skillset, and often yields cryptic results. Know that the ultimate technical documentation in the software world includes, but is not limited to, well-commented and -structured code in a vendor-neutral language like ANSI C, Fortran77 (as opposed to, say, VBasic or Oracle Java). Recognize that the whole system stack, from the bare metal hardware up to your end-user application, may impact your system's reliability and maintainability, even its ability to function. It does no good to have a vendor write a VBA-based solution when your infrastructure is to be run on a Portable Operating System Interface-compliant operating system like Linux. Given the massively interconnected, constant operation of many DoD

software-intensive and DBS systems, interface control (now central to your form, fit, function and interface [F3I] thinking) to standards are paramount, leverage them!

Now your arrival from the hardware-centric world does not totally disadvantage you; you bring some humility into software systems acquisition with that general lack of knowledge and therefore lack of institutional inertia. You are primed to foresee things those who have grown up within the AIS/IT world often totally miss or assume away:

First, unlike your IT brethren, you realize software often is the long pole in the tent for major systems schedule and technical risk; you may well have directly experienced this in previous tenure. I certainly did: Unlike many born-in-the-DoD program managers, I was a performer-integrator. In the late 1990s, the Office of Naval Research commissioned a deep-ocean intervention robotic submarine. The basic hardware of the vehicle—ballast, pressure vessels, sensors, fairing, thrusters, power distribution and major computing systems hardware, among other things—were all ready within 2 years of program kickoff. But realizing all the proposed capabilities in the software portion of this effort (SAUVIM) took yet another 3 to 4 years.

Second, your AIS/IT brethren often lack configuration management discipline, but you are sold on it. Let's face it, it's hard to change things around once you've "cut metal," and there is much lead time in sourcing extra material, tooling and skilled manpower. Meanwhile, the software developer's lexicon is salted with "sprints," "scrums," "jams" and "rapid spirals"; this is indicative of a Red Bull-fueled, Wild West mentality. And while it may lead to the next killer application like Angry Birds or Facebook, it can also doom a project for which the stakes on configuration are a little higher due to much more massive integration requirements, not to mention differing consequences for failure. Know that software program complexity does not scale linearly with project size; figure it to be more exponential in nature.

Third, you possess a holistic life-cycle view of programs from the outset since you come from a world where systems and components wear out, and so you already think in terms of bathtub curves, ancillary equipment, facilities, maintenance documentation and spares provisioning—perhaps because items are more tangible. Software program managers often neglect to plan provisioning for compilers, development environments, documentation and long-term interoperability; you can help save them from neglecting these life-cycle issues. While IT-pedigreed folks are accustomed to everything being "COTS-on-a-warranty," you can see beyond this paradigm and are not blind to other options with their life-cycle cost implications. Your IT brethren may blindly accept yearly software licensing burdens as "the cost of doing business." Your hard-won hardware experience may see a more optimal solution. Is the best plan buying government-off-the-shelf with well-commented code or should you look at COTS code, or even a free open source software ([F]OSS)-based solution? Is the 3-year warranted blade server iron in-house running GOTS software truly the best solution or would sourcing an accredited infrastructure- or platform-as-a-service (IaaS, PaaS) contract better meet the requirements with enhanced capabilities and feature a cheaper life cycle to boot?

Continue to assert your data rights with vigor as in this systems realm they are even more at risk due to your colleague's easy acquiescence to "it's always done this way" (a corollary of "You can't go wrong buying Microsoft/Oracle/Novell/etc.!"), the rarity of skill needed to reverse engineer compiled codes, and the statutory hooks that COTS software vendors load into their EULAs.

IT folks have a culture of doing it in-house, as a material systems expert that you know to engage industry and academia early and often to keep tabs on the state-of-the-art and best practices. And for this fast-moving area, do not skip engaging these folks for the informal market survey and the more formal analysis of alternatives, even for a low-dollar-value program.

