

www.dau.mil | January-February 2015



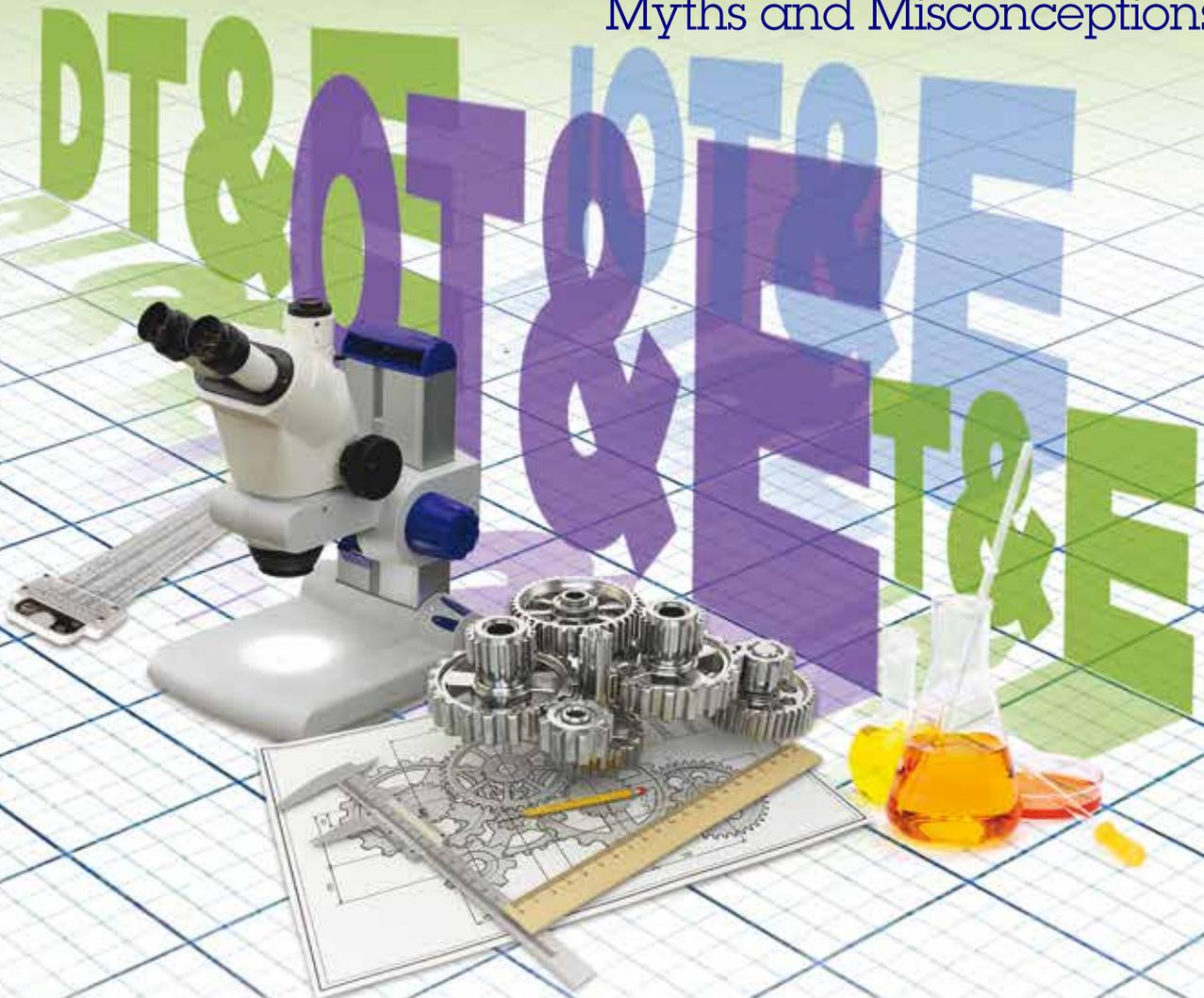
*Defense*

# AT&L

Acquisition, Technology and Logistics

A PUBLICATION OF THE DEFENSE ACQUISITION UNIVERSITY

## Test and Evaluation Myths and Misconceptions



### **Risk and Risk Mitigation—Don't Be a Spectator**

by the Under Secretary of  
Defense for Acquisition,  
Technology, and Logistics

### **The 21st-Century Acquisition Leader**

**A Contract That  
Manages Itself  
The Time Has Arrived**

**Performance  
Based Logistics  
For Achieving  
Affordable Readiness**

# CONTENTS



# 2

From the Under Secretary of Defense for Acquisition,  
Technology, and Logistics

## **Risk and Risk Mitigation—Don't Be a Spectator**

Frank Kendall

# 6



### **Test and Evaluation**

#### ***Myths and Misconceptions***

Steve Hutchison, Ph.D.

Getting to the truth perhaps can help reduce the tension between testers and developers and help acquisition programs deliver capabilities.

# 13



### **The 21st-Century Acquisition Leader**

Paul E. Turner

Constantly changing technology and a diverse workforce require new and challenging leadership qualities.

# 16



### **A Contract That Manages Itself *The Time Has Arrived***

Russell Chesebro

In today's information technology environment, smart contracts can become dynamic and self-directing rather than static documents.

# 20



### **Performance Based Logistics**

#### ***For Achieving Affordable Readiness***

Betsy Lederer and Knob Moses

Using an outcome-based sustainment strategy, Performance Based Logistics offers a well-tested contribution to meeting the Defense Department's budgetary challenges.

# 24



### **Defense Exportability Features Initiative**

#### ***A New Paradigm for International Cooperation***

Frank D. Kenlon and Jay Mandelbaum

To facilitate transfers, program managers now must consider developing and incorporating features into systems likely to be exported.

# 29



### **What Program Managers Need to Know**

#### ***A New Book to Accelerate Acquisition Competence***

Col. William T. Cooley and Brian C. Ruhm

A new guide provides practical advice across the range of diverse topics and issues with which a program manager needs familiarity.

# 32



### **Swamped by Regulations**

#### ***Perils of an Ever-Increasing Burden***

Allen Friar

Published regulations have been at historic levels for the last decade, posing for many small businesses a serious barrier to participation in the federal procurement process.

# 36



## Why I Won't Be a Prime Contractor

*John Krieger*

Requirements involved in contracting with the government contrast strikingly with those that pertain to contracting in the private sector.

# 40



## The Modular Instrumentation Family

*Defense and Industry Applications*

*Gerome Q. Banks*

The "multi-commodity" approach to testing at Aberdeen Proving Ground strives for enhanced economies and effectiveness by utilizing a common instrumentation set across an entire platform.



Defense

# AT&L

Vol XLIV

No. 1, DAU 242

Published by the  
**DEFENSE ACQUISITION UNIVERSITY**

*Under Secretary of Defense for Acquisition, Technology, and Logistics*  
Frank Kendall

*Assistant Secretary of Defense for Acquisition*  
Katharina G. McFarland

*DAU President*  
James P. Woolsey

*DAU Chief of Staff*  
Joseph Johnson

*Director, DAU Operations Support Group*  
Leo Filipowicz

*Director, DAU Visual Arts and Press*  
Randy Weekes

**Defense AT&L Editorial Staff**

*Managing Editor/Senior Editor, DAU Press*  
Benjamin Tyree

*Online Content Editor*  
Collie J. Johnson

*Assistant Art Director*  
Tia Gray

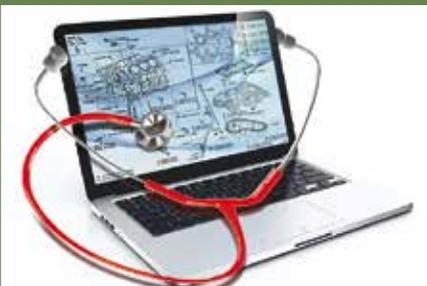
*Production Manager*  
Frances Battle

*Copy Editor/  
Circulation Manager*  
Debbie Gonzalez

*Art Director*  
Harambee Dennis

*Editorial Support*  
Noelia Gamboa  
Michael Shoemaker

# 45

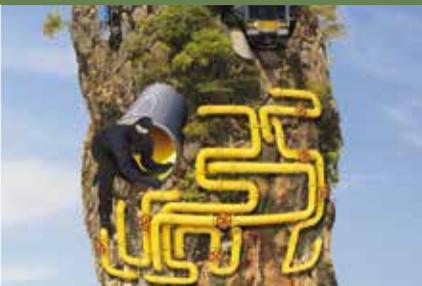


## Repair, Replace or Throw Away Linking Sustainment Strategies to Data Requirements

*William Decker and Julianne Nelson, Ph.D.*

The linkage between program architecture, data rights and sustainment strategies is explored to understand how initial decisions in those areas affect future procurement and sustainment.

# 50



## Securing Cyber Acquisitions

*Michael Cook*

Many challenges emerge along with new technology, such as securing against theft the integrity and confidentiality of data and the critical U.S. defense infrastructure.

## ALSO

**5** MDAP/MAIS Program Manager Changes

**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](mailto:datl@dau.mil) or by phone to 703-805-4282 or DSN 655-4282.

**Subscribe/unsubscribe/change of address:** Fill out, sign, and mail the postage-free self-mailer form at the back of this issue, or download the form at <<http://www.dau.mil/pubscats/pages/defenseatl.aspx>>.

### 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

### Disclaimer

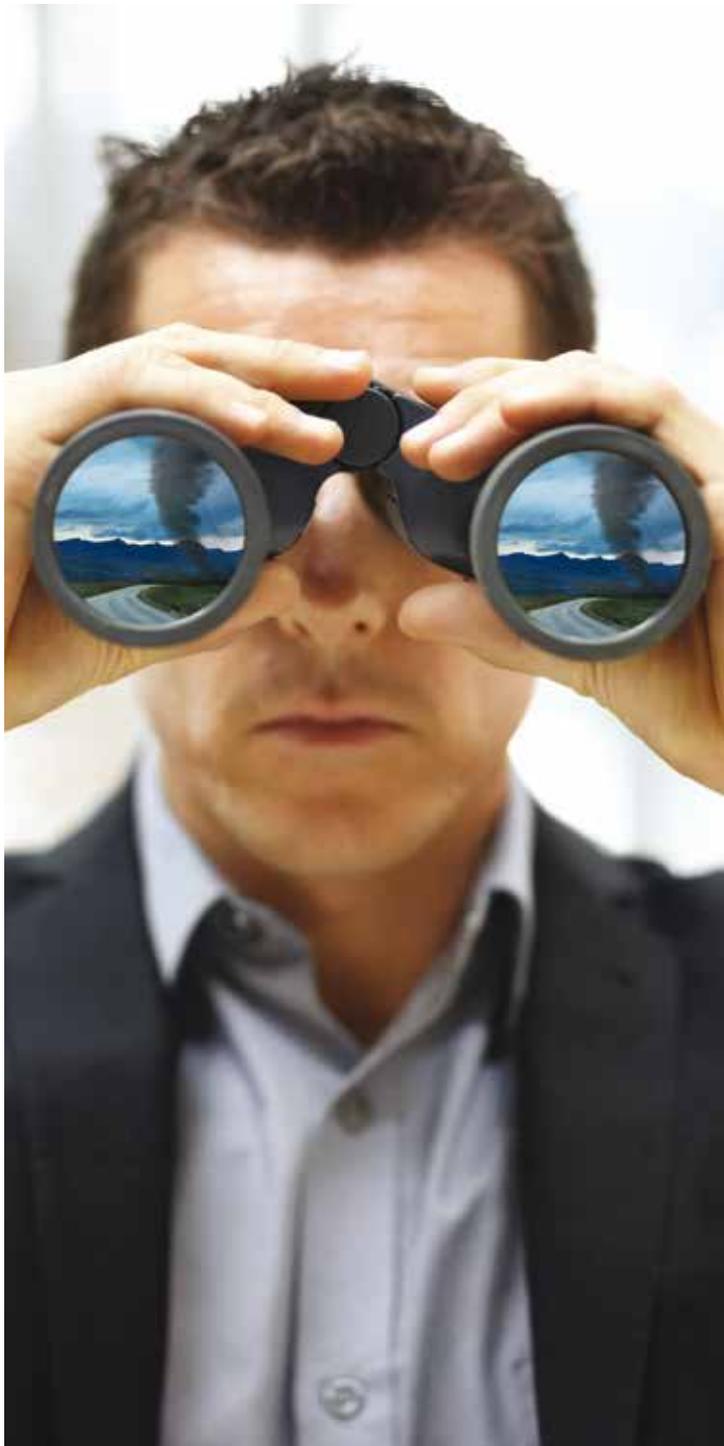
Statements of fact or opinion appearing in *Defense AT&L* are solely those of the authors and are not necessarily endorsed by the Department of Defense, the Office of the Under Secretary of Defense, Acquisition, Technology and Logistics, or the Defense Acquisition University. Articles are in the public domain and may be reprinted or posted on the Internet. When reprinting, please credit the author and *Defense AT&L*.

Some photos appearing in this publication may be digitally enhanced.



# Risk and Risk Mitigation— Don't Be a Spectator

Frank Kendall



As I have watched programs come through for Milestone Decisions and other reviews, I have gained the impression that our processes for risk management may have focused too much on the process and not enough on the substance of identifying and controlling risk. I think I may be seeing risk identification—categorization in the “risk matrix” showing likelihood and consequence and with risk burn-down schedules tied to program events. From my perspective, this by itself isn’t risk management; it is risk watching. We need to do what we can to manage and control risk, not just observe it.

All programs, but particularly all development programs, involve risk. There is risk in doing anything for the first time, and all new product developments involve doing something for the first time. The Department of Defense (DoD) has a good tool that lays out in detail the process of identifying, evaluating, categorizing and planning for risk in programs. Recently updated to version 7.0 by our Chief Systems Engineer Dr. Steve Welby, it is called the *Department of Defense Risk Management Guide for Defense Acquisition Programs* and is available online at <https://acc.dau.mil/rm-guidebook>. I don’t want to duplicate that material here, but I would like to make some comments on the substance of risk identification and risk mitigation and how it drives—or should drive—program structure and content.

I think of every development program primarily as a problem of risk management. Each program has what I call a risk profile that changes over time. Think of the risk profile as a graph of the amount of uncertainty about a program’s outcomes. As we progress through the phases of a program—defining requirements, conducting trade studies, defining concepts and preliminary designs, completing detailed designs, building prototypes and conducting tests—what we really are doing is removing uncertainty from the program. That uncertainty encompasses the performance of the product, its cost and how



**Our task as  
managers involves  
optimization—  
what are the  
highest-payoff  
risk-mitigation  
investments we  
can make with the  
resources available?**

much time is needed to develop and produce the product. We can be surprised at any point in this process. Some surprises can be handled in stride, and some may lead to major setbacks and a restructuring or even cancellation of the program. It is our job to anticipate those surprises, assess their likelihood and their impacts and, most of all, do something either to prevent them or, if they do occur, to limit their impacts. All this effort is risk management.

As managers, we can take a number of proactive measures to mitigate risk. These measures all tend to have one thing in common: They are not free. In our resource-constrained world, we can't do everything possible to mitigate risk. The things we can do cover a wide spectrum: We can carry competitors through risk reduction or even development for production, we can pursue multiple technical approaches to the same goal, we can provide alternative lower-performance solutions that also carry lower risks, we can stretch schedule by slowing or delaying some program activities until risk is reduced and we can provide strong incentives to industry to achieve our most difficult program challenges. Our task as managers involves optimization—what are the highest-payoff risk-mitigation investments we can make with the resources available? I expect our managers to demonstrate that they have analyzed this problem and made good judgments about how best to use the resources they have to mitigate the program's risk. This activity starts when the program plan is just beginning.

The most important decisions to control risk are made in the earliest stages of program planning. Very early in our planning, we determine the basic program structure, whether we will have a dedicated risk reduction phase, what basic contract types we will use, our criteria for entering design for production and for entering production itself, and how much time and money we will need to execute the program. Once these decisions are in place, the rest is details—important but much less consequential. As I've written before, these decisions should be guided not by an arbitrary process or best practice but by the nature of the specific product we intend to design and build.

What we call "requirements" determines a great deal—almost everything—about the risks we need to manage. Do the requirements call for a product like an Mine-Resistant Ambush Protected vehicle, which is basically a heavy truck built from existing off-the-shelf components? Or do they call for a Joint Strike Fighter built from all new design subsystems and much greater capability and complexity than anything we have ever built? In the first case, we probably can go directly into detailed design for production. In the second case, we need to spend years maturing the highest risk elements of the design, and it would be wise to build prototypes to reduce integration and

performance risk before our performance requirements are made final and we start designing for production.

The contracting approach, fixed price or cost plus, is driven by risk considerations. We need to be careful about the illusion that all risk can be transferred to industry. This is never the case, even in a firm fixed-price contract. The risk that the contractor will not deliver the product is always borne by the government. We are the ones who need the product. Industry's risk is always limited to the costs a firm can absorb—a very finite parameter. There certainly are cases where we should use fixed-price contracts for product development (the Air Force's new KC-46 refueling and transport tanker is an example), but we should limit such contracts to situations where we have good reason to believe industry can perform as expected and where the risk is not more than the contractor can reasonably bear.

As a risk-mitigation measure, cost-plus development has a very attractive feature from the risk-management perspective—its flexibility. In a fixed-price environment, the government should have defined the deliverables clearly and should not make changes or direct the contractor about how to do the work. In a fixed-price world, we have chosen to transfer that responsibility to the contractor. In a cost-plus environment, the government can be (and should be) involved in cost-effectiveness trades that affect requirements and in decisions about investments in risk-mitigation measures. These decisions affect cost and schedule, and in a cost-plus environment the government has the flexibility to make those trade-offs without being required to renegotiate or modify the contract.

At certain points in programs, we make decisions to commit both time and funding to achieving certain goals. Sometimes

the commitments include several years of work and require spending billions of dollars. These are the milestones and decision points we are all familiar with in the acquisition process. These milestones and decision points are critical risk-management events. At each of these points, we need a thorough understanding of the risks we face and a clear plan to manage those risks. Understanding these risks is rooted in a deep understanding of the nature of the product we are building.

The nature of the product should determine whether a dedicated technology maturation and risk-reduction phase is needed and what will have to be accomplished in that phase. Although they can be useful indicators, we can't rely solely on metrics like Technology Readiness Levels (TRLs) to make these decisions for us. A bureaucrat can determine if something meets the definition of TRL 6 or not. It takes a competent engineer (in the right discipline) to determine if a technology is too immature and risky to be incorporated into a design for production. The nature of the product also should determine whether system-level prototypes are necessary to reduce integration risk prior to making the commitment to design for production. We did not need those prototypes on the new Marine 1 helicopter. We did need them on the F-22 and the F-35 fighter aircraft.