You've got homework and reading lists ahead, but as the able science, technology, engineering and mathematics person who is a newbie to the world of DoD IT intensive program management, where do you start? It would be hard to begin with a short list. But to bootstrap your thinking across such diverse topics as architecting, cybersecurity and recent historical developments in the cloud consider, respectively: Barry Boehm, Peter Kind and Richard Turner's article "Risky Business: 7 Myths about Software Engineering that Impact Defense Acquisitions," in the May-June 2002 issue of the Defense Acquisition University's *Program Manager*; Kim Zetter's "An Unprecedented Look at StuxNet, the World's First Digital Weapon" published in *Wired* on Nov. 3, 2014; and, if you get a chance, Gartner Vice President and analyst Doug Laney's Gartner Symposium presentation "55 Examples of Big Data Case Studies in 55 Minutes." Get to know the nuances of the following terms via a little primary school-style vocabulary drill: seven-layer OSI model, virtualization, datacenter, Internet Protocol Version 6, IaaS/PaaS/SaaS, the internet of things (IoT), net-centricity, asymmetric-key, Big Data and cloud computing. Most of all, do a little refresher "Hello World" programming in code to familiarize yourself with the software creation process. May I suggest Brian Kernighan and Dennis M. Ritchie's book *The C Programming Language* as very good exercise for the new program manager or systems engineer?

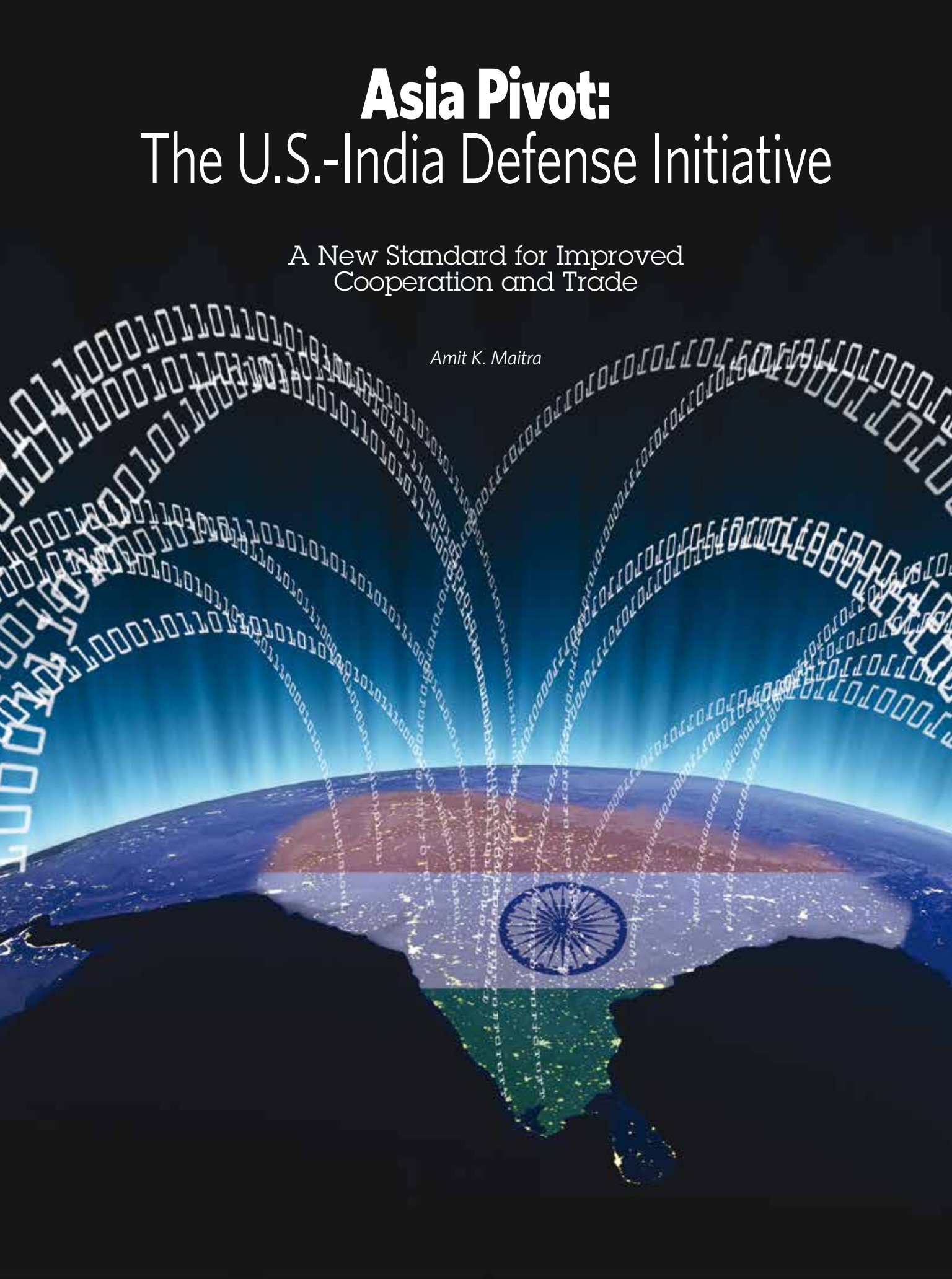
In closing, I also mention that the Defense Acquisition University itself has some very helpful short course modules to help with initially getting up to speed. Yes, you may be the newbie in the room, but at the same time realize you also bring a very valuable outsider's viewpoint and humility to this world. The DoD really needs this perspective given the 26 percent "success ratio" in software intensive systems, with the DoD managing only 18 percent (and 0 percent once above a $10 million level-of-effort) as cited upfront in the Boehm-Kind-Turner article.

The author can be contacted at **oliver.easterday@us.af.mil**.

Asia Pivot:
The U.S.-India Defense Initiative

A New Standard for Improved Cooperation and Trade

Amit K. Maitra



Today many people have different attitudes when they try to formulate manufacturing technology transfer policies. On one hand, some proponents of technology transfer see it as a way to improve the U.S. international competitive position. On the other hand, concerns with undesirable and sometimes unanticipated side effects of the transfer of sensitive and critical technology have led to sentiments against technology transfer.

In the absence of consensus, U.S. policy makers, both in the legislative and executive branches, face the challenge of constantly evaluating what kind of U.S. technology that the leaders of other countries want to import. Can this technology safely be exported to help develop other countries' industrial sectors and, more specifically, their manufacturing bases, while substantially enhancing U.S. strategic interests? What risks will these exchanges pose to specific U.S. industries and defense contractors?

These are complex questions, and the procedural hurdles are complex. There are different opinions on a whole range of issues. One opinion is that of U.S. Secretary of Defense Ashton Carter. In 2013, Carter spoke before the Confederation of Indian Industry (CII) in New Delhi. His views and recommendations and the expressed intentions of various administration officials interviewed by the author are that the U.S.-India relationship is global in scope. They see a convergence of our security interests, which include maritime security across the Indian Ocean region; Afghanistan, where India has done much to assist economic development and the Afghan security forces; and broader regional issues where the United States and India share long-term interests. Hence their view is that U.S.-India defense cooperation should be an essential part of a new partnership between the two countries.

Maitra *is a founding member and President of the Foundation for Emerging Solutions, which was established to strengthen the capacity of people throughout the world to evaluate the challenges, operations and solutions facing governments as they formulate national strategies to keep their defensive and offensive cyber capabilities current and in line with the international community.* *The author thanks Mukesh Aghi, President of U.S.-India Business Council (USIBC), Washington, DC, and Rahul Madhaban, Director of USIBC for Defense and Aerospace, who graciously reviewed the ongoing programs involving the U.S. and India business communities. Keith Webster, Director of International Cooperation, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.*

Carter spoke about practical steps the two countries can and should take to identify new opportunities and make new and innovative investments that will benefit both countries for generations. There is a need to define where we want to go and then make it possible to get there. The United States is building a force for the future, which Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey calls the joint force of the year 2020. Former Secretary of Defense Leon Panetta added, "The joint force is going to be agile, lean, ready, technologically advanced, and able to conduct full spectrum operations and defeat any adversary, anywhere, anytime."