One risk-mitigation rule of thumb for program planning is to do the hard things first. In the Comanche helicopter program during the 1990s, the Army didn't have enough funding to mature both the mission equipment package and the airframe. The choice was made to build prototype airframes—the lower-risk and less ambitious part of the program. This was done (over my objections at the time), because it was believed that, without flying prototypes, the program risked cancellation for political reasons. In other words, political risk trumped development risk. It didn't work, and the program ultimately was canceled anyway. I do not advocate this approach; there are other ways to deal with political risk. In general, we should do the hardest things as early as we can in acquisition program planning. Eat your spinach first; it makes the rest of the meal taste much better.

Preferably, we should do the hardest (most risky) things in a Technology Maturation Risk Reduction (TMRR) phase where the risk can be reduced with a lower financial commitment and with less severe consequences. Once Engineering and Manufacturing Development (EMD) begins, a program quickly has a marching army moving forward in a broad synchronized plan of work. When something goes wrong, that marching army often will mark time while it waits for the problem to be solved—an expensive proposition. We recently had a problem with the F-35 engine that led first to grounding the fleet and then to a restricted flight envelope. All this delayed the test program, and the effects rippled through much of the EMD effort. It would have been much

better to have found this problem before it could disrupt the entire flight test program.

Within either a TMRR or EMD phase, we should structure workflow to reduce or realize as early as possible the likelier and more consequential risks. Risk should influence program planning details. We can use internal "knowledge points" to inform commitments within phases. Our chief developmental tester, Dave Brown, emphasizes "shifting left" in test planning. The benefits of this are that technical performance uncertainty is reduced as early as possible and that the consequences of realized risks are less severe in terms of lost work, rework or program disruption.

The major commitment to enter production should be driven primarily by achieving confidence in the stability of the product's design, at least as regards any major changes. The key risk to manage here is that of discovering major design changes are required after the production line is up and running. This always is a trade-off; time to market does matter and our warfighters need the product we are developing. How much overlap is acceptable in development and production (concurrency) is a judgment call, but it is driven by an assessment of the risks of a major design problem that will require correction—and the consequences of such a discovery. We recently had a fatigue failure in an F-35 bulkhead, a major structural member. We are in our eighth year of production. Fortunately, in this case, a reasonable cost fix seems viable, and we should be able to modify at modest cost the aircraft we already have built. I say "should be" because the fix will take time to verify through testing, and there remains some risk that the fix will be ineffective.

For all our major commitments, but particularly for exiting TMRR and for entering production, I demand specific accomplishments as criteria and I put them in Acquisition Decision Memoranda. The pressures are very high in our system to move forward, to spend the money appropriated and to preserve the appearance of progress. I recommend that this practice of setting specific criteria for work package initiation (or other resource, work-scope expansion or contractual commitments) be used internally throughout our programs. By setting these criteria objectively and in the absence of the pressure of the moment, I believe we can make better decisions about program commitments and better control the risks we face. Delaying a commitment has impacts now; gambling that things will work out has impacts in the future. It often is tempting for managers under cost and schedule pressures to accept risk and continue as planned. We are paid to get these judgments right—and to have the courage to make the harder decision when we believe it is the right decision.

A source of risk nearly all programs face is uncertainty about external dependencies, often in the form of interfaces with

other programs that may not themselves be defined or stable. In other cases, a companion program (user equipment for the satellite Global Positioning System, for example) may be needed to make the system itself viable or useful, but that program experiences its own risks that affect schedule and performance. We often expect program managers to coordinate with each other, but in many cases this isn't enough. Controlling potential cyber vulnerabilities across program interfaces is a good example of an area in which we have problems. No affected program manager may be willing to change or have any incentive to adjust his or her program to bring it into synchronization with the other programs. If there is a negative cost or schedule impact, the question always is, "Who will change and who will bear the cost of any needed adjustments?" I'm of the view that the DoD could do a better job at managing this type of risk. We can do so by establishing an appropriate technical authority with directive control over interfaces and program synchronization.

The sources of some of our greatest risks can go unnoticed and unchallenged. Gary Bliss, director of my Program Assessment and Root Cause Analysis Office, has introduced the concept of "framing assumptions" into our lexicon. One example of a framing assumption, again on the F-35, was that modeling and simulation were so good that actual physical testing wasn't necessary to verify performance prior to the start of production. In the case of the Littoral Combat Ship, the assumption was that commercial construction standards were adequate to guide the design. Gary's point, and it's a good one, is that programs often get into trouble when framing assumptions prove invalid. However, these assumptions are so ingrained and established in our thinking that they are not challenged or fully appreciated as risks until reality rears its ugly head in a very visible way. This type of risk can be mitigated by acknowledging that the assumptions exist and by providing avenues for us to become aware of sources of evidence that the assumptions may not be valid. Our human tendency is to reject evidence that doesn't agree with our preconceptions.

Gary found several cases where program management failed to recognize as early as it should have that core framing assumptions were false. The best way to manage this source of uncertainty is to take the time and effort during early program planning to identify a program's framing assumptions, to understand that they are a source of risk and then to actively reexamine them for validity as more information becomes available. Again, "knowledge points" can be helpful, but we shouldn't merely be passive about this. In our planning, we should create knowledge points as early as possible. If we do so, we can respond to any problems that emerge sooner rather than later.

I'll conclude by reiterating two key points: Risk management is not a passive activity, and proactive risk-management invest-

ments are not free. Those investments, however, can be the most important resource allocations we make in our programs. As managers, we need to attack risk the way we've been attacking cost. Understand risk thoroughly, and then go after the risk items with the highest combined likelihoods and consequences and bring them under control. Allocate your scarce resources so you achieve the highest possible return for your investments in risk reduction. Do this most of all at the very start of program planning. The course set then will determine the direction of the balance of the program and whether it succeeds or fails. 

## 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 changes of leadership for both civilian and military program managers in recent months.

### **Army**

**Col. James W. Schirmer** relieved **Col. William H. Sheehy** as project manager for the Paladin Integrated Management (PIM) Program on July 30.

**Col. Michael W. Milner** relieved **Col. William H. Sheehy** as project manager for the Armored Multi-Purpose Vehicle (AMPV) Program on Aug. 28.

### **Navy/Marine Corps**

**Capt. Jeffrey S. Dodge** relieved **Capt. Patrick W. Smith** as program manager for Multi-Mission Tactical Unmanned Aircraft System (PMA-266) on Oct. 16.

**Capt. James G. Stoneman** relieved **Capt. John K. Martins** as program manager for Air to Air Missile Systems (PMA-259) on Oct. 9.

**Col. Robert D. Pridgen** relieved **Capt. Gordon D. Peters** as program manager for Presidential Helicopter Fleet Replacement Program (PMA-274) on July 2.

### **Air Force**

**Col. Michael A. Guetlein** relieved **Col. James B. Planeaux** as program manager for the Space Based Infrared System (SBIRS) program on Sept. 8.

# Test and Evaluation

## Myths and Misconceptions

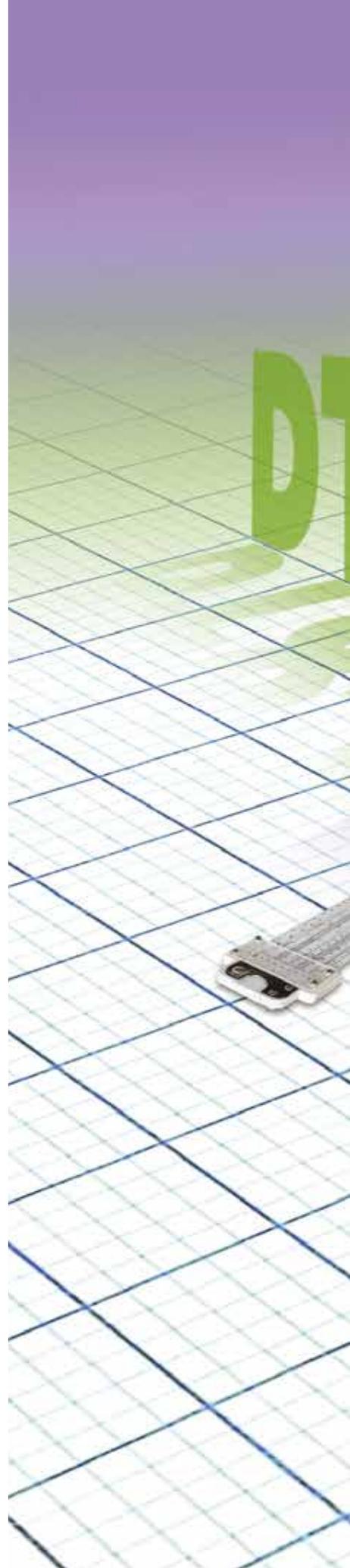
Steve Hutchison, Ph.D.

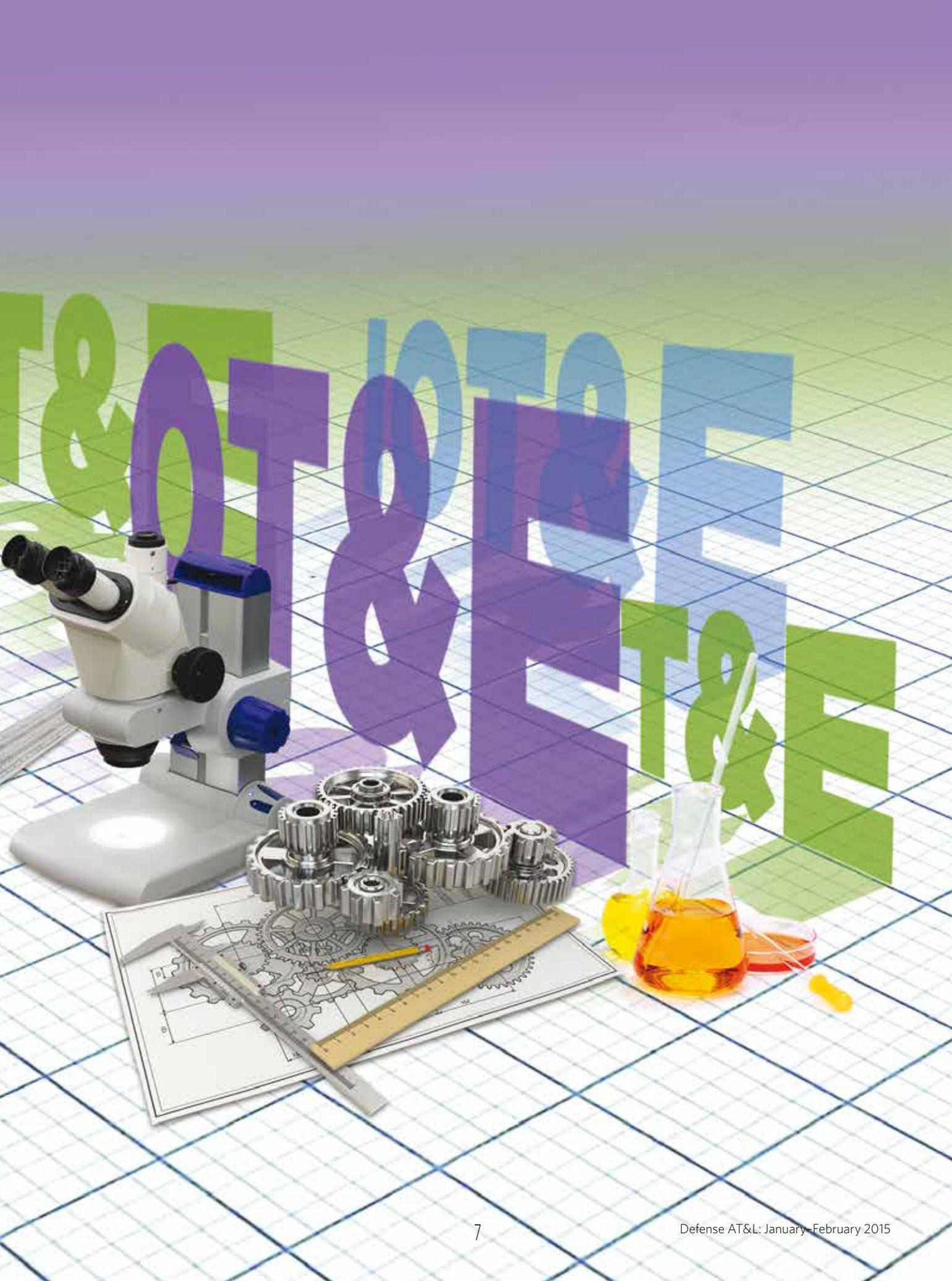
**T**est and Evaluation (T&E) is essential to successful system acquisition. For the last 43 years, the Office of the Secretary of Defense (OSD) has included various formations providing T&E oversight. Interested readers can review some of the history in the articles “The Original DT&E” and “What Happened to DT&E?” in the January–February 2014 and March–April 2014 issues, respectively, of the *Defense AT&L* magazine. Having been witness to just over a third of this history, I thought I would share some of the great myths and misconceptions about T&E that I have observed over the years. If we can dispel some of these myths, perhaps we can reduce the tension between testers and developers and get on with helping acquisition programs deliver capabilities more effectively and efficiently. After all, the Department of Defense (DoD) is not investing the nation’s resources for programs to fail—our job as testers is to help programs succeed.

That actually might be one of the myths—that, because some testers are “independent,” they actually are not supposed to “help” programs. I am going to take it on faith that most testers don’t actually believe that; rather, even the most independent test organizations understand that it doesn’t take a lot of talent to show up at the end of system development and point out the flaws. Instead, programs maximize their T&E Return on Investment (ROI) when their testers are engaged early, run meaningful tests and provide quick feedback to help move the program forward, not act as gatekeepers to block progress (the source of this idea is the book *Agile Testing: A Practical Guide for Testers and Agile Teams* by Lisa Crispin and Janet Gregory). The hard work of testing is not gatekeeping—it’s providing constructive feedback. With that out of the way, I’ll briefly count down my top five myths in T&E, and offer some thoughts on how to resolve them.

---

**Hutchison** is director of test and evaluation for the Department of Homeland Security and previously served as the principal deputy for developmental test and evaluation in the Office of the Secretary of Defense.





**Myth No. 5: Only Operational T&E Matters**

Many programs base their acquisition strategy on the belief that the only T&E that matters to decision makers is Operational Test and Evaluation (OT&E); after all, it's written in law—therefore, it must be the only T&E that matters. Title 10 USC §2399 “Operational test and evaluation of defense acquisition programs” stipulates that the Secretary of Defense may not permit Major Defense Acquisition Programs (MDAPs) to proceed beyond Low-Rate Initial Production (LRIP) until initial OT&E (or IOT&E) is completed and the Director of Operational Test and Evaluation (DOT&E) has submitted a report (commonly referred to as the “BLRIP report” [the B stands for “beyond”]), stating whether the operational test was adequate and the results confirm that the system is effective and suitable. Obviously, there is value in operational testing, particularly as the confirmatory activity stated above. However, the problem with this mandate is that it puts OT&E and the DOT&E in a gatekeeping role. Missing are the checks and balances prior to the start of production; in other words, feedback to programs is missing when it is needed most.

Once a program has formally entered the acquisition process, I would argue that the most important decision in the program life cycle is the decision to begin production. Program managers need to have it right at production start because, once the decision is made to begin production, designs are essentially locked and production fixtures set. If programs have not discovered and corrected design problems or key failure modes earlier, those problems will almost certainly become the warfighter's problems, because it will cost too much to correct them, and the tyranny of the urgent will demand that the capability get to the field. Permitting development problems to become the warfighter's problems is the real definition of acquisition malpractice. Thus, if you accept the premise that the most important decision is entry into production, then the T&E that matters most must inform that decision.

In the DoD process shown in Figure 1, the decision to begin production typically is made to authorize LRIP at Milestone C. Since 10 U.S.C. §2399 requires IOT&E to inform the full-rate production decision, acquisition decision authorities must rely on Developmental Test and Evaluation (DT&E) to inform the Milestone C decision. If programs get it right at production start, then OT&E will be that confirmatory activity described above rather than a discovery activity that tarnishes most operational test outcomes today.

There are a couple corollaries to this myth. They include:

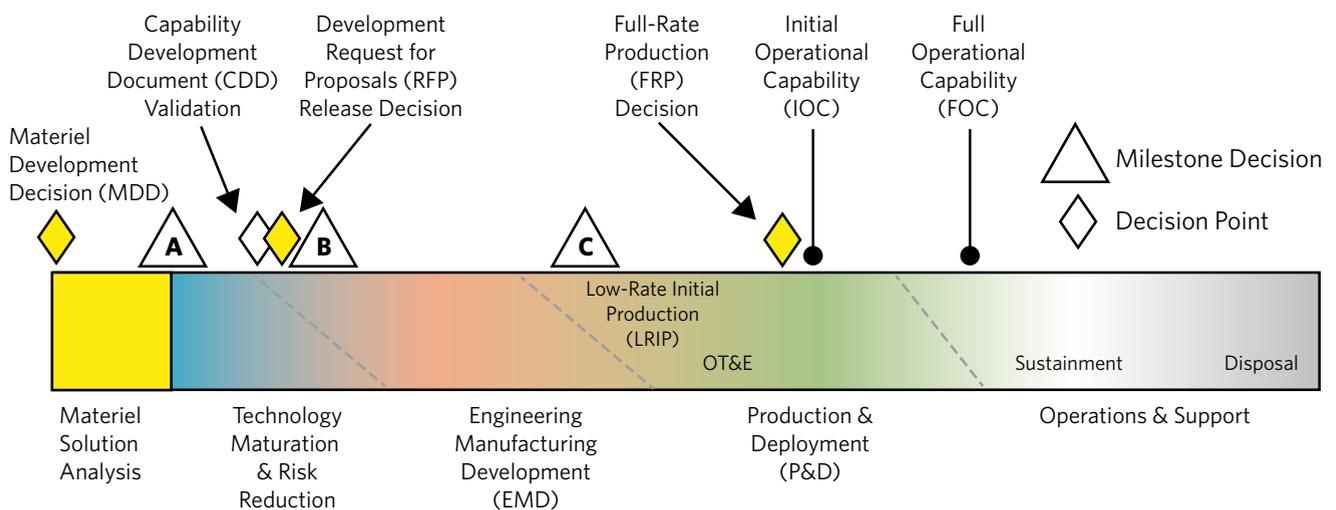
- Corollary 1: DT&E is technical testing.
- Corollary 2: Users aren't involved in DT&E.

These are the leading contenders for what I would call “T&E malpractice” and the reason so many programs discover problems during OT&E; hence the rallying cry to “shift left!” DT&E should never be considered just technical testing. Sad to say though, this is not myth. The *Glossary of Defense Acquisition Terms*, 15th Edition, December 2012, defines DT&E as:

Any engineering-type test used to verify status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial operational testing (see the full definition online at <https://dap.dau.mil/glossary/>).