Organisation (ISRO) harnesses space technology for national development, while pursuing space science research and planetary exploration. Both DRDO and ISRO have been removed from the Commerce Department Entity List, thereby allowing the United States and India to conduct joint research and co-develop technologies such as the unmanned aerial vehicles (UAVs).

The U.S. Government strictly controls foreign sales of larger UAVs, but approved sales of RQ-11 "Raven" built by AeroVironment Inc., whose partnership with its Indian counterpart will

The United States would do its due diligence and make approval decisions sooner. This is a new initiative to build exportability into its technology systems from the start and thereby avoid time-consuming delays and added expenses.

Underlying the new strategy is the U.S. decision to rebalance in the Asia-Pacific region. New investments by the United States in technology, weapon systems, innovative operational plans and tactics—and regional alliances and partnerships reflect this rebalance. According to Carter, the U.S. partnership with India is a key part of the U.S. rebalance to the Asia-Pacific area for broader security and prosperity in the 21st century. He emphasizes that the United States wants to leverage "the unique strengths of India to confront critical challenges and meet emerging opportunities." Toward that end, the United States is streamlining its internal processes and security cooperation programs to enhance sharing and cooperation with India.

U.S.-India military-to-military engagement has increased steadily over the years to include a robust set of dialogues, exercises, defense trade and research cooperation. India now is a top priority in U.S. export considerations, as the United States reforms the internal processes of the Department of Defense (DoD). (See author's related article, "Defense Technology and Trade Initiative—Ashton Carter's Strategy in India," *Defense AT&L* magazine, March-April 2016, Page 26—http://dau.dodlive.mil/2016/02/16/defense-technology-and-trade-initiative-ashton-carters-strategy-in-india/.)

These reforms make it easier for India to work with the United States. For example, Defence Research and Development Organisation (DRDO), an agency of the Republic of India, headquartered in New Delhi, is responsible for developing technology for the military. And the Indian Space Research

serve as a critical framework to rapidly build confidence and trust. This in turn will fortify an enduring partnership in military modernization, technology and manufacturing. In concert with these policy changes, an overwhelming and increasing majority of munitions license requests have been approved more quickly under direct commercial sales (DCS), and this will continue, as Carter stated categorically.

Bureaucratic hurdles are being removed, and processing speed relative to export decisions for India is improving. More striking is the recent U.S. move to make strategic export decisions for India. The U.S. Government wants its decisions to become more anticipatory about what India is likely to need in the future. As Defense officials have said, the United States would do its due diligence and make approval decisions sooner. This is a new initiative to build exportability into its technology systems from the start and thereby avoid time-consuming delays and added expenses. The combination of these efforts and the U.S. commitment to facilitating India's admission into all four global technology control regimes—the Nuclear Supplier Group (NSG), the Missile Technology Control Regime (MTCR), the Wassenaar Arrangement and the Australia Group—are designed to help the United States respond more rapidly to India's requests for U.S. equipment and systems, particularly advanced technologies. A rapid-reaction cell has been instituted in the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]) to attain this goal.

The purpose behind all these moves is to move swiftly toward cooperative research and development and co-production

with India. There are programs underway to streamline procedures and processes and showcase what the United States and India can achieve together in the global arena. Secretary Carter points to Tata Advanced Systems, Ltd, and Lockheed's joint efforts to produce parts for the C-130J in Hyderabad, India. Henceforth, every C-130J around the world will contain parts made from this joint production, exemplifying the kind of co-production that is the future. In his own words, Carter says, "it underscores what can be achieved when the two countries unleash the potential of the private industries in the two countries; ... when there is a common strategic view, when the bureaucratic barriers are down, and, importantly, when the strategic interests and genuine economic and business interests of the two countries and their private sectors are aligned."

Export control reform is just one element of overall improvement. Recognizing that India was the second-largest foreign military sales (FMS) customer in 2011 with $4.5 billion in total FMS transactions, which included the six C-130Js delivered on time, the United States is improving its FMS programs. One advantage of FMS is that government-to-government agreement through FMS offers competitive pricing, slightly more than DCS. These costs go to DoD, which affords protections India cannot get from industry alone. Further, it addresses long-term sustainment needs.