If the developmental tester focuses only on assessing technical performance specified in the contract, programs will completely miss the sense of whether the capability could satisfy user needs in performing the mission. If, however, DT&E has a mission context, not only will programs and decision makers understand the technical issues, they also will obtain user feedback that is essential early in the life cycle, when there is time to adjust course if necessary. Mission context does not mean program managers have to shift the IOT&E to the left,

**Figure 1. DoD Acquisition Life Cycle (Source: Interim DoD Instruction 5000.02)**



but user involvement should be a DT&E priority. Using the Operational Test Agencies (OTAs) to help design and conduct mission-relevant developmental tests with typical operators would be a really good DT&E strategy. Ultimately, DT&E must employ the right resources to provide confidence in the decision to enter production.

#### ***Myth No. 4: Cybersecurity T&E Is Someone Else's Responsibility***

I was an operator once, a boots-on-the-ground infantryman. My radio was perhaps the most valuable weapon in my arsenal; with it, I could change the terms of the current fight and the next engagement. Keeping my communications secure, and therefore keeping my mission parameters secure, was my responsibility. Technology has far exceeded the capability

accreditation of an AIS shall be supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards and a certification report, all approved by the DAA." In today's "risk management framework," the DAA is called an Authorizing Official (AO), and the AO retains responsibility for information security and approves the system authority to operate. To assist with these functions, the AO designates a Security Controls Assessor (SCA) to perform the checks of security controls. The SCA typically is not one of the program's DT&E or OT&E organizations.

The assignment of cybersecurity responsibilities outside mainstream requirements and acquisition channels, not to mention outside the operator's channels, has many downstream

## **The assignment of cybersecurity responsibilities outside mainstream requirements and acquisition channels, not to mention outside the operator's channels, has many downstream impacts.**



of those old radio days, but one thing remains unchanged: Security is an operator's responsibility. In the (dare I say it) "unfamiliar" cyberspace domain, providing "good" cybersecurity may well be today's most challenging development task. As testers, we put ourselves in the operator's boots to answer the "so what" question. So, when it comes to cybersecurity, why do we (sometimes) leave that part of the "so what" question for someone else to answer? It's an artifact of security processes that have become very specialized over the decades.

Beginning in the 1970s, DoD managed the acquisition of information technologies and their security requirements separately from the mainstream Defense Acquisition System and requirements processes. For example, the first DoD Directive (DoDD) 5000 formalized the acquisition process back in July 1971, but in October 1978 the Department issued DoDD 7920.1, Life Cycle Management of Automated Information Systems (AIS), and managed information technology under this separate acquisition process until eventually merging it with the DoDD 5000 in 1996. Security requirements appeared even earlier with the 1972 DoDD 5200.28 Security Requirements for Automatic Data Processing (ADP) Systems, reissued in 1988 as Security Requirements for Automated Information Systems (AISs), eventually becoming today's DoD 8500 series on Cybersecurity and the Risk Management Framework. These directives introduced another decision maker—the Designated Approving Authority (DAA)—with assigned responsibilities, many of which are still in use today. For example, the 1988 directive stated: "The

impacts. Since the modus operandi in the T&E community is to test to requirements, when cybersecurity considerations are absent from operational requirements documents they likely also will be absent in the T&E Master Plan (TEMP), DT&E and OT&E event test plans, and the test reports. The downstream effect is that the "cyber so what" question may not be adequately answered at critical acquisition decision points.

Cybersecurity is an operator's responsibility; therefore, it is incumbent on the T&E community to answer the "cyber so what" question: Does this new capability operate securely in the cyberspace domain? Our challenge is to fully integrate cybersecurity into our test processes to help programs identify risks, minimize the attack surface and reduce kill chain effects to improve resilience. Cybersecurity should be integrated into every test activity and inform acquisition decision making. In the summer of 2013, the Deputy Assistant Secretary of Defense (DASD) for DT&E and the DOT&E offices collaborated to produce a set of procedures for cybersecurity T&E that would go a long way toward helping testers develop and execute such plans and help programs close the gap between authorities to operate and operating securely.

#### ***Myth No 3: OTAs Can't Do DT&E***

OTAs have often told me that they can't do DT&E (as in "not permitted" to do DT&E as opposed to lacking competence to perform DT&E). I'm not sure how this myth came to be, but unless the Component T&E regulations actually prohibit the OTAs from conducting DT&E, then it simply remains a myth that OTAs can't do DT&E.

The idea may have originated as an extension of statutory language limiting DOT&E involvement in DT&E. Specifically, 10 U.S.C. §139 (d) states that the DOT&E “may not be assigned any responsibility for developmental test and evaluation, other than the provision of advice to officials responsible for such testing.” Component acquisition authorities may simply be extending this limitation to their OTAs, perhaps to protect their independence—the idea being that, if an OTA is involved in DT&E, it is not independent. That’s just absurd. Independence seeks to ensure that an agent separate from the developer and user perform the test and evaluation; it has nothing to do with when the tester is involved or the type of testing performed.

the Under Secretary of Defense for Acquisition, Technology, and Logistics MDAPs/major automated information systems (MAIS)/Special Interest list includes 150 programs.

In the wake of the BRDP recommendations, the DoD has focused almost singular emphasis on OT&E (more reason there is Myth No. 5), and DT&E oversight became the glaring deficiency. The Weapons Systems Acquisition Reform Act (WSARA) (PL111-23) of 2009 directed the DoD to establish the office of what is now the DASD (DT&E), and more legislation followed to bring more attention to DT&E. For example, the National Defense Authorization Act for Fiscal Year (FY)

## **In the 21st century, we generally know how to build the machinery that makes things go (or go “bang”); our challenges arise when we connect them to a network.**



Guidance on independence appeared in May 1976 with the issuance of Office of Management and Budget (OMB) Circular A-109, *Major System Acquisitions*. The A-109 established policy that federal agencies acquiring major systems should “provide strong checks and balances by ensuring adequate system test and evaluation” and “conduct such tests and evaluation independent, where practicable, of developer and user.” The A-109 did not make a distinction between DT&E and OT&E; it made a distinction between tester, user and developer.

2012 (PL112-81) requires that each MDAP be supported by “a governmental test agency, serving as lead developmental test and evaluation organization”—in other words, a “DTA.” Thus, OSD has a DOT&E and a DASD(DT&E), and programs have an OTA and a DTA, not to mention the SCA.

To its credit, the DoD had embarked on this course several years earlier. The July 1970 Report of the Blue Ribbon Defense Panel (BRDP) had some very critical findings on OT&E and highlighted the lack of OT&E oversight in OSD as a “glaring deficiency.” Deputy Secretary of Defense David Packard responded by tasking the DoD’s chief acquisition official, the Director of Defense Research and Engineering, to establish a Deputy Director for Test and Evaluation, who would have “across-the-board responsibilities for OSD in test and evaluation matters.” More than a decade later, however, Congress found the reporting relationship between the test overseer and chief acquisition official to be unsatisfactory and created the office of the DOT&E (Public Law 98-94, September 1983), independent of officials in the acquisition decision-making chain.

An alternative and perhaps more efficient approach might have been to revise the statute already in place (i.e., 10 U.S.C. §139) and remove the arbitrary boundary to DT&E, establishing an office whose function is to provide independent T&E oversight throughout the life cycle. Likewise, additional efficiencies can be gained, including actually achieving the elusive “early involvement,” by having the OTAs engaged throughout the life cycle as a program’s independent test agent (ITA versus OTA). As this is entirely consistent with the independence requirement of the A-109, it would improve synchronization of the overall T&E effort, bring needed mission context into early testing and may produce the downstream benefit of reducing the scope of testing later. The Army Test and Evaluation Command, for example, already serves as both OTA and DTA.

There have since been two T&E camps in OSD: operational testers under the DOT&E and developmental testers under the chief acquisition official. Unfortunately, though, considering the relative proportion of DT versus OT during a program life cycle, OSD resources for these offices have shifted significantly out of balance and today are almost exactly opposite of where they need to be, and the DOT&E oversees an acquisition portfolio almost twice as large as DoD’s chief acquisition official. There are 310 programs under DOT&E oversight;

### ***Myth No. 2: Effectiveness and Suitability Completely Describe Today’s Systems***

Having worked in information technology T&E for most my testing career, I have a particular bias for the terms “effective and suitable” used to evaluate systems and inform system acquisition decisions, and it goes something like this: In the 21st century, we generally know how to build the machinery that makes things go (or go “bang”); our challenges arise when we connect them to a network. Interoperability and cybersecurity are today’s chief concerns. I see effectiveness and suitability as industrial-age bins into which we try to stuff information-age issues. I have read countless evaluation plans and test

reports, none of which has a compelling structure where interoperability and cybersecurity fit into the evaluation of effectiveness and suitability; some of them, in fact, do not even address these issues and rely instead on certification agents (i.e., the Joint Interoperability Test Command and SCA) to assess them. More disconcerting, however, is that, because we are obliged to report in terms of effectiveness and suitability, interoperability and cybersecurity are rarely discussed during acquisition decision events.

What about that other bin: survivability? Is cybersecurity part of survivability? In short, survivability is another industrial-age bin that also has a basis in law. First written in Public Law 99-500 in October 1986 (now 10 U.S.C. §2366), realistic survivability testing places "... primary emphasis on testing vulnerability with respect to potential user casualties ..." and is required for "covered systems," which include vehicles, weapon platforms or conventional weapon systems when they have "... features designed to provide some degree of protection to users in combat."

In other words, if the system has features designed to protect the human, it has to be tested to ensure it protects the human. Survivability is about saving lives, not saving data—so cybersecurity is not a good fit in the survivability bin.

When the terms effectiveness, suitability and survivability were written into laws back in the 1980s, the DoD was acquiring information technologies through a separate acquisition process with separate security procedures (see discussion of Myth No. 4), and it is unlikely that anyone foresaw the challenges associated with today's network-enabled technologies. Interoperability and cybersecurity are the developmental challenges that concern me most today, and subordinating them within the effectiveness and suitability model marginalizes their importance and reduces their exposure to decision makers. So let's compromise for today's network-enabled systems: Let us evaluate them based on effectiveness, suitability, interoperability and cybersecurity.

Finally, my No. 1 myth in T&E is:

### **Myth No. 1: The Purpose of DT&E Is To Get Ready for OT&E**

This is what happens when developers, testers and decision makers believe Myth No. 5. Except it's not a myth; it's doctrine written in the DAU *Glossary* (quoted above): "... to certify readiness for initial operational testing." Just like the terms "effectiveness" and "suitability," this is an outdated idea that stuck, and most of our acquisition leaders, program managers and testers describe DT&E in these terms today. At one point, the DASD(DT&E) office even published an "assessment of operational test readiness (AOTR)" and briefed the assessment at operational test readiness reviews. The AOTR had a lot of good information; in fact, it was a very good predictor of the test outcome, but it was too late to help programs positively

affect the outcome. We had to change the value proposition for the DASD(DT&E) office, and change the paradigm of conducting DT to determine readiness for OT. To help programs improve outcomes, we had to shift left and provide the DT&E assessment at the point when the program could act on the information provided—prior to starting production. All tests inform production decisions—build-it or fix-it decisions—and acquisition decisions. The purpose of DT&E is to help programs set the conditions for entry into production.

Figure 1 positions OT&E in accordance with statute to bring data to inform the Full-Rate Production decision. DT&E brings data to inform all the other decisions programs make but with particular emphasis on ensuring readiness to begin production at Milestone C. Ultimately though, this type of DT&E-OT&E "stovepiping" or bureaucratic separation is inherently inefficient. The more effective strategy is to combine what we now think of as DT&E, OT&E, interoperability and cybersecurity testing into an integrated test approach to maximize the ROI of every test activity throughout the life cycle. To help programs reduce discovery of deficiencies late in the life cycle, testers must develop a comprehensive evaluation framework and then formulate a logical sequence of integrated test activities to collect the data needed to answer the so-what questions before commitment to production. When properly planned and executed, integrated testing will enable improved acquisition outcomes.

### **Summary**

We've learned some very important lessons over the last 43 years, and as a result, we do a lot of things very well in T&E. However, we should always look for ways to improve our support to programs and decision makers, and there are a few myths and misconceptions we need to dispel. Program managers understand that T&E is essential to helping move development forward; they are not looking for us to be gatekeepers. There are enough gatekeepers as it is. Rather, program managers look for the T&E community to be engaged throughout the life cycle, to treat every test activity as a shared resource and to provide feedback. However, to maximize their testing ROI, programs must weight the T&E effort early—shift left—to set the conditions for a successful acquisition outcome. We need to work with programs to help them shift left, and bring the same kind of post-LRIP OT&E rigor that we have developed over the years into an integrated T&E approach—and, for today's network-enabled technologies, include tests to help programs deliver not just effective and suitable capabilities but interoperable capabilities that operate securely in the cyber domain. We must also be draconian stewards of the nation's resources and ensure tests support decisions that drive development forward. The paradigm of doing DT&E to get ready for OT&E has had its day, and that day is past. The future of T&E is to be an integrated, life-cycle activity that informs acquisition decisions. And, while independent, we also are a partner because we share the goal of ensuring that development problems do not become the warfighter's problems. 

---

The author can be contacted at [steven.hutchison@hq.dhs.gov](mailto:steven.hutchison@hq.dhs.gov).



# The 21st-Century Acquisition Leader

Paul E. Turner

**A**cquisition leaders of the 21st century face challenges that differ from any previous time in history. A constant change in technology, government financial instability and a diverse workforce require leadership attributes that may seem unattainable.

However, three attributes are crucial to being a successful acquisition leader in the 21st century. These attributes include communicating, empowering and being a servant leader. While this is by no means a complete list, all other attributes build upon these three. Having a vision, collaborating and being transparent also are important qualities.

## Communicate

The ability to communicate efficiently and effectively is important to today's acquisition leader. This may seem simple and obvious, but it is an area that is often the most difficult to master. On climate surveys, communication consistently is the top issue with employees. (Information does not flow or management does not share information are frequent complaints, according to data from an unpublished 2007 study by the author of this article.) It is imperative that leaders develop strong communication skills. To communicate effectively, leaders must learn to simplify their messages so their followers understand what the leader wants. Deborah Blagg and Susan Young, in "What Makes a Good Leader," published by the *Harvard Business School Bulletin* in February 2001, stated that, "You need a talent for simplicity—for saying things in a few words."

**Turner** is director of systems engineering and integration for the Precision Fires Rocket and Missile Systems Program Management Office (PFRMS PMO), Program Executive Office Missiles and Space, U.S. Army. He is responsible for technical oversight and engineering management and leadership of the PFRMS portfolio.



To be able to do this, the leader must understand his followers as well as what those followers can and cannot appreciate. The leader may need to use various examples or props to convey his or her message to the followers. Leaders must communicate on a level that followers understand. Doing so can decrease resistance and increase comprehension on the part of their followers. “[Leaders] understand the people they’re trying to reach and what they can and can’t hear. They send their message in through an open door rather than trying to push it through a wall,” Blagg and Young added.

Communication is not just the leader talking to his or her followers; the leader also must truly listen. Real leaders will listen

happier, more satisfied employees. In addition, empowerment allows an organization to transform itself into a flexible, adaptable and fast-moving entity that can adjust to change rapidly.

The empowerment skills of a 21st-century acquisition leader include asking questions, staying balanced, controlling boundaries and living the vision, values and goals of the organization. By asking productive questions, the leader prompts the team to think about the problems and solidifies the empowerment of individuals; this, in turn, builds their trust. When a leader maintains balance, manages risks, controls distractions and removes boundaries, the team is pushed continually toward its goals, building the confidence of team members in the future



**To communicate effectively, leaders must learn to simplify their messages so their followers understand what the leader wants.**

to what their followers are saying and determine the necessary course of action to address concerns, complaints or suggestions. As communication receivers, both leaders and those they lead must listen as well as speak in order to achieve the desired outcome. Organizations that focus on improving the communication skills of their leaders—through training, connecting with them emotionally, providing a focused message, minimizing the gray areas of their communication and, above all, by being honest—have a better chance of surviving tough times and keeping employees from leaving.

By listening and hearing, the leader builds trust among the followers. Over time, this leads to more commitment to the leader’s vision. The 21st-century acquisition leader must strive for clarity of message and a commitment to listen to his or her followers; in doing so, the leader will develop the followers’ commitment and respect—and that will allow the organization to meet its goals.

### **Empower**

In order to take the organization to the next level, today’s acquisition leader will need to empower his or her employees. According to Golnaz Sadri’s 2011 article, “Empowerment for the bottom line,” published in the Institute of Industrial Engineers’ journal, *Industrial Management*, empowerment refers to “the various ways in which nonmanagerial workers are enabled to make autonomous decisions without consulting a boss, supervisor, or manager.” Empowerment provides a crucial tool in motivating and satisfying employees. By empowering employees, the organization benefits through greater productivity and

and solidifying the vision, values and goals of the organization. Open communication at all levels in an organization creates successful work environments and fuels empowerment. E.D. Staren’s 2009 article on “Optimizing staff motivation” in the *Physician Executive Journal*, reinforced this idea: “staff particularly need to feel empowered ... besides the evident team-building and camaraderie associated with it, effective communication encourages such empowerment.” Encouraging communication at all levels of the organization and listening to the resulting dialogue raises the bar for individual and group performance. The empowerment of the individuals within it allows an organization to be agile, responsive, customer focused, cost effective and flexible.

### **Being a Servant Leader**

In his 2002 book, *Servant Leadership*, Robert K. Greenleaf stated, “Caring for persons, the more able and the less able serving each other, is the rock upon which good society is built.” To be a servant leader, one must also have a strong tendency to empathize with one’s followers. Today’s leader possessing the attributes of a servant leader has the following characteristics: is a voluntary subordinate, has authentic self, has covenantal relationships, has responsible morality, has transcendental spirituality and has a transforming influence.

Voluntary subordination, was described by Sen Sendjaya, James C. Sarros and Joseph C. Santora in their 2008 article, “Defining and measuring servant leadership behavior in organizations” in the *Journal of Management Studies*. They wrote that voluntary subordination is a “willingness to take up

opportunities to serve others whenever there is a legitimate need regardless of the nature of the service, the person served, or the mood of the servant." Because these servant leaders are authentic in their leadership, they are transparent to their followers. A covenantal relationship is the ability of the servant leader to accept followers for who they are, not for how they make the servant leader feel.

This relationship is "an intensely personal bond marked by shared values, open-ended commitment, mutual trust, and concern for the welfare of the other party," according to Sendjaya, Sarros and Santora. These bonds remain strong in times of conflict, because the parties care for each other. The 21st-century servant leaders illustrate moral responsibility when they ensure "that both the ends and the means they employ are morally legitimized, thoughtfully resolved, and ethically justified," the authors added. This responsible morality elevates the ethical culture of the organization and encourages an environment where everyone is doing the moral, ethical and legal things needed to succeed.

A servant leader with transcendental spirituality is "attuned to basic spiritual values and in serving them serves others

including colleagues, the organization and society," Sendjaya and coauthors maintained. This allows the servant leaders to self-motivate and to motivate their followers.

Finally, today's servant leader has a transforming influence. "The personal transformation that servant leaders bring about in others occurs collectively and repeatedly, and in turn, stimulates positive changes in organizations and societies," Sendjaya, Sarros and Santora wrote in their 2008 article.

This transforming influence becomes a force multiplier and allows leaders to transform their followers through the leaders' vision, modeling through personal examples, mentoring and empowering others and developing trust. If leaders will serve their followers, give praise to their followers' talents and empower them, they will, in turn, take the initiative, accept responsibility, volunteer and continually learn to become better leaders themselves. When this happens, the organization as a whole grows. If the 21st-century acquisition leader will develop the attributes of a servant leader, he or she will unleash an energy that will propel the organization to meet the vision. 📧

*The author may be contacted at [paul.e.turner.civ@mail.mil](mailto:paul.e.turner.civ@mail.mil).*



## Where Can You Get the Latest on the **Better Buying Power** Initiatives?

- **BBP Gateway (<https://dap.dau.mil/bbp>)** is your source for the latest information, guidance, and directives on better buying power in defense acquisition
- **BBP Public Site (<https://acc.dau.mil/bbp>)** is your forum to share BBP knowledge and experience

# A Contract That Manages Itself

The Time Has Arrived

*Russell Chesebro*





his article is about change. It is about taking a brave new step in the way contracting is performed within the Department of Defense (DoD) and how contracts are handled.

In fact, this article goes further. The contract will cease being a static document file on a computer server. The contract will manage itself. The contract will have a voice and it will speak. The contract will become empowered, and it will take action apart from human direction. The technology exists to bring the contract to life—and, once the first step on this road is taken, the world of contract administration will leap into the next century. The cost potential savings are so great that they are incalculable.

For those who are intrigued by the opening paragraph, for the skeptics, for everyone with a vested interest in how contract management within the DoD is performed, read on and you won't be disappointed. A computer file has been brought to life and has spoken its first words, "Hello Contracting World." We will never be the same.

In the year 2010, The DoD doled out \$368 billion in contract awards. Each contract award resulted in a physical contract that was turned into a PDF file and stored as a static document on a computer network. How many contractors are supplying goods to DoD? How many of those contractors are still in business? How many unpaid contracts are out there, and how do they get closed if the contractor is no longer in business? How many information-technology (IT) business systems and spreadsheets does the Army use to manage contracts? The Navy? The Air Force? How many static contract files are there for each Service?

---

**Chesebro** has an MBA in Information Technology Management and was a member of the engineering team that created the PDF file.

The Office of the Secretary of Defense (OSD), on its public website for Defense Procurement and Acquisition Policy, lists nine software tools/websites that contractors can use for eBusiness. That is just one portion of the conglomeration of IT business systems used for managing DoD acquisition. But what is the essence of acquisition? It is a contract. Currently, contracts reside as static files on one or more IT business systems. These contracts are accessed by scores of people, all of whom have their own interest in the contract information and perform varied functions of contract management.

With so many people handling so many contracts on so many various IT business systems, how can that be managed? This is what is referred to as a wicked problem. A wicked problem is one that cannot be solved but must be continually managed. Some examples of wicked problems are poverty, disease, hurricanes and war. Trying to manage \$368 billion worth of contracts across the different branches of Service within the DoD is a wicked problem. Breaking that problem down into smaller problems reveals an interesting pattern.

***Wicked Problem No. 1: Data Integrity. A contract that is a static file can be copied, amended and stored in many different locations and versions.***

The first small problem to look at is that of one contract residing on multiple systems in multiple locations. Although the contract may be the same in its original form, not all modifications will be synchronized across the multiple systems. That leaves a contract in many different states and—depending on which system a person uses to access the contract—will result in getting a correct or incorrect version of that contract.

***Wicked Problem No. 2: Factoids. A static-file contract is dependent on institutionalized knowledge.***

The second problem to note is one of institutionalized knowledge. Perhaps there is a contract that cannot be closed because there is an unpaid amount of \$3.50. The company to whom the money is to be paid no longer is in business and the only person with the knowledge to close out contracts such as this retired last year. The contract then becomes an unresolved problem that will require extra labor costs to resolve.

These two wicked problems revolve around one reality: The contract is a static file managed by humans. In an age in which airplanes fly themselves and cars drive themselves, it is time to create a contract that manages itself. Contracting challenges technology and, in turn, technology inspires contracting.

## **The Smart Contract**

The paradigm of a contract as a static document is about to change. The days of a contract being read, interpreted, acted upon and managed by contracting personnel is over. We don't need people to manage contracts because contracts can manage themselves. This concept was first discovered in 2014 at the Defense Contract Management Agency (DCMA)

Contract Management Office (CMO) in Philadelphia, Pennsylvania. Having one contract reviewed by many people is an inefficient use of time and resources. In these days of tightening federal budgets, efficiency is of paramount importance in order for an organization to perform its mission.

## **The Smart Contract as an Object**

In discussions about programming, the word "object" means a component with properties and methods. Properties are what an object knows about itself and methods are what an object knows it can do. A contract, as an object, will know things about itself. It will know how much it is worth. It will know who signed the contract, who administers the contract and when the contract is supposed to be complete. With a little additional development in the environment in which the contract object (smart contract) exists, the contract will be able to interact with other objects. That will enable the contract to know how much money has been paid to the contractor and how much is left. The contract will know how to close itself out. And if a problem arises, such as funds still not spent with the contractor no longer in business, the contract will know how to handle the situation. Among its many advantages, the smart contract will eliminate the problems associated with institutionalized knowledge. This is not an implementation of push notification. It is bringing a contract to life within its environment.

The smart contract will understand itself, its environment, the objects with which it must interact and the personnel with whom it will interact. A smart contract won't be ignored. A smart contract will know what actions to take when timelines are not met. A smart contract will manage itself, and that in turn will eliminate many contract management functions currently performed by humans.

## **Beyond the Smart Contract**

The first problem to note before beginning this section is one of catch-up-to-fall-behind. In its basic form, this problem arises when an organization begins planning an upgrade to its system. By the time the planning and execution of the upgrade are completed, the upgraded technology already is obsolete. The smart contract is a first step. But a bolder move, a leap into the future, is needed so that—when the development is finished—the system remains far advanced.

## **The Intelligent Contract**

The intelligent contract can be described in one word: ontology—the study of being. In this context, ontology involves describing information and relationships in an informative way. That sounds like a database. But unlike a relational database that stores and retrieves data items, an ontological database system brings understanding into the realm of data queries.

What does that mean in simple terms? Look at the iPhone assistant Siri as an example. When a person asks Siri a question, such as "Do I need an umbrella," Siri has to understand

that this is a weather-related question and then search the national weather database for the weather conditions at the user's location to provide an answer. Siri understands the question in context, and also knows how to find the answer and report that answer to the user.

The World Wide Web Consortium is involved in this endeavor of creating smart, understanding programs and ontological databases by developing OWL (Web Ontological Language). It also supports a new query language developed for OWL called SPARQL—a pattern-matching scheme in which a database is queried for matches and certain of the results are graphed to determine a pattern. This is an enormous development because giving meaning to data has many practical uses. The future is here. But how does that fit with the DoD and the contracting world?

### **Knowledge Is Power**

A contractor has made two variations of the same product for one of the branches of the Armed Services. A modification to the product is requested, a new contract is signed and work begins. During final testing in a field environment, a major failure occurs. The representative of the Armed Services tells the contractor that the product does not meet the requirements put forth in the contract. The contractor states that the equipment meets the requirements to perfection. When asked to explain the failure, the contractor states that the requirements are met perfectly when the equipment is tested in a laboratory and that the requirements don't state anything about passing a test in a field environment.

Even though the contractor had produced two similar products and met the requirements for field performance, this contract did not specify field performance in the requirements. The Armed Forces representative failed to specify that part in the requirements section of the contract. Now the contractor has to be awarded more money to meet the new specification. Does this happen often? Yes. And it can be stopped with the implementation of an intelligent contract.

### **The Intelligent Contract Knows Itself**

A smart contract knows details about itself (properties) and how to interact with other objects (methods). An intelligent contract knows its own being. Every member of the military who has driven a tracked vehicle knows that it must be able to pivot 360 degrees in the mud. But the mere fact that this is known does not mean it is written in the contract. An ontological database will solve this problem.

**In an age in which airplanes fly themselves and cars drive themselves, it is time to create a contract that manages itself. Contracting challenges technology, and, in turn, technology inspires contracting.**

In the intelligent contract paradigm, an ontological database will be developed to link data from the disparate departments of the DoD into understandable knowledge. The chief focus at first will be the linking of data that deal with requirement specifications found in contracts. The methods used in the intelligent contract ontology are semantic methods. Interestingly enough, this effort was begun by the Defense Advanced Research Projects Agency (DARPA) in

1999. DARPA developed the DARPA Agent Markup Language (DAML) and a variety of programs, tools and datasets for use by government and commercial clients. It was the foundation of semantic Web programming.

Linking data from various organizations within the DoD—with the links based on semantics—will form the ontological database that will be used for understanding requirements specifications. What documents exist on the Army website that describe 360-degree pivot steering on a tracked vehicle? How would those documents match other documents within the Air Force web, or the Navy web?

The basic concept of the semantic methods is to search domains looking for similar data tags. The tags are matched in a logical order. This results in a semantic match. Then the matter of intent has to be evaluated. Hence, when Siri is asked whether an umbrella is needed, a search of the Web for the word "umbrella" would be insufficient. The intent of the person posing the question is to see if the weather forecast calls for rain. To understand the intent, the ontological database is built on semantic relationships.

### **Conclusions**

When the ontological database is incorporated and the smart contract has dominion over its environment, amazing potentials become ripe for the harvest. Imagine using your voice to ask a contract who its suppliers are on its supply chain. Imagine asking the contract how a particular supplier has performed in the past. Imagine asking a contract if the supplier is likely to complete the order on time and within budget.

Turning those exercises in imagination into reality now becomes a matter of action because the foundational blocks already exist. These steps—implementing a smart contract and then an intelligent contract—will take the contracting IT business systems for the DoD into the future. There will be no catch-up-to-fall-behind issues. 

The author can be contacted at [russell.chesebro@dcma.mil](mailto:russell.chesebro@dcma.mil).



# Performance Based Logistics

## For Achieving Affordable Readiness

*Betsy Lederer ■ Knob Moses*

In February 2014, the Secretary of Defense announced a plan to shrink the Pentagon’s budget by more than \$75 billion over the next two years. Secretary Chuck Hagel said these cuts would come by reducing manpower without degrading training or readiness. In order to help achieve these aggressive goals, there has been an increased focus on greater efficiency and productivity. This is reflected in the April 24, 2013, memorandum from Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) Frank Kendall, “Implementing Directive for Better Buying Power 2.0—Achieving Greater Efficiency and Productivity in Defense Spending.” As part of a broad range of initiatives, Kendall’s BBP 2.0 memorandum promotes Performance Based Logistics (PBL) as one tool for achieving the Department of Defense (DoD) goal of affordable readiness. Using an outcome-based sustainment strategy, PBL offers a well-tested contribution to meeting the DoD’s budgetary challenges.

---

**Lederer** is the performance learning director for Performance Based Logistics at the Defense Acquisition University. **Moses** is a specialist leader at Deloitte Consulting LLP.

PBL works by incentivizing desired outcomes across the product life cycle, from design through sustainment to retirement. In a PBL product support arrangement—which rewards the achievement of performance results—a support provider is incentivized to reduce the number of unscheduled maintenance and repairs as well as the cost of the parts and labor used in the repair process. This improves availability at lower cost. Under a traditional transactional product support model, by which the government purchases parts or maintenance services for repairs, the provider does not receive incentives to improve availability or reduce the need for repairs and repair parts. The opposite is true: In the transactional model, the provider’s revenue increases as equipment failures increase. This model creates a fundamental product support misalignment for DoD, and PBL arrangements address this misalignment. In PBL, commercial providers are incentivized to reduce system downtime and costs because the contract specifies weapon system, subsystem or component performance outcomes—not transactions.

In November 2011, the Office of the Deputy Assistant Secretary of Defense for Logistics and Materiel Readiness (ODASD[L&MR]) completed an analysis of more than 20 PBL arrangements executed over 10 years. The resulting Project “Proof Point” PBL Study noted that annual savings or cost avoidance of between 5 percent and 20 percent are considered possible for properly structured and executed PBL programs. Given a 2014 sustainment budget of approximately \$273.2 billion, the potential savings or avoided costs are not insignificant and have re-energized the focus on more effective use of PBL product support strategies.

### Performance Based Logistics Guidance

In addition to the BBP 2.0 memorandum mentioned above, the Office of the Secretary of Defense (OSD) issued two other applicable guidance documents:

- The Acting ODASD (L&MR) “PBL Comprehensive Guidance” Memorandum of Nov. 22, 2013, amplifies the DoD’s plan to expand the use of PBL arrangements and provides detailed guidance to assist the Military Departments with increasing this effort.
- In collaboration with the Services and the Defense Acquisition University (DAU), ODASD(L&MR) also promulgated the *PBL Guidebook: A Guide to Developing Performance-Based Arrangements* on May 27, 2014. It was designed as a reference manual and how-to guide for both new and experienced PBL practitioners. Because developing PBL contracts is a team effort, the *Guidebook* is intended to be a cross-career field resource and to include practical information for life-cycle logisticians, engineers, business/cost estimators and financial managers, and contracting officers.

### Performance Based Logistics Definition

OSD succinctly defines PBL, and provides guidance regarding characteristics of effective PBL arrangements:

PBL is synonymous with performance-based life-cycle product support, where outcomes are acquired through performance-based arrangements that deliver warfighter requirements and incentivize product support providers to reduce costs through innovation. These arrangements are contracts with industry or intragovernmental agreements.

Attributes of an effective PBL arrangement include:

- Objective, measurable work description that acquires a product support outcome
- Appropriate contract length, terms and funding strategies that encourage delivery of the required outcome
- A manageable number of metrics linked to contract requirements that reflect desired warfighter outcomes and cost-reduction goals
- Incentives to achieve required outcomes and cost-reduction initiatives
- Risks and rewards shared between government and commercial product support integrators and providers
- Synchronization of product support arrangements to satisfy warfighter requirements

### Types of Performance Based Logistics Arrangements

There are many different types of PBL arrangements. They can be established at the system, subsystem or component level and can address anywhere from one to all the 12 Integrated Product Support (IPS) Elements listed below:

- Product Support Management
- Design Interface
- Sustaining Engineering
- Supply Support
- Maintenance Planning and Management
- Packaging, Handling, Storage & Transportation (PHS&T)
- Technical Data
- Support Equipment
- Training and Training Support
- Manpower and Personnel
- Facilities and Infrastructure
- Computer Resources

Also, it is important to know that a PBL arrangement can be formed with government support providers, such as DoD maintenance Depots, which are facilitated by the use of intergovernmental Memorandums of Agreement (MOA) or Memorandums of Understanding (MOU), while others are with industry and implemented via various types of contracts. Many, however, are a mix of both organic and industry support providers, in constructs specific to each program’s performance requirements.

The PBL arrangement level and IPS elements selection can be adjusted in scope, based on the program’s performance requirements. For instance, a system failing to meet performance requirements because certain parts are unavailable should consider a PBL arrangement focused on supply support. Similarly, a system facing significant issues with parts

reliability should implement a PBL that includes reliability improvement and sustaining engineering activities. Tying the root causes of performance deficiencies with the appropriate PBL arrangement type is crucial to a successful outcome.

### **Hurdles to Adoption**

Despite DoD policy requiring that programs “employ effective Performance Based Logistics planning, development, implementation and management in developing a system’s product support arrangements” (Interim DoDI 5000.02, November 2013), research indicates that the number of PBL contracts actually declined over the last few years. While the exact number of PBL arrangements is difficult to measure, research indicates that less than 5 percent of DoD systems, subsystems and components currently are covered by a PBL arrangement.

If they are required and can be so effective, why has the number declined? And, given the savings potential, what can be done to increase their use?

The DoD recognizes that PBL implementation can be a challenge. PBL contracts can be complex and often take a long time to implement. They also require teams who have an in-depth understanding of the PBL implementation process and who share performance goals and agree to focus resources on those common goals. The teams also need a solid grasp of Title 10 United States Code (U.S.C.) requirements related to the use of organic depots, as stated in statute 10 U.S.C. 2460, and insight into what motivates industry. But there is good news: Help is here, and more is in the works.

Let’s start by looking at three common challenges to implementing PBL arrangements followed by information on resources and available tools and on future efforts.

Common challenges to increasing the effective use of PBL include:

#### **Organizational Structure and Funding Sources**

As stated above, establishing a PBL contract requires a broad-based team approach, and involves multiple stakeholders and subject-matter experts (SMEs) working within an Integrated Product Team (IPT). The warfighter, program manager (PM), product support manager (PSM), engineering,

finance, contracting and other government representatives are required to coordinate and collaborate with each other and with both government and industry support providers to develop and implement a sound outcome-based product support strategy.

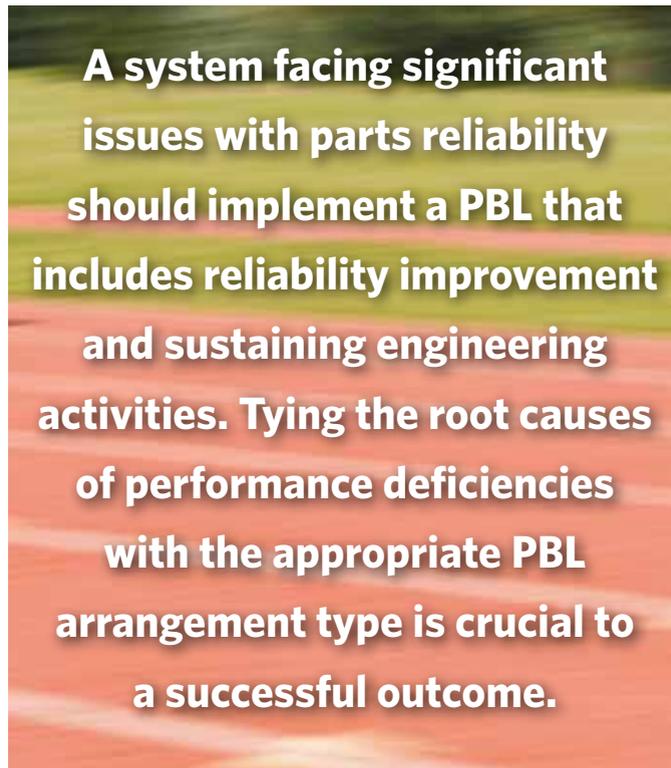
Within these IPTs, however, there usually is a mixture of goals and separate sources of funding, stemming from the aims of each participant’s separate organizational hierarchy. The warfighter representative typically “owns” the Operations and Maintenance (O&M) funds and supports demanding and dynamic global operational requirements. The PM—who has Total Life Cycle Systems Management (TLCSM) accountability—may have research and development (R&D) and procurement (not O&M) appropriations in his acquisition checkbook. There is the PSM, who serves as the PM’s representative and lead in the product support management IPT and who usually has access to the PM’s acquisition checkbook but very little influence on sustainment funds. Then there are the de-

pots and inventory control points (ICPs) that manage working capital funds (WCF), which are “revolving”-type funds often used to facilitate long-term PBL contracts. The warfighter, PM and PSM usually have little control of DWCF. Add the possibility of joint Service or enterprise-level PBL efforts, and the organizational complexity increases exponentially. This mixture means that developing an executable life-cycle solution becomes a demanding process that requires a mature ability to make trade-offs and compromises.