The United States is prepared to adapt its system to the unique needs of India and India's Defence Procurement Procedure (DPP). Carter referred to the programs under way to clarify the U.S. acquisition system, which can be difficult to interpret under some circumstances. First, a new fund allows the U.S. Government to procure long-lead high-demand items so that they are in its inventory in anticipation of partner requests. Second, a cadre of acquisition experts is ready to go to other countries to define their requests through cooperation and streamline the U.S. response. These programs will help India.

While U.S.-India high-value technology cooperation is gathering momentum, India can make changes to increase U.S. investment. One particular area where change has to be carefully planned is its ceiling on permitted foreign direct investment (FDI). It is reasoned that India raising its FDI ceiling to international standards could increase commercial incentives to invest in India. In August 2014, the Union Cabinet approved a proposal to raise FDI in defense to 49 percent from 26 percent. However, the U.S. defense industry was not satisfied with 49 percent FDI and preferred a controlling stake for "groundbreaking" weapons technology and manufacturing equipment transfer on par with its closest allies and in accordance with industry best practices and international quality standards. The *Make in India* online brochure published on the eve of the April 2015 international trade fair Hanover Messe in Hanover, Germany, enunciates India's plans for a graduated scale in the FDI ceiling. This contentious issue will require India to process its FDI policy logically and judiciously.

Similarly, India needs to work on offset requirements, which, if carefully orchestrated, could be immensely helpful in growing industry capability. If offset requirements are too arduous or narrow, the interest on the part of companies so diminishes that alignment with strategic intent is lost. The bottom line, as Carter has emphasized, is that the U.S.-India provisions must make good economic and strategic sense for companies to participate. The challenge, as he pinpoints it, is to identify the right companies and ensure that absorptive capacity is there to apply or use the technology being transferred.

Absorptive capacity also implies that there should be administrative structures that manage and oversee integration of technology development, production and acquisition to ensure success in co-production and co-development. Carter believes that such changes in all these areas could be a real help.

During the interview with Keith Webster, OUSD(AT&L) Director for International Cooperation, the author learned firsthand that DoD has instituted special training programs to train Indian officials in U.S. operations in all domains. Training is arranged through the United States' National Defense University and other notable institutions to raise the U.S.-India relationship to the next level for building manufacturing capacity, design and engineering services, and more. To the U.S. administration, India is a "Global Partner" and "Indispensable Partner." However, India has yet to realize its potential in this regard and the U.S. strategic partnership with India seeks to help India do so.

As the main architect of the India-U.S. Defense Technology and Trade Initiative (DTTI), Secretary Carter is a staunch advocate of treating India the same as some of the closest U.S. partners in terms of technology transfer, co-development, co-production and collaborative ventures, expedited approval process for licenses, etc. Under his leadership, the Pentagon, with its special India team, is ready to help senior officials cut through their own bureaucracy. DTTI, conceived to enhance the U.S.-India defense relationship, emphasizes co-production, co-development, procurement, and sale in defense sector, with sensitivity to offset clause requirements and to provide transparency in defense trade. The degree to which the United States and India can meet each other's strategic requirements and make necessary compromises will prove decisive to the future of this relationship.

During his June 2015 visit to India, Carter finalized the details of two small research projects that the American and Indian militaries would conduct together. These projects are very small, but their importance could be significant, depending on their outcomes. The expectation, say U.S. officials accompanying Carter on the visit, is that Washington and New Delhi will become accustomed to working with each other through these small, initial projects.

The author can be contacted at **amaitra@emerging-solutions.us**.

FREE ONLINE SUBSCRIPTION

☐ *Defense ARJ* ☐ *Defense AT&L*

Thank you for your interest in *Defense AT&L* magazine and *Defense Acquisition Research Journal*. To receive your complimentary online subscription, please answer all questions below—incomplete forms cannot be processed.

*When registering, please do not include your rank, grade, service, or other personal identifiers.