Putting a PBL contract in place is a team exercise, and requires alignment of requirements and resources. The team should leave “stovepipe” or segmented thinking at the door and take a holistic approach. The new team mantra should be “Let’s be good stewards of the whole versus the defenders of ‘my’ portion.”

#### **System Support Requirements Definition With Analytical Rigor**

Defining support requirements and securing agreement on them across the IPT are challenging and important to the success of PBL efforts. While the top-level Sustainment Key Performance Parameter (KPP) and other associated Key System Attributes (KSA) are captured, for example, in the Capability Development



**A system facing significant issues with parts reliability should implement a PBL that includes reliability improvement and sustaining engineering activities. Tying the root causes of performance deficiencies with the appropriate PBL arrangement type is crucial to a successful outcome.**

Document (CDD) and Capability Production Document (CPD), lower-level system support requirements and metrics need to be addressed in PBL arrangements. These lower-level metrics are based on both operational requirements and an in-depth understanding of system, subsystem and component performance capabilities and support challenges. This requires the PSM to work with the warfighter and sustainment organizations to address the predicted future operational tempo—as well as associated equipment and inventory optimization analyses, including the financial impact. These, in turn, require insight into performance data that may or may not be available within the government, depending on the equipment type and the program's Intellectual Property (IP) strategy.

This challenge of accessing data often contributes to a quick-fix mentality addressing the symptoms of a problem rather than developing a root-cause cure. For example, equipment performance problems often are solved by buying more spare parts and repairs, rather than identifying—and fixing—the problem with the equipment itself. Successful adoption of PBL contracts requires a strategic problem-solving approach, pushing the IPT (including industry) to work together toward proactive and long-lasting sustainment solutions.

### **PBL Expertise**

Knowledge and experience with PBL arrangements are critical to their success, but many Defense acquisition professionals have little experience with PBL because transactional sustainment is the predominant methodology used today. As discussed above, PBL contracts demand sophistication and teamwork above and beyond what is required in the status quo transactional model. As with the support requirements definition challenge, the acquisition workforce challenge will require a shift in focus and expansion of skillsets to facilitate the more wholesale adoption of the PBL business model and associated processes.

The current environment has not been conducive to creating a large number of experienced PBL specialists. Training, and increasing focus on practical PBL “how to” information, plus an increase in experiential learning opportunities, are needed to produce the level of workforce improvements required.

### **Leading Practices**

The good news is that the DoD is facing the obstacles head on. Per the ODASD(L&MR) “PBL Comprehensive Guidance” memorandum, OSD is committed to addressing PBL challenges with the following ongoing initiatives and actions:

- Cultivate an enabling, collaborative environment including more component acquisition executives (CAEs) communication with the workforce, and PBL efforts in milestone reporting and identification of (intended or unintended) policy obstacles.
- Develop documented processes and tools—including use of the processes and tools captured in the newly released *PBL Guidebook*.

- Create a cadre of PBL professionals. This should include assessing gaps in workforce PBL competencies and using this information to change workforce training and DAU learning assets. This initiative also refers to using the comprehensive PBL Community of Practice, designed as an interdisciplinary platform to connect PBL practitioners from across multiple career fields and to provide a knowledge repository for PBL-related material across the DoD. The action encourages pursuit of PBL training through DAU as well as hands-on experience in structuring and executing PBL arrangements.
- PBL Reporting. CAEs are to provide an annual summary of their PBL implementation efforts to the Business Senior Integration Group. This should include the current use of PBL arrangements, savings achieved, lessons learned and future opportunities.

While these efforts are significant, it is understood that they may not be enough to appreciably expand use of this sustainment method and that additional work may be required. But recent comments by Kendall clearly indicate that the DoD is committed to increasing the use of this powerful tool:

The data shows that we have not been able to expand the use of PBL for the last two years and that prior to that the use was declining. Declining budgets as well as the budget uncertainty itself, and therefore contract opportunities, are part of this story, as is the fact the PBL arrangements are harder to structure and enforce than more traditional approaches. Those factors, combined with the imposition of sequestration, furloughs and a government shutdown last year are likely to have suppressed the increased use of PBL. This area will receive additional management attention going forward; we are going to increase the use of this business approach.

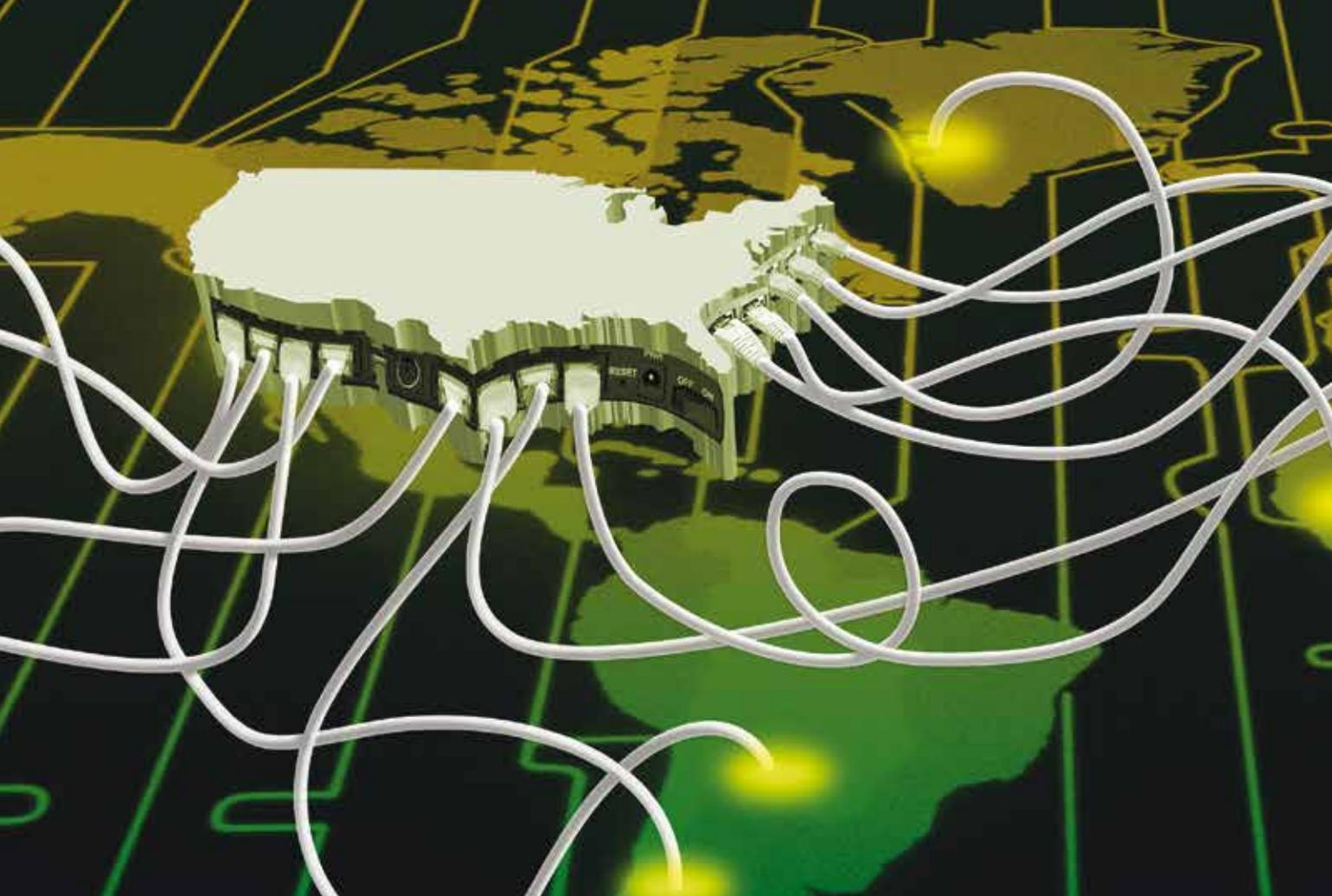
Specifics regarding the “additional management attention” have not yet been provided, but, at the August 2014 Armed Forces Communications and Electronics Association Defense Acquisition Modernization Symposium, Kendall did not mince words. Acquisition workforce members need to “understand what they’re doing. And that’s a never-ending process. I think we’re going to grow that body of work continuously—over the next—forever, basically. So that’s here to stay.”

### **Conclusion**

PBL arrangements provide a potent way to help the DoD deliver affordable readiness. Implementing PBL strategies can be a challenge, but there are increasing resources to help build successful PBL contracts—and more to follow, if necessary. It is an effort used in the DoD for some time, but, due to our constrained budget environment, it has received renewed focus in BBP 2.0 and is likely to be addressed in BBP 3.0 as well. Make no mistake, however: This is not just a rehash of an old topic; the DoD’s commitment to communicate, educate and improve our level of PBL expertise is reborn and is very, very real. 📢

---

The authors can be contacted at [betsy.lederer@dau.mil](mailto:betsy.lederer@dau.mil) and [romoses@deloitte.com](mailto:romoses@deloitte.com).



# Defense Exportability Features Initiative

## A New Paradigm for International Cooperation

Frank D. Kenlon ■ Jay Mandelbaum

**D**epartment of Defense (DoD) program managers (PMs) are now required to consider developing and incorporating Defense Exportability Features (DEF) into a system or subsystem likely to be exported to enable future U.S. Government-DoD International Cooperative Programs (ICPs), Foreign Military Sales (FMS) or Direct Commercial Sales (DCS) or other U.S. Government-authorized Building Partner Capacity (BPC) transfers.

---

**Kenlon** is a professor of international acquisition management (intermittent) in the Defense Systems Management College's International Department at the Defense Acquisition University, Fort Belvoir, Va. He retired from Department of Defense full-time employment as Director of International Negotiations in the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics in January 2013 after more than 35 years of service in various domestic and international acquisition positions in the U.S. Navy and the Office of the Secretary of Defense (OSD). **Mandelbaum** is a research staff member at the Institute for Defense Analyses, where he has been involved in studies of international cooperation, obsolescence management, value engineering, technology readiness assessments, manufacturing, systems engineering and acquisition for the last 10 years. He retired from the OSD systems engineering office in April 2004.



Activities in support of this DEF requirement may be pursued throughout the acquisition life cycle but, in general, are more efficient and affordable when pursued during a program's early development phases. These activities can and should also be pursued during the Engineering and Manufacturing Development (EMD) phase of defense acquisition, as well as during product upgrade efforts for fielded systems that are authorized by the U.S. Government for export in support of USG foreign policy and national security objectives.

Fortunately, there is a process for DoD PMs to become a designated system in the DoD DEF Pilot Program initiative managed by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) that helps implement this recently issued change to DoD acquisition policy. This pilot program, for which programs are nominated by their Service Acquisition Executive (SAE) and selected by the Defense Acquisition Executive (DAE), allows appropriated dollars to be used to support the design and development of exportable variants of acquisition systems early in their life cycle. In particular, the Fiscal Year (FY) 2011 Na-

tional Defense Authorization Act (NDAA), as amended, and corresponding appropriations bills, established and funded pilot program efforts that focus on incorporating DEF-related technology protection features during the research and development phase (typically the Technology Maturation and Risk Reduction [TMRR] and early EMD phases) of the DoD acquisition process. These technology protection features provide the technical modifications necessary to protect critical program information (e.g., anti-tamper and information assurance), as well as differential capability changes required prior to U.S. Government-authorized export.

The details of these technology protection features vary as a function of the capabilities of the system, the critical program information or critical technologies used, and the prospective foreign partner or customer nations authorized for export. DEF Pilot Program funding covers the cost of the feasibility studies used by DoD to evaluate the business case for informing a decision on making such investments, as well as the cost of performing preliminary DEF design work; it does not currently include the costs for incorporating these features into production articles.

Beyond DEF Pilot Program participation, PMs always have the option of pursuing defense exportability design and development efforts using funding obtained through ICPs, FMS, DCS, or BPC transactions to implement defense exportability features outside of the DEF Pilot Program.

### Why DEF Is Important

Section 2350a of Title 10, Subtitle A, Chapter 138, Subchapter 2, "Cooperative research and development agreements: NATO [North Atlantic Treaty Organization] organizations; allied and friendly foreign countries," identifies questions to determine the appropriateness of pursuing international acquisition and exportability to achieve the following traditional benefits:

- Building international military and economic partnerships
- Increasing interoperability
- Enhancing U.S. defense capabilities and influence by leveraging partner nations' defense investment and technologies
- Providing flexibility for DoD production and sustainment by maintaining active production and sustainment capability longer

The latter benefit has applicability to the defense industry from two perspectives—increasing contractors' revenue and profit and maintaining a healthy U.S. industrial base. However, if production capability is extended because most foreign sales could not be made during U.S. Government production, as has often been the case, there will be higher costs to export variants, a potential reduction in foreign sales, and suboptimized technology protection.

The new DEF authority facilitates a paradigm shift, potentially enabling allies to obtain DoD systems earlier than the more typical exportability process. Consequently DEF should enhance these traditional benefits in two important ways:

- By providing advanced capability to allies and coalition partners earlier, thereby improving upon the benefits listed in the first three bullets of the previous paragraph.
- By strengthening the DoD industrial base (the fourth bullet).

Furthermore, DEF enables an extremely significant additional benefit by potentially lowering the average procurement unit cost (APUC) that DoD pays for the system. APUC may be reduced for two reasons:

- A greater number of U.S. units may be purchased at a lower cost because the learning curve is extended.
- Combining U.S. and foreign production leads to larger lot sizes during full-rate production, resulting in economies of scale.

Figure 1 illustrates the potential APUC savings as a function of the ratio of foreign transfers to the U.S. procurement during full-rate production. The figure is based on a 90 percent learning curve, typical of defense electronics. Foreign production is assumed to start during the first year of full-rate production, and low-rate initial production quantities are assumed to be 10 percent of the U.S. procurement. The figure also assumes that the foreign variants have very high commonality with the U.S. version.

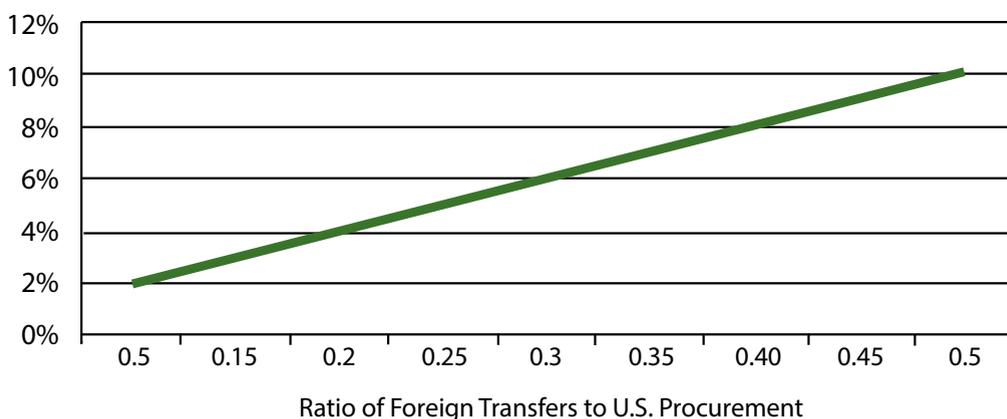
In recognition of all this, DEF was incorporated into the Better Buying Power (BBP) 2.0 as an initiative to control costs throughout the life cycle as follows:

#### Increase the incorporation of defense exportability features in initial designs:

Foreign sales of and cooperation on U.S. defense products provide a range of win-win benefits: reduced costs, improved U.S. competitiveness, stronger ties to friends and allies, and improved interoperability. Rather than waiting until products are fully designed and in production for U.S. use, we should assess and incorporate exportability design features and any needed anti-tamper features early in the acquisition process. This will reduce the cost of exportable versions of U.S. systems and ensure that they are available for sale sooner, benefiting all concerned.

While the DEF initiative is currently addressed in the Interim DoDI 5000.02 and *Defense Acquisition Guidebook (DAG)*, it is expected that the final version DoDI 5000.02 and the corresponding DAG changes, will provide additional DEF policy and implementation guidance to the DoD acquisition workforce as part of continuing BBP 2.0 DEF implementation

**Figure 1. Percent Reduction in U.S. Average Procurement Unit Cost**



under the BBP 3.0 initiative announced Sept. 19, 2014, by USD(AT&L) Frank Kendall.

### Legislative History

As noted above, Section 243 of the FY 2011 NDAA, "Pilot Program to Include Technology Protection Features During Research and Development of Defense Programs," established the DoD DEF Pilot Program, including a requirement for an annual report to Congress regarding DEF Pilot Program efforts, including a list of each designated system in the program. The FY 2012 NDAA modified the law based on a request from DoD to require industry to bear at least half of the cost of any DEF

These studies would determine whether to proceed to a detailed design with a requirement to include export variants. The export variant may be the same as the U.S. baseline version, or the U.S. baseline may be designed in such a way as to make it easily adaptable to producing an export variant.

### Evaluation of DEF Viability Using Pilot Program Results

DoD is using the results of DEF Pilot Programs to demonstrate and document key aspects of DEF viability. One area of potential analysis is whether DoD has (or will have) the ability to accurately assess its potential Return on Investment (ROI)



**The details of these technology protection features vary as a function of the capabilities of the system, the critical program information or critical technologies used, and the prospective foreign partner or customer nations authorized for export.**

Pilot contractual effort, to match U.S. Government expenditures. If the defense industry did not agree, there would be no investment from either party. In order to give the DEF Pilot Program adequate time to evaluate its impact, the FY 2014 NDAA extended the DEF Pilot Program five additional years to Oct. 1, 2020.

Based on subsequent feedback from the defense industry, DoD recently recommended another legislative change concerning the cost-sharing provisions. Industry indicated that a requirement for a fixed cost share may be a deterrent to DEF success. DoD agreed and is seeking the flexibility to adjust the cost-share requirement to levels appropriate to the particular situation. The draft FY 2015 NDAA currently under consideration on Capitol Hill includes a provision that would change the current 50-50 government-industry statutory DEF cost-sharing requirement to "an appropriate share of the cost of such activities, as determined by the Secretary."

### DEF Activities

As of the December 2013 report to Congress, 16 acquisition programs have been nominated by their SAE and selected by the DAE to conduct DEF studies. The programs qualified for feasibility study funding based on the following criteria:

- High defense sales potential
- Significant military capability to build partner capacity
- Technology that requires export protection
- Component International Program Office validation

based on the fidelity of the information available from a DEF feasibility study. After a feasibility study, DoD must decide whether to include requirements for export variants in the statement of work for a competitive Milestone (MS) B request for proposal (RFP) or—for programs that have already entered the EMD phase—to modify the existing EMD contract. That decision should be based largely on the ROI to DoD. One of the objectives for DEF Pilot Programs is to produce feasibility studies that can provide sufficient data to make an ROI calculation meaningful to decision makers. ROI is calculated from the ratio of DoD investment to APUC reductions. Therefore, one aspect of DoD's evaluation of DEF viability will focus on whether feasibility studies can provide accurate answers to the following ROI-related questions for use in DoD acquisition decision making:

- Investment: Can the feasibility study determine what exportability features are needed, how they should be implemented and what that will cost? Can DoD determine the accuracy of these data?
- APUC reductions: Are the industry estimates of foreign transfers and APUC savings documented in the feasibility studies of sufficient fidelity for DoD to calculate ROI? Can DoD conduct an independent estimate of foreign transfers? Can APUC savings be validated?

DoD also is using pilot program results to develop repeatable best practices and standard operating procedures for effective integration of DEF into the overall operation of the defense acquisition system in areas such as:

- **Incentives and disincentives.** Prior to MS B, one of the principal goals of any program office is to accomplish what is necessary to become a program of record. This usually entails convincing decision makers that the program will meet cost, schedule and performance requirements. For most DoD programs, defense exports eventually will contribute to meeting these objectives. But the potential beneficial impact of foreign cooperation or sales is uncertain, particularly early in the program's life cycle. From a pilot program perspective, DEF is welcome because it adds visibility and a source of funds that will help the program achieve mid- to long-term affordability objectives. After MS B, however, international considerations are often deemphasized or postponed as a result of the inevitable technical challenges in detailed design and development. In developing standard operating procedures for integrating DEF into the defense acquisition

include: (1) How many export versions should be designed? (2) To what extent should prototypes be developed and tested? (3) What work should be part of the base contract? (4) What effort should be included in option Contract Line Items Numbers (CLINs)? (5) If option CLINs are used, what are the criteria for executing them? (6) To what extent will DEF information be used in evaluating proposals? (7) What has to be done to ensure that all bidders compete on an equal basis?

### Conclusions

While the DEF initiative has the potential to change the international cooperation paradigm, it is still too early to gauge its success in doing so. The challenge ahead is to develop repeatable best practices and standard operating procedures for integrating DEF into the defense acquisition system. Fortunately,



**One of the objectives for DEF Pilot Programs is to produce feasibility studies that can provide sufficient data to make an ROI calculation meaningful to decision makers.**

system, DEF Pilot Programs are intended to provide PMs incentives to design in exportability features early to save the program from higher redesign costs later, and to hold out the potential for lower APUCs through economic order quantities from foreign sales.

- **Sources of funding.** DEF Pilot Program results have already shown that moving beyond DEF feasibility studies and initial DEF designs into implementation during EMD will require additional sources of funding beyond the DoD DEF Pilot Program. Several potential funding sources for DEF efforts during EMD are being considered. Examples include foreign partner and/or customer funding; Defense Security Cooperation Agency's Non-Recurring Cost (NRC) Recoupment funding and (in limited circumstances) the Special Defense Acquisition Fund; Title 10 funds; and use of value engineering change proposals to implement DoD/contractor cost sharing for exportability modifications. If additional funding cannot be made available when needed, DoD's ROI may decrease (and foreign customer costs increase) due to the rework and delays required to add the necessary exportability features during production.
- **Contracting approaches.** DEF pilot program contractual activities to date have shown that structuring the DEF-related elements in a competitive EMD phase RFP is challenging but manageable. Examples of key issues that contracting officers should address in the RFP and contracting process

we understand that the USD(AT&L) is drafting a DEF Implementation Policy Memorandum that will address incentives for program offices to engage in international cooperation and sales, DEF Pilot Program nomination criteria, sources of DEF funding, contracting approaches and other standard operating procedures for execution of DEF in DoD programs. Results from current and future DEF Pilot Programs should be used to provide the data necessary to evaluate the likelihood of the initiative's success and to determine how to effectively implement future DEF activities. As USD(AT&L) Kendall stated in congressional testimony on April 20, 2014:

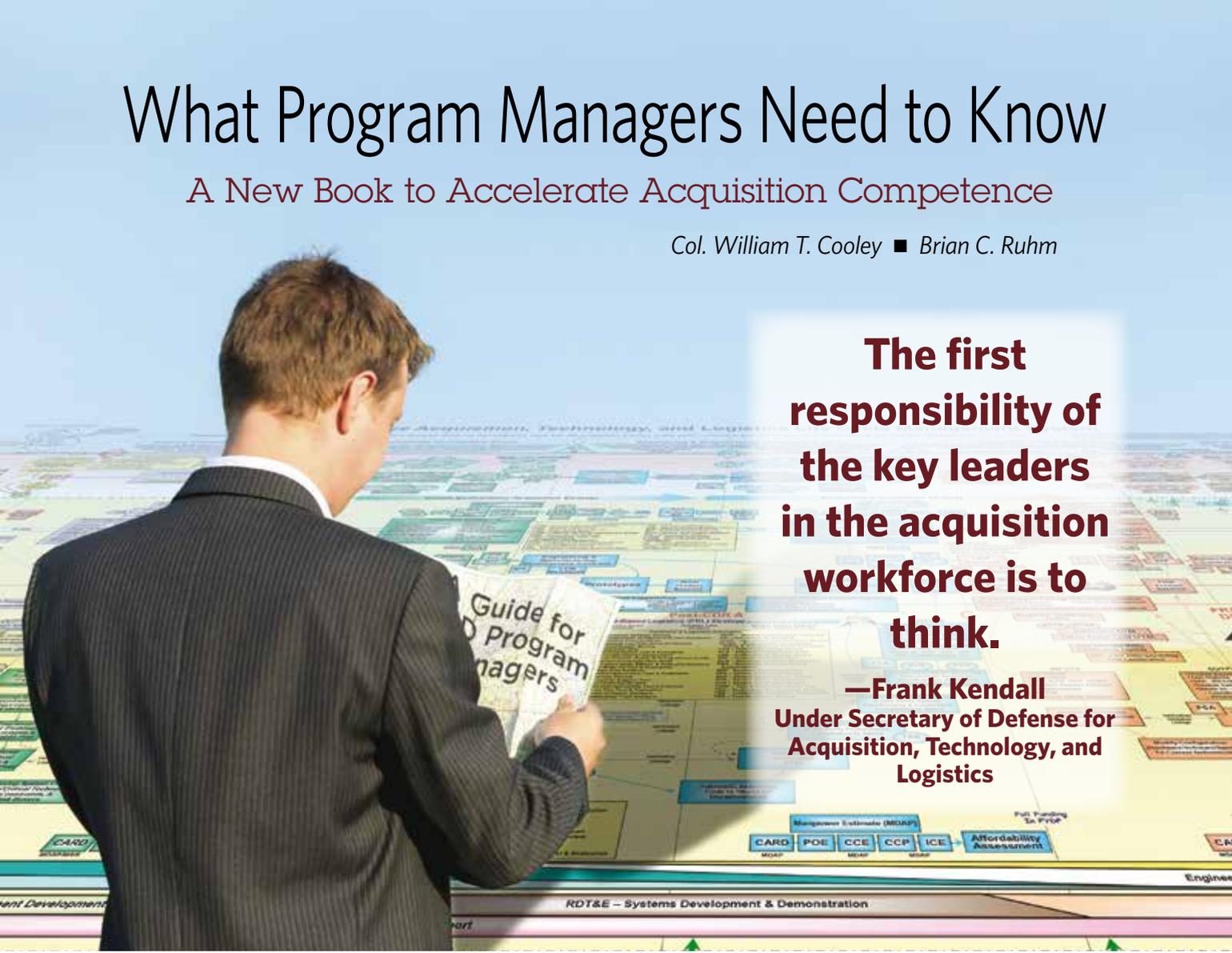
The BBP 2.0 program to increase the use of defense exportability features in initial designs is still in the pilot stage. The concept is sound, but implementation is difficult because of some of the constraints on our budgeting, appropriations and contracting systems. Support for U.S. defense exports pays large dividends for national security (improved and closer relationships), operationally (built in operability and ease of cooperative training), financially (reduced U.S. cost through higher production rates), and industrially (strengthening our base). This initiative will continue on a pilot basis, but hopefully be expanded as the implementation issues are identified and adjudicated. 

The authors can be contacted at: [frank.kenlon@dau.mil](mailto:frank.kenlon@dau.mil) and [jmandel@ida.org](mailto:jmandel@ida.org).

# What Program Managers Need to Know

A New Book to Accelerate Acquisition Competence

Col. William T. Cooley ■ Brian C. Ruhm



**The first responsibility of the key leaders in the acquisition workforce is to think.**

**—Frank Kendall**  
Under Secretary of Defense for Acquisition, Technology, and Logistics

The Department of Defense (DoD) acquisition management process is complex. Despite the DoD's best efforts to standardize acquisition processes and strategies, running a large acquisition program rarely lends itself to a "checklist" approach. Success as a program manager (PM) requires not only understanding acquisition principles, processes and terminology but also attaining a sound working knowledge of the acquisition functional areas—contracting, financial management, systems engineering and integrated logistics.

The Defense Acquisition University (DAU) provides quality training in the processes, terminology, skills and functional expertise acquisition professionals need in order to succeed. DAU also has created several outstanding

---

**Cooley** is the program director for the Global Positioning System (GPS) at the Space and Missile Systems Center at Los Angeles Air Force Base. He is a graduate of Rensselaer Polytechnic Institute, has a doctorate of philosophy in Engineering Physics from the Air Force Institute of Technology and attended the National War College. **Ruhm** has more than 26 years of experience in program management. He has worked on battle management, command and control, intelligence surveillance and reconnaissance, aircraft, satellite, and missile defense programs at all acquisition categories. He is a graduate of the U.S. Air Force Academy and has a master's in public policy from Harvard University, attended Air Command and Staff College and completed Air War College.

“case-based” courses that allow senior acquisition professionals to capture lessons learned from real-world programs.

But classroom-based acquisition training doesn’t always “meet the needs” of the acquisition community. Sometimes it’s difficult for a busy PM to find the time for an acquisition course that might take as long as 10 weeks to complete. PMs may also be pressed into service from another career field or after several years of career broadening and find themselves in need of a rapid tutorial or quick refresher. Occasionally there’s just a mismatch between the demands of a particular program and the lessons that the existing curriculum offers. Finally, as Under Secretary Kendall suggests in the quote above, critical but intangible skills like ethics and judgment also are difficult to impart via formal training. Training also is an incomplete substitute for experience. The “school of hard knocks” often is the best training ground for acquisition professionals.

This left us wondering ... given the complex nature of the program management profession, the demands it places on a typical PM’s time and the value of acquisition experience, is there a way to accelerate the competence building of our junior and mid-level acquisition workforce members?

We’re not sure, but many of the acquisition professionals we consulted with pointed to the lack of a concise and comprehensive “how to” guide. Such a guide would provide practical advice across the range of diverse topics and issues with which a PM needs to be familiar. With this in mind, we set out to create an easy-to-digest book that lends itself to either a cover-to-cover read or targeted reference as needs merit. Acknowledging the importance of context-based training, we included a number of real-world examples. And although we believe senior PMs will find it useful, the contents provide a beginners’ guide and quick reference to the foundation of program management. We’ve titled it *A Guide for DoD Program Managers—90 Percent of What Department of Defense Program Managers Need to Know to Run an Effective and Efficient Program*. DAU is e-publishing the book for acquisition professionals on DAU’s website at [www.dau.mil/publications/pages/guide-books.aspx](http://www.dau.mil/publications/pages/guide-books.aspx). Below, we briefly describe the contents of the book and provide some examples of ways we’ve attempted to make it easy to digest as an “airplane read.”

In addition to an initial review of “The Basics,” the book has three main sections: (1) “Tools of the Trade”; (2) “Critical Artifacts”; and (3) “Intangibles.” Each of these sections is further broken into sub-sections and subordinate pieces as needed to cover each topic. For example, “The Basics” section includes (no surprises here) cost, schedule, performance and risk sub-sections. The goal is not to provide the comprehensive reference—that is why the *DAU Guidebook* exists—but rather to provide a readable synopsis along with experience accelerators in the form of “Proverbs for PMs” and useful quotes.

Although we have condensed the book to what we consider the “bare minimum” necessary to successfully lead an

acquisition program, not everyone will have time to read it continuously from end to end. So we’ve employed a few presentation techniques and quickly comprehended features to ease the reader’s experience and emphasize key points. We make abundant use of graphics and tables, include quotes from members of the acquisition community and prominent historical figures, highlight important “Proverbs for PMs” and include acquisition stories that illustrate key points.

The analogy we use to help explain the role of the PM is that of expedition leader—responsible for the safety of the team and overall outcome but also reliant on team experts to accomplish particular portions of the mission. Accordingly, the major sections of the book—“Tools of the Trade”; “Critical Artifacts”; and “Intangibles”—broadly apply to both adventurers and PMs. Below are brief descriptions of each section and the appendices that include some useful and entertaining checklists.

**The Tools of the Trade** (section 1) is the longest and is intended to provide a foundational understanding of key functional areas for all programs—financial management, contracting and systems engineering. We also provide a brief discussion of three other “tools” that we have found very useful—“battle rhythm,” earned value management and independent reviews of the program.

**Critical Artifacts** (section 2) identifies the documents to which a PM must pay particular attention as these documents will very likely determine success or failure. The four documents we have found most critical for program success are the Acquisition Strategy, the Acquisition Program Baseline (APB or just “Baseline”), the Integrated Master Plan (IMP) and the Integrated Master Schedule (IMS).

**Intangibles** (section 3) may be the most important section of the book (we debated moving it to the front for this reason). Section 3 discusses ways to think about the role of PM. We do this by looking closely at (1) integrity (three subtly different definitions of the word), (2) leadership and (3) collaboration and compromise.

Although acquisition is not a checklist activity, some checklists initiate or challenge our thinking. To that end, we also included an appendix that captures items such as “Battle’s Law—Principles of Program Management from 1961” and “Norm Augustine’s Checklist for an Acquisition Adventure—A Formula for Failure.” We hope readers will find these both enlightening and entertaining and that the book will help you and your team members succeed in the complex business of DoD acquisition management. Although our subtitle “90 Percent of What Department of Defense Program Managers Need to Know to Run an Effective and Efficient Program” may be optimistic, we hope that this book will “accelerate acquisition competence.” 

The authors can be contacted at [william.cooley@us.af.mil](mailto:william.cooley@us.af.mil) and [brian.ruhm.1@us.af.mil](mailto:brian.ruhm.1@us.af.mil).



## **Defense ARJ** and **AT&L** have become online-only publications for **individual subscribers**

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

**All Readers:** Please subscribe or resubscribe so you will not miss out on receiving future publications.

- Send an e-mail to [darjonline@dau.mil](mailto:darjonline@dau.mil) and/or [datlonline@dau.mil](mailto: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.



# Swamped by Regulations

Perils of an Ever-Increasing Burden

*Allen Friar*

**T**he Department of Defense (DoD) acquisition process is too complicated, too slow, too expensive and includes too many competing objectives. The ever-increasing new laws, regulations and policies are adversely affecting the federal acquisition process and the ability of federal agencies to provide services and perform their missions.

The regulatory burden has been growing for a long time, but the pace of new regulations has increased at an unprecedented rate in the last few years. According to a May 2013 Congressional Research Service report,

---

**Friar** is a professor of Contract Management at the Defense Acquisition University-South in Huntsville, Alabama. He spent the last 12 years as a DAU instructor and has more than 15 years of contracting experience with the U.S. Army, including the U.S. Army Aviation and Missile Command at Redstone Arsenal in Huntsville.



published regulations have been at historic numbers for the last decade. Contrary to the intended effect, this tsunami of regulations prevents many small businesses from participating in the federal procurement process. In some cases, small firms are withdrawing from participation.

Today, largely because of constantly increasing regulations, many small business contractors are unwilling to compete for federal contracts. Last year, the National Federation of Independent Business randomly surveyed 1,615 small businesses and found their top concerns were health-care costs, regulations, tax complexity and economic uncertainty. The ever-growing regulatory burden raises the cost of doing business and prevents many small firms from entering the market—reducing competition, job growth and innovation.

Tinkering with acquisition regulations or issuing policy directives to emphasize this or that regulation does not resolve the matter. Many of our senior leaders have recognized the problem of overregulation for some time. Frank Kendall, Under Secretary of Defense Acquisition, Technology, and Logistics, in July 2014 testimony

before the House Committee on Armed Services said of the DoD acquisition process, “Our system over time accumulated excessive levels of complex regulatory requirements that are imposed on our program managers and other acquisition professionals.” He added, “One thing I hope we can all agree on is the need to simplify and rationalize the bureaucratic burdens we place on our acquisition professionals.”

Indeed what is needed is comprehensive acquisition reform that concentrates on lean and efficient management, clearly identified requirements and true competition in the marketplace. Constantly expanding regulations, often with competing objectives and declining revenues, imperil the federal acquisition process and the DoD’s ability to accomplish its primary mission of deterring war and protecting U.S. security interests. To remain viable, DoD must get back to its core mission. And reforming the contracting and acquisition process is a vital first step.

An old Chinese proverb states that “The man who chases two chickens catches neither.” Trying to accomplish too many, often competing, objectives



during the acquisition process makes it nearly impossible to buy an airplane, a tank or a battleship. The Air Force refueling tanker contract, ostensibly the Service's top priority, took 10 years to award and is a classic example of the many problems plaguing the acquisition system and the military-industrial complex.

Any student of government knows that the first goal of bureaucratic organizations, usually unstated, is to perpetuate the organization. This is done largely for selfish reasons such as providing opportunities for promotion, protecting and expanding turf and increasing the bureaucracy's importance and thereby getting more resources. The DoD is no stranger to this practice, and the contracting and acquisition community is especially adept at growing the bureaucracy. One way organizations grow is to acquire more responsibilities, and this often involves passage of legislation and the writing of regulations to implement the legislation. This in and of itself has been a growth industry for more than 30 years.

After the end of World War II, the Armed Services Procurement Regulation (ASPR) in 1947 had 125 pages. It continued to grow rapidly and was replaced in 1984 by the Federal Acquisition Regulation (FAR), which was 1,953 pages long. In July 2014, the FAR had 2,193 pages and the DoD FAR Supplement (DFARS) was 1,554 pages long. In addition, each Service—Army, Navy and Air Force—and some other federal agencies have their own FAR supplements and countless policy directives, instructions, guidebooks and memorandums.