☐ *New Online Subscription*

☐ *Cancellation*

☐ *Change of E-mail Address*

Date

Last Name: _____

First Name: _____

Day/Work Phone: _____

E-mail Address: _____

Signature: (Required) _____

PLEASE FAX TO: 703-805-2917, or

E-MAIL TO: datlonline@dau.mil

The Privacy Act and Freedom of Information Act

In accordance with the Privacy Act and Freedom of Information Act, we will only contact you regarding your *Defense ARJ* and *Defense AT&L* subscription. If you provide us with your business e-mail address, you may become part of a mailing list we are required to provide to other agencies who request the lists as public information. If you prefer not to be part of these lists, please use your personal e-mail address.

SUBSCRIPTION

Defense AT&L

Writers' Guidelines in Brief

Purpose
Defense AT&L is a bimonthly magazine published by DAU Press, Defense Acquisition University, for senior military personnel, civilians, defense contractors and defense industry professionals in program management and the acquisition, technology and logistics workforce.

Submission Procedures
Submit articles by e-mail to datl@dau.mil. Submissions must include each author's name, mailing address, office phone number, e-mail address, and brief biographical statement. Each must also be accompanied by a copyright release. For each article submitted, please include three to four keywords that can be used to facilitate Web and data base searches.

Receipt of your submission will be acknowledged in 5 working days. You will be notified of our publication decision in 2 to 3 weeks. All decisions are final.

Deadlines
Note: If the magazine fills up before the author deadline, submissions are considered for the following issue.

Issue	Author Deadline
January–February	1 October
March–April	1 December
May–June	1 February
July–August	1 April
September–October	1 June
November–December	1 August

Audience
Defense AT&L readers are mainly acquisition professionals serving in career positions covered by the Defense Acquisition Workforce Improvement Act (DAWIA) or industry equivalent.

Style
Defense AT&L prints feature stories focusing on real people and events. The magazine seeks articles that reflect author experiences in and thoughts about acquisition rather than pages of researched information. Articles should discuss the individual's experience with problems and solutions in acquisition, contracting, logistics, or program management, or with emerging trends.

The magazine does not print academic papers; fact sheets; technical papers; white papers; or articles with footnotes, endnotes, or references. Manuscripts meeting any of those criteria are more suitable for DAU's journal, *Defense Acquisition Research Journal (ARJ)*.

Defense AT&L does not reprint from other publications. Please do not submit manuscripts that have appeared elsewhere. *Defense AT&L* does not publish endorsements of products for sale.

Length
Articles should be 1,500–2,500 words.

Format
Send submissions via e-mail as Microsoft Word attachments.

Graphics
Do not embed photographs or charts in the manuscript. Digital files of photos or graphics should be sent as e-mail attachments. **Each figure or chart must be saved as a separate file in the original software format in which it was created.**

TIF or JPEG files must have a resolution of 300 pixels per inch; enhanced resolutions are not acceptable; and images downloaded from the Web are not of adequate quality for reproduction. Detailed tables and charts are not accepted for publication because they will be illegible when reduced to fit at most one-third of a magazine page.

Right to Use Illustrations
Non-DoD photos and graphics are printed only with written permission from the source. It is the author's responsibility to obtain and submit permission with the article. **Do not include any classified information.**

Author Information
Contact and biographical information will be included with each article selected for publication. Please include the following information with your submission: name, position title, department, institution, address, phone number and e-mail address. Also, please supply a short biographical statement, not to exceed 25 words. We do not print author bio photographs.

Copyright
All articles require a signed Work of the U.S. Government/Copyright Release form, available at http://www.dau.mil/pubscats/pages/defenseatl.aspx. Fill out, sign, scan and e-mail it to datl@dau.mil or fax it to 703-805-2917, Attn: Defense AT&L.

Alternatively, you may submit a written release from the major command (normally the public affairs office) indicating the author is releasing the article to *Defense AT&L* for publication without restriction.

The Defense Acquisition University does not accept copyrighted material for publication in *Defense AT&L*. Articles will be considered only if they are unrestricted. This is in keeping with the University's policy that our publications be fully accessible to the public without restriction. All articles are in the public domain and posted to the University's website, www.dau.mil.