On top of all these contracting regulations, we have the DoD Directive 5000.01, "The Defense Acquisition System" and its companion, DoD Instruction 5000.02, "Operation of the Defense Acquisition System," the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System made up of the Joint Capabilities Integration and Development System (JCIDS) and the Planning, Programming, Budgeting and Execution Process (PPBE). None of these is static or unchanging, especially the last one. The 5000.02 recently was revised, almost doubling in size—and other revisions are planned or under way.

The Integrated Defense Acquisition, Technology, and Logistics Life Cycle

Management System process is often called the "Big A" acquisition process and has three parts: the requirement generation part or JCIDS; the Defense Acquisition System or "Little A"; and the PPBE. These three processes originally were designed to be linked and streamlined but over the years have evolved into a system that is anything but streamlined—some would say it is dysfunctional. As former Secretary of Defense Robert Gates said of procurement in 2008 remarks before the Heritage Foundation, "The DoD procurement cycle of adding layer upon layer of cost and complexity onto fewer and fewer platforms that take longer and longer to build must come to an end." In Gates' opinion, this process is unsustainable. It remains to be seen if his warning will be heeded.

Recent DoD acquisition initiatives have addressed some problem areas by allowing urgent responses to wartime needs, bypassing many existing regulations and implementing some Better Buying Power Initiatives to incentivize productivity and industry innovation and to improve tradecraft in the acquisition of services.

The latest initiatives focus on controlling costs and improving workforce leadership and training to change the acquisition culture. And the Joint Requirement Oversight Council (JROC) has cut paperwork requirements and accelerated decision making for new systems development. These changes have been positive, and more are coming. But much more drastic action is needed.

The Defense Business Board in its Fiscal Year 2012 report to the Secretary of Defense found that the "Big A" acquisition

**Figure 1. Number of Pages Published Annually in the Federal Register, 1937–2011**



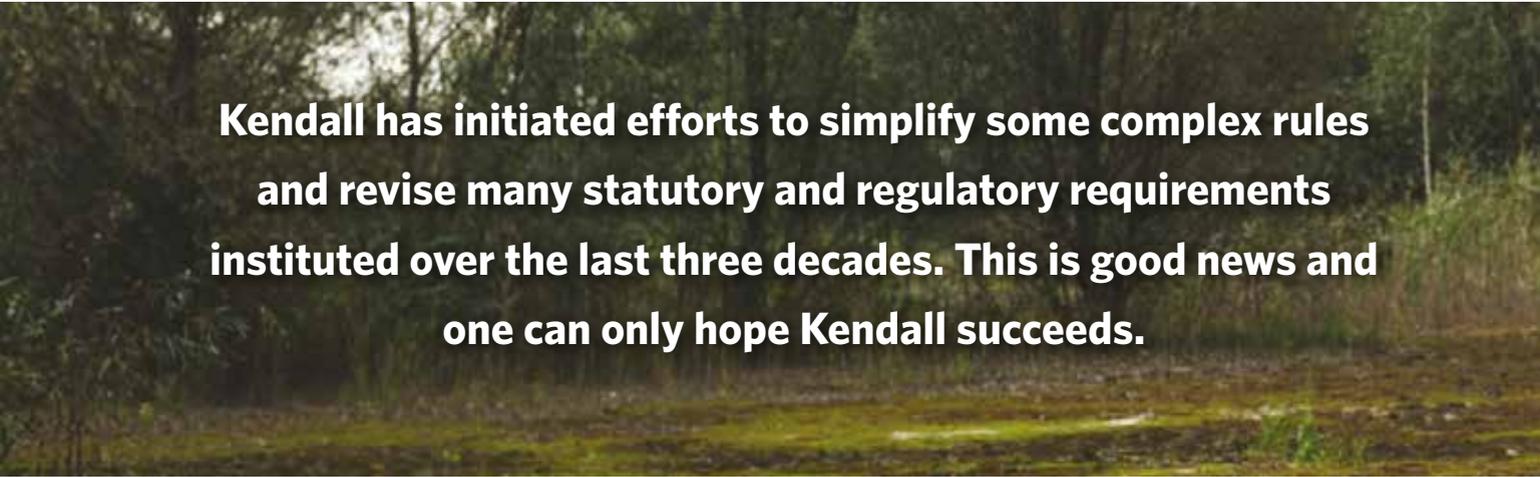
Source: Office of the Federal Register, National Archives and Records Administration, and United States Government Printing Office. Data are not yet available (as of April 10, 2013) for 2012. Chart from a May 2013 Congressional Research Service (Library of Congress) report, "Counting Regulations," by analyst Maeve P. Carey.

system is too complex. Its No. 1 recommendation was to “zero-base” the entire system, including all directives and regulations. The goal was to start over and reduce all three bureaucratic procedures in order to simplify the process.

Kendall has initiated efforts to simplify some complex rules and revise many statutory and regulatory requirements instituted over the last three decades. This is good news, and one can only hope Kendall succeeds. But the DoD has been trying to “fix” its weapon systems procurement process for many

one certainty is that big changes are necessary if the system is to survive and function. It is vital that DoD determine how to equip the acquisition workforce with the tools to navigate the heavily regulated federal acquisition process in a time of upheaval.

Noted author and futurist Alvin Toffler has said that in the 21st century, “the illiterate will not be those who cannot read or write but those who cannot learn, unlearn and relearn.” Currently, the DoD emphasizes training but also recognizes



**Kendall has initiated efforts to simplify some complex rules and revise many statutory and regulatory requirements instituted over the last three decades. This is good news and one can only hope Kendall succeeds.**

years without much success. Past efforts have produced a piecemeal approach, piling one new regulation or policy on top of another, and have led to the current dysfunctional system. Change, however, will not come easy. Stiff resistance to meaningful change can be expected from industry lobbyists and others who benefit from the current system.

The prospect for reduced regulations is remote. In fact, given the proposed changes to the acquisition system and the number of new laws out there that have not been fully implemented, it is much likelier that the deluge of new regulations, not to mention policy directives, will continue for some time. So how can we keep the acquisition process afloat? The answer may lie in the acquisition workforce itself.

Another perhaps equally important and necessary approach to changing the DoD acquisition process and increasing its efficiency is to change the culture of the acquisition organization and its workforce. This will require leadership commitment to bringing institutional change in acquisition workforce behavior. Again, as Under Secretary Kendall has said, there is renewed focus on the acquisition workforce and on streamlining decision making and increasing professionalism.

Education, training and experience all will play a role in transforming the workforce. The Secretary of the Army recently said that Army leaders must be trained to deal with uncertainty and must know “how to think, not just what to think.” He summed up a key difference between training and education, but both are necessary in the acquisition workforce. The

that education and experience are keys to successful performance in the acquisition career field. The challenge of the future will be to educate the acquisition workforce in a way that will prepare its members to think, do research and make ethical decisions in a rapidly changing regulatory environment. Training them to use the available resources and tools for doing their jobs is important. But training them to perform rarely used processes or arcane tasks is of little value in today’s rapidly changing environment.

Many changes are planned for the federal acquisition system, and the DoD acquisition workforce must be prepared to meet this challenge. The DoD is the world’s largest purchaser of goods and services, and what it does will be felt both within the United States and around the globe. The acquisition workforce will bear the brunt of the coming changes. Workforce members are a vital component for change management and must know how to think, not just what to think, in order to respond to rapid changes.

The mission hasn’t changed, but the workforce culture must change to accomplish the mission. That is the message from our senior leaders. Training is important, but workforce members must become lifelong learners—to do research and use the many online resources available to them. As the poet William Yeats said, “Education is not filling a pail but lighting a fire.” Perhaps if we can light the fire and help change the culture, we won’t be overwhelmed. 

---

The author can be contacted at [allen.friar@dau.mil](mailto:allen.friar@dau.mil).



# Why I Won't Be a Prime Contractor

*John Krieger*

**B**ecause I don't have to.

It is as simple as that.

You may wonder why I wrote this article. (Actually, I did too—but probably for different reasons.) So, before we proceed any further, let me provide the genesis. Dr. D. Mark Husband, senior advisor, Root Cause Analyses, Office of Performance Assessments and Root Cause Analyses (PARCA) asked the Defense Systems Management College (DSMC) to gather “subject matter experts” (SMEs) from various career fields to discuss issues related to doing business with the federal government, specifically the Department of Defense. I was invited to discuss contracting issues.

The discussion was in support of the Better Buying Power (BBP) 2.0 effort to achieve greater efficiency and productivity in defense spending. Frank Kendall, Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]),

---

**Krieger** is an intermittent professor at the Defense Systems Management College at Fort Belvoir, Virginia.

sent letters to the chief executive officers of major defense contractors seeking similar information. During one part of the discussions, I made the bold assertion that I wouldn't contract with the federal government as a prime contractor. We discussed that for a time and moved on.

Shortly after that gathering, my supervisor, manager and the dean of DSMC received an e-mail from Dr. Husband on the topic (i.e., Subject: Request for info from John Krieger iso of USD(AT&L) study on "Eliminating Requirements Imposed on Industry Where Costs Outweigh Benefits"). He wanted a white paper on my thoughts and rationale on why I wouldn't contract directly with the federal government. My initial, flip response was "Look at the table of contents of FAR Part 52 and DFARS Part 252. Is that short enough for a White Paper?" He heeded my suggestion. It gave him a headache. But, he asked for more. The "more" is found below.

I make a comfortable living when you consider my salary as a reemployed annuitant, intermittent professor of contract

management at the DSMC, leading sessions of The FAR Bootcamp, and occasional consulting. With the wages and payments I receive, combined with my civil service retirement pay, my income exceeds my needs. Why would I want to inflict contracting with the federal government on myself? Just so we are clear on what I mean, consider the first two definitions of "inflict":

*verb (used with object)* 1. to impose as something that must be borne or suffered: to inflict punishment. 2. to impose (anything unwelcome): The regime inflicted burdensome taxes on the people. (Dictionary.com)

As I am not (particularly) greedy, the answer to the question is, "No reason." If I were younger, more ambitious, it might be different.

Let's look at why I use the term "inflict" in relation to contracting with the federal government. The table in this article compares contracting with the federal government and contracting

**Table 1. Comparison of Federal Government and Commercial Contracting Requirements**

| Federal Government Contracting Requirements   | Commercial Contracting/Subcontracting Requirements   |
|---|--|
| <p><b>Rules:</b><br/>           Federal Acquisition Regulation (FAR)—1,885 pages<br/>           Defense FAR Supplement (DFARS)—1,308 pages<br/>           DFARS Procedures, Guidance and Information (PGI)—657 pages<br/>           Deviations (34)—177 pages<br/>           Air Force Federal Acquisition Regulation Supplement (AFFARS)<br/>           Air Force Materiel Command Mandatory Procedures and Information Guidancel (AFMC MP/IG)<br/>           Air Force Life Cycle Management Center<br/>           645th Aeronautical System Group</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For the Navy, Army or a Defense Agency, everything below the DFARS will be a different set of supplements.</li> <li>For any Executive Agency outside of the DoD, everything below the FAR will be a different set of supplements.</li> <li>Deviations, which have not been published for public comment, may affect me as a contractor.</li> <li>AFMC MP/IG is locked (unavailable) on the FARSite.</li> <li>Page counts as of June 26, 2014.</li> </ul> <p>(For all notes, see "Contra Proferentem and the Christian Doctrine," below.)</p> | <p><b>Rules:</b><br/>           Uniform Commercial Code (UCC)—270 pages</p> <p>Note: The UCC deals with multiple aspects of commerce (i.e., sales, leases, negotiable instruments, bank deposits and collections, funds transfer, letters of credit, bulk sales, documents of title, investment securities, and secured transactions). The portion that would match the FAR's procurement contracts is Article 2, Sales—70 pages.</p>  |
| <p><b>Rate of Rule Change:</b><br/>           77 Federal Acquisition Circulars (FACs) issued since the March 2005 reissuance of the FAR. [Through FAC 2005-77]</p> <p>Changes can be extensive. For example, FAC 2005-73 was 642 pages long.</p> <p>174 Defense FAR Supplement Publication Notices, previously designated as Defense FAR Supplement Change Notices, issued since the January 2008 reissuance of the DFARS. [Through DPN 20141106]</p> <p>(See "Contra Proferentem and the Christian Doctrine," below.)</p>  | <p><b>Rate of Rule Change:</b><br/>           Article 2 of the UCC was issued in 2002.</p>   |
| <p><b>Potential Solicitation Provisions and Contract Clauses that may be used, excluding alternates:</b><br/>           FAR 580<br/>           DFARS 341</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Even with many clauses incorporated by reference, Section I of a Uniform Contract Format (UCF) will go on for pages and pages.</li> <li>Many FAR and DFARS clauses require that they be "flowed down" below the level of the prime contractor. In some instances, that will be to subcontractors, where applicable, at any tier.</li> </ul>  | <p><b>Potential Solicitation Provisions and Contract Clauses that may be used, excluding alternates:</b><br/>           UCC 0</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>On two occasions in the last four years, I have had written contracts containing clauses. One of those two was a subcontract to a federal government contract.</li> <li>There is the potential for the "battle of the forms." You will have experienced this whenever you have made a major purchase (e.g., large appliance, car, home). Read the fine print.</li> </ul> |

in the commercial or private sector. In the right-hand column of each pair, “commercial” does not refer to commercial item acquisition as discussed in Federal Acquisition Regulation (FAR) Part 12, but to contracting with private, for-profit organizations.

In the table, the requirements associated with contracting with the federal government are in the left column and those associated with commercial contracting or as a subcontractor are in the right column.

Not mentioned in the table are some other concerns (e.g., bureaucracy, current competency of federal personnel and their

market knowledge). All have a tendency to detract from the experience of doing business with the federal government.

So, why then do people contract with the federal government?

- It’s the only game in town for them. Some products and services (e.g., tanks, bombers, aircraft carriers) are of such a nature that the federal government is the only customer.
- To diversify their portfolios and protect against downturns, or other issues, in a single market (i.e., having many eggs in many baskets). For example, the Boeing Company building both commercial and military aircraft.

**Table 1 (Continued).**

| Federal Government Contracting Requirements   | Commercial Contracting/Subcontracting Requirements   |
|---|--|
| <p><b>Registering to be able to contract:</b><br/>To do business with the federal government, I was required to get a Tax Identification Number (TIN). In addition to my TIN, I was required to obtain a Data Universal Numbering System Number (i.e., DUNS Number).<br/>Having a TIN and a DUNS Number allowed me to go through the onerous, and time consuming, process of entering my data in the System for Award Management (SAM).<br/>Once entered in SAM, this data must be updated at least annually. Passwords are only good for six months.<br/>Note: Failure to accurately complete the data in SAM could result in a violation of the civil False Claims Act (FCA), which carries a penalty of treble damages.</p>  | <p><b>Registering to be able to contract:</b><br/>I have a TIN for tax purposes.</p>   |
| <p><b>Competition:</b><br/>FAR Part 6 implements the Competition in Contracting Act (CICA), which require full and open completion.<br/>Absent CICA, still “The contracting officer must promote competition to the maximum extent practicable . . .” (FAR 13.104)<br/>No brand loyalty. If you do an excellent job, the best you can hope for is a good past performance review, which may help in a future source selection.</p>  | <p><b>Competition:</b><br/>I have never had to participate in a competition to be selected for contracted or subcontracted work.</p>   |
| <p><b>Contract Formation:</b><br/><b>Time to contract:</b><br/>Days (atypical)<br/>Weeks<br/>Months<br/>Years</p> <p><b>Solicitation/Contract Instrument:</b><br/>Must be in writing.<br/>Can be quite lengthy.</p> <p><b>Proposal Requirements:</b><br/>Proposal requirements for the federal government can be quite extensive. Just completing, or verifying, representations and certifications can be a chore. There will be a requirement for a cost proposal to justify price. Above \$700,000, certified cost or pricing data may be required under the Truth in Negotiations Act, 41 U.S.C. chapter 35. Now referred to in the FAR as “Truthful Cost or Pricing Data.” In addition, there may be requirements for technical and management proposals and others (e.g., risk).<br/><b>Negotiations:</b><br/>Negotiations may be simple or wide ranging. They will probably include discussion of price, including profit. Although there is no limitation on profit or fee, except for cost-plus-fixed-fee contracts, the government will be guided by a “structured approach” for prenegotiation objectives.<br/>Overall, this process can be costly in time and money to the offeror, as can be demonstrated by some of the settlements the government has reached for paying proposal preparation costs.</p> | <p><b>Contract Formation:</b><br/><b>Time to contract:</b><br/>Minutes<br/>Hours<br/>Days (atypical)</p> <p><b>Solicitation/Contract Instrument:</b><br/>Many of my contracts are oral.<br/>Written contracts are quite short. My longest contract was six pages.</p> <p><b>Proposal Requirements:</b><br/>I have only submitted a proposal (i.e., statement of objectives, and price) on one occasion. Total submittal, one page.</p> <p><b>Negotiations:</b><br/>Very limited.<br/>Overall, this process is much less costly in time and money. In the majority of my contracts, this has been negligible.</p> |
| <p><b>Accounting Requirements:</b><br/>As a federal government contractor, I would have to maintain an acceptable accounting system. Depending on the dollar amount and type of contract, that system would be subject to approval and audit. To help, the government provides guidance in the form of Defense Contract Audit Agency Pamphlet No. 7641.90, <i>Information for Contractors</i>. The pamphlet is 100 pages long.<br/>If I got enough business, I would be subject to the Cost Accounting Standards (CAS). Certain contractors and subcontractors are required to comply with CAS and to disclose in writing and follow consistently their cost-accounting practices.<br/>In addition, for cost-reimbursement contracts, Contract Cost Principles are applicable. The cost principles are a set of 46 rules applicable to deciding whether contractor costs are allowable.</p>   | <p><b>Accounting Requirements:</b><br/>I keep an Excel spreadsheet, which is subject to no one’s review, but my own.<br/>I have never been questioned concerning allowability of cost.</p>   |

- To leverage federal government research and development dollars for infusion into commercial products and services.
- The return on assets employed is great in the sense that the government pays you for the assets you employ. If you have many contracts, the rate of return is predictable. Remember that the owners of some government contractor firms are largely widows and orphans and retired public employees, including some from Canada, if you look at the institutional investors.
- Patriotism. I have it from a usually reliable source (one of my brothers) that a major commercial firm built telescopes/

cameras for spy satellites out of patriotism, though the company wasn't allowed to talk about it.

- (Unlike me) for additional money. After all, as Willie Sutton is purported to have said, but didn't, about why he robbed banks, "That's where the money is."

Whatever the reason, there is one thing I do know: If I were to decide to become a prime contractor with the federal government, the first thing I would do is hire someone like me to ensure that I followed the rules. By the way, my mobile phone is 703-772 ---- 

The author may be contacted at [john.krieger@dau.mil](mailto:john.krieger@dau.mil).

**Table 1 (Continued).**

| Federal Government Contracting Requirements  | Commercial Contracting/Subcontracting Requirements   |
|--|--|
| <p><b>Payment:</b><br/>Payment in federal government contracts is governed by the Prompt Payment Act, a statute enacted to delay payment of the government's bills.</p> <p>Payment is the later of:<br/>(A) The 30th day after the designated billing office receives a proper invoice from the contractor.<br/>(B) The 30th day after government acceptance of supplies delivered or services performed.</p> <p>Requires use of electronic funds transfer (EFT), and Wide Area Workflow (WAWF). The WAWF approval process is daunting.</p>  | <p><b>Payment:</b><br/>Payment is much quicker. In most cases, it is my choice whether I am paid by EFT or check.</p> <p>For my most favored customer, if I invoice on Saturday, I am paid before the next Saturday (i.e., less than seven days).</p> <p>Only two customers have required electronic submission of billing information. One of those was a subcontract on a federal government contract.</p>                                       |
| <p><b>Contract Interpretation:</b><br/>Includes standard procedures for contract interpretation (e.g., Order of Precedence Rule, Express Language Rule, Conduct of the Parties, Prior Course of Dealings Rule, Whole Instrument Rule, Contra Proferentem*).</p> <p>In addition to the standard procedures for contract interpretation, in federal government contracting there is application of the "Christian Doctrine."** The Christian Doctrine ignores the "four corners" of the contract to establish meaning.</p> <p>* Used in connection with the construction of written documents to the effect that an ambiguous provision is construed most strongly against the person who selected the language. (Black's Law Dictionary, Sixth Edition.)</p> <p>** A legal rule providing that clauses required by regulation to be included in government contracts will be read into a contract whether or not physically included in the contract, unless a proper deviation from the regulations has been obtained. (<i>The Government Contracts Reference Book</i>, Fourth Edition.)</p> | <p><b>Contract Interpretation:</b><br/>Includes standard procedures for contract interpretation, but no Christian Doctrine.</p>  |
| <p><b>Litigation:</b><br/>This may be the one area in which the federal government excels. The most commonly used (i.e., by the Government Accountability Office, Court of Federal Claims, Boards of Contract Appeals) have a significant amount of statutes, regulations and case law on which to rely.</p> <p>Between protests and disputes, there is a large amount of litigation in federal government contracting. I have been lucky, having only been involved in such litigation on four occasions. A federal government contract can be liable to litigation for a time. In one instance, I was contacted by Air Force lawyers 11 years after I had left the program involved. I was contacted 16 years later in another case.</p> <p>Contractors are subject to the FCA, the "Lincoln Law," which includes treble damages. Under the FCA, qui tam lawsuits can be initiated by whistleblowers who hope to receive a portion of any recovered damages.</p>   | <p><b>Litigation:</b><br/>Litigation is done at the state and local level. Judges may have limited or no experience in contract law. Case law may differ from state to state, locality to locality.</p> <p>Litigation, however, is rare, as parties seek to resolve differences. In some instances, the written word of the contract may be ignored in order to reach a settlement.</p> <p>I have never been involved in a protest or dispute.</p> |
| <p><b>Changes:</b> Federal government contracts contain a changes clause that allows the government to unilaterally change the contract, without the contractor's consent, in specifically enumerated areas. Such changes are subject to an equitable adjustment; however, the contractor must assert its right to the adjustment under the changes clause within 30 days from receipt of the written order. The contractor must continue work, as changed, even if it disagrees that the work should be done.</p>   | <p><b>Changes:</b> All changes must be by mutual agreement of the parties, otherwise it is a breach of contract.</p>   |
| <p><b>Termination:</b> Federal government contracts contain a termination for convenience clause that allows the government to terminate this contract, in whole or in part when it is in the government's interest.</p>   | <p><b>Termination:</b> All terminations must be by mutual agreement of the parties, otherwise it is a breach of contract.</p>  |
| <p><b>Limitation on Allowable Government Contractor Compensation Costs, \$487,000 per fiscal year, adjusted annually.</b></p>  | <p>[It's the thought that counts.]</p>   |
| <p><b>Renegotiation:</b> As if all the above were not enough, if the federal government believes it "got taken," the contract may be subject to renegotiation by a Renegotiation Board.</p> <p>Note: Admittedly, for the three years that I was a member of the Navy's Renegotiation Board we never met.</p>   | <p>[It's the thought that counts.]</p>   |

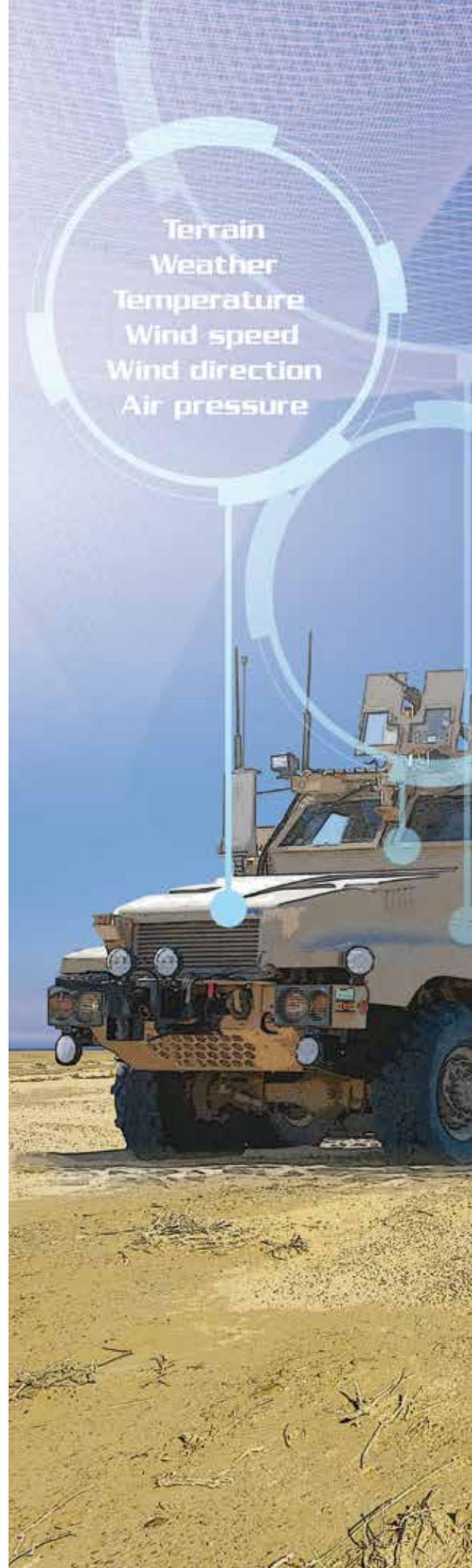
# The Modular Instrumentation Family

Defense and Industry Applications

Gerome Q. Banks

To effectively meet the needs of today's fiscally constrained mission, Department of Defense (DoD) agencies have developed critical ways to do more with less. One way organizations advance in testing is by using modular instrumentation to perform a wide array of data collection, storage and processing across various platforms. The author has explored several broad functions of modular instrumentation within the context of collecting data for government and commercial applications.

**Banks** is the Protocol and External Affairs Officer at the U.S. Army Aberdeen Test Center (ATC) in Aberdeen, Maryland. He has also served in several roles, since 2003, in the U.S. Air Force and the Pennsylvania Army National Guard.



The image shows a line of military vehicles, likely Humvees, parked on a dirt road. Overlaid on the image are three large, semi-transparent blue circles containing text. The top-left circle lists: GPS location, Speed, Fuel levels, Tire pressure, Fluid levels, Ride quality, and # passengers. The top-right circle lists: System reliability, Maintenance sched, and System updates. The bottom-right circle lists: Accelerometer data, Blast survivability, and Rollover prevention. Vertical lines connect these circles to the vehicles below. The background is a clear blue sky.

**GPS location**  
**Speed**  
**Fuel levels**  
**Tire pressure**  
**Fluid levels**  
**Ride quality**  
**# passengers**

**System reliability**  
**Maintenance sched**  
**System updates**

**Accelerometer data**  
**Blast survivability**  
**Rollover prevention**

**The key benefit of ADMAS: It is designed to collect data that can provide valuable, additional insight into the performance of a system undergoing test.**



Family of Medium Tactical Vehicles (FMTV) and High Mobility Multipurpose Wheeled Vehicle (HMMWV) on test course at Aberdeen Proving Ground, Maryland. U.S. Army photo.

### **Defense and Commercial Platforms**

It should come as no surprise that the DoD operates under increasing fiscal constraints and that creative and resourceful Service members and civilians find additional ways to do more with less each day. This is nowhere more evident than at the U.S. Army Aberdeen Test Center (ATC) at Aberdeen Proving Ground, Maryland, where ATC leads a critical effort with its “multi-commodity” approach to testing. This philosophy strives to effectively use integrated testing—performing the greatest possible range of analysis, across an entire platform, through the use of a common instrumentation set.

This common instrumentation, known as the Advanced Distributed Modular Acquisition System (ADMAS), is designed to facilitate rapid data collection, mass storage and near-real time data processing. ADMAS is versatile, supports a wide range of real world applications and is an extraordinarily useful resource for Major Range and Test Facility Bases, like ATC, that supply test efforts across the DoD, other government agencies and commercial industries.

### **ADMAS Versatility**

ADMAS is a complex family of modular instrumentation. With its flexible design, it is available in many sizes, shapes and capability configurations to allow it to be quickly customized to meet a wide variety of rapidly changing test requirements across multiple commodity areas.

The key benefit of ADMAS: It is designed to collect data that can provide valuable, additional insight into the performance of a system undergoing test. Regardless of size, shape or capability configuration, ADMAS instrumentation collects information from systems and sensors that indicate how a product is functioning.

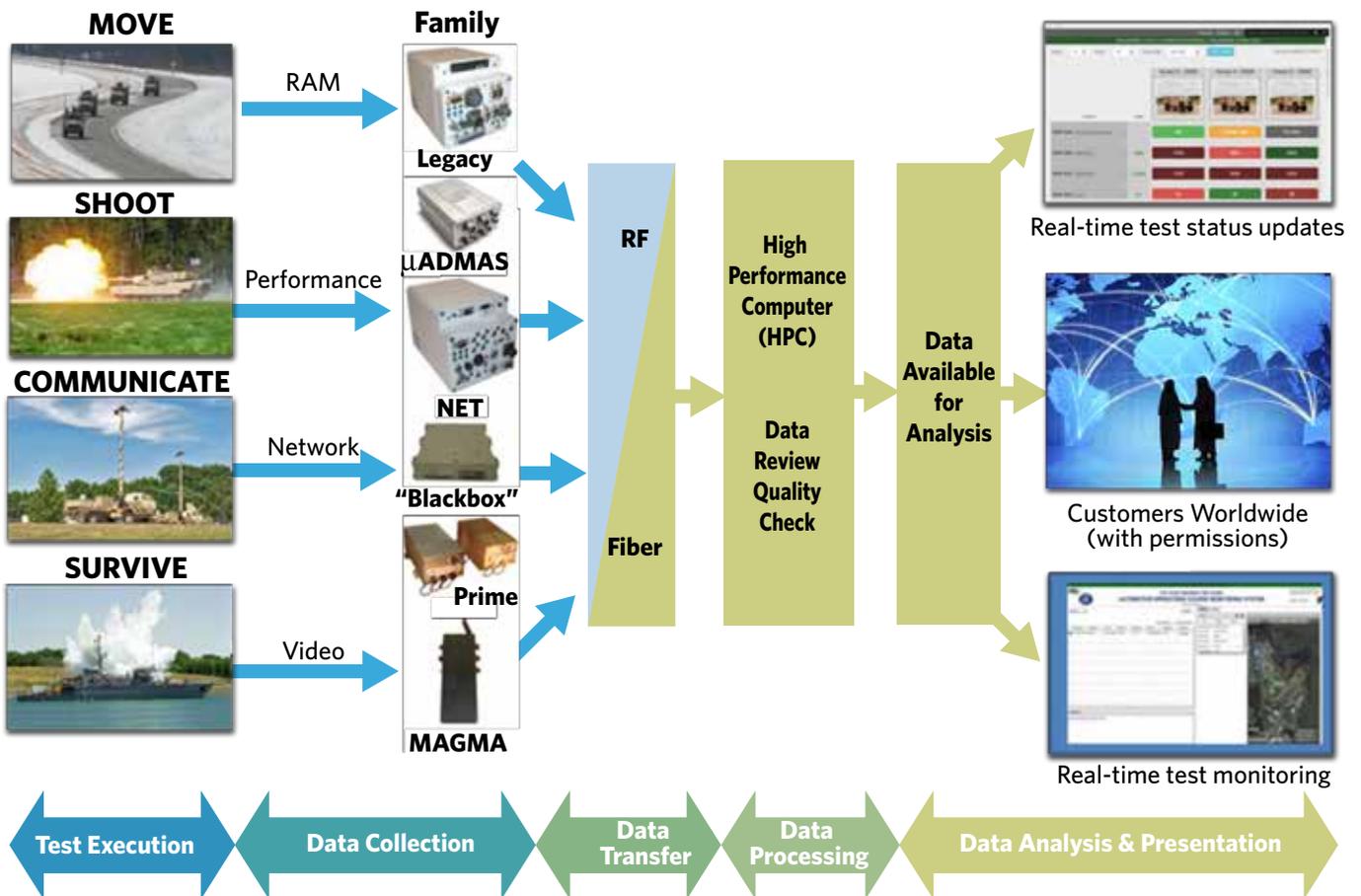
“We break down the information we collect into two main categories, ‘data’ which are raw engineering measurements such as Global Positioning System location, speed or oil pressure, and ‘metadata’ which are used to provide more context to the data and to describe factors about the test that may not be obvious in the raw data, such as weather conditions or terrain profiles,” said Ryan Stowell, the leader of ATC’s ADMAS efforts. “Both data and metadata are critical to getting a complete picture of how the system was being tested.”

### **ADMAS Data Flow**

The data collected from all tests using ADMAS instrumentation are stored in a database that provides the unique and powerful capability to look through the history of an individual system as well as across different platforms for evaluations and comparisons among systems. Stowell explains that the information can then be used by system developers to make critical product improvements.

The goal of the ADMAS family of instrumentation is to improve DoD’s overall testing capability. This includes not

Figure 1. ADMAS Multi-Commodity Test Data Flow



only the collection of data but transportation, processing and storage as well. Collected ADMAS data are processed by way of an intricate central computing hub called a Defense Supercomputing Resource Center (DSRC). The DSRC at Aberdeen, one of five developed by the U.S. Army Research Lab, allows access through high-speed secure networks and provides accessible mass storage for volumes of data. Using this computing center capability allows agencies to process immense quantities of information on multiple computer cores in mere hours, versus the days or weeks required in using only a single computer. The principal benefit of this increased turnaround time is faster, more apt results, using fewer resources, and near-real time relevance in testing for the varied platforms ADMAS supports.

### Real-World Applications

In a test, data are critical in demonstrating and predicting how the system will perform in real-world environments. Engineering data collected, processed and stored are used for many practical applications such as identifying logistical requirements, predicting reliability and maintenance schedules and aiding in future system updates and designs.

ADMAS is used not only for developmental testing but also captures Soldier data through operational testing and theater operations. ADMAS instrumentation has been provided to war theaters such as Iraq and Afghanistan since 2010. An ADMAS called “black box” was designed specifically for collecting data from Mine-Resistant Ambush Protected (MRAP) vehicles in theater.

The black box system was developed using the existing ADMAS architecture to meet the precise requirements of collecting data in a dynamic theater setting. More than 1,200 major MRAP systems have been instrumented with black boxes providing data on more than 267,000 miles—demonstrating systems use under operational conditions.

One extremely important ADMAS feature is that, in addition to basic automotive data (engine parameters, terrain profiles, ride quality information and environmental temperatures), black box captures ballistic accelerometer data that can be used to characterize a system’s response to an explosive impact or rollover. Every blast survivability test on a vehicle at ATC is instrumented with ADMAS so data from in theater

**Every blast survivability test on a vehicle at ATC is instrumented with ADMAS so data from in theater can be compared to controlled test data.**



Boeing 747 undergoing cargo hold vulnerability testing at Aberdeen Proving Ground's Philips Army Airfield in Maryland.  
*U.S. Army photo.*

can be compared to controlled test data, ultimately making systems safer and more resilient for Service members and even commercial users.

### **Broad Defense and Industry Applications**

While the Army boasts a long history of developing, using and improving instrumentation to collect data, ADMAS' versatile application renders it valuable in virtually every DoD arena. In fact, ATC began using the Legacy ADMAS in 1999 after a run during previous years with its predecessor, the Vehicle Performance Recorder. Yet modern instrumentation now is used at many other DoD test centers and in the Network Integration Evaluation. Another 300 systems have been installed with instruments at training sites such as the Marine Corps Air Ground Combat Center in Twentynine Palms, California, for identifying system reliability in long-term training applications.

As a Major Range and Test Facility Base, ATC is a national asset sized, operated and maintained to provide test services to DoD, other federal agencies, state and local governments, allied foreign governments and commercial entities. Consequently, ADMAS models are designed for various types of applications, including traditional tracked and wheeled vehicles, man-portable equipment, unmanned aerial vehicles, watercraft, helicopters and planes. And because it is designed to be architecturally open and flexible, it can even be used on commercial vehicles and nonvehicular applications such as communications equipment and robotic platforms.

One of the first collaborative uses for ADMAS instrumentation was a joint Army-Department of Transportation-private

industry project that provided instruments for commercial tractor-trailer trucks. The instrumentation was designed to collect data about the trucks and the driving conditions as they traveled throughout the United States. Data from the trucks automatically were transferred to the test center daily. As they moved, data were concurrently processed and stored but, most importantly, gave the joint partners the needed input for vehicle fleet analysis.

ADMAS also has been used on several U.S. Navy projects designed to collect data on how ships operate under various conditions. The data provide insight into key nautical improvements. Furthermore, micro ADMAS units have been successfully used in several unmanned aerial vehicle systems in critical events.

### **Conclusion and Outlook**

Whether in MRAPs, tractor trailers or unmanned aerial vehicles using black box or micro ADMAS, accurate test data are imperative for the DoD's critical decision-making process. ADMAS instrumentation's flexibility, reliability and ease of use can help testers conduct concurrent, multicommodity testing to save time and resources while providing developers the opportunity to easily identify areas of improvement. ADMAS instrumentation is thoughtfully designed to meet these data-collection needs. Because the Army owns the complete design of ADMAS software and hardware, it is well positioned to be able to meet the rapidly changing requirements of future DoD and commercial industry systems. 

*The author can be contacted at [gerome.q.banks.civ@mail.mil](mailto:gerome.q.banks.civ@mail.mil).*

# Repair, Replace or Throw Away

## Linking Sustainment Strategies to Data Requirements

William Decker ■ Julianne Nelson, Ph.D.



One of the significant challenges faced by program managers (PMs) is determining what formal data deliverables need to be included in solicitations. Historically, the lack of sufficient technical data and software and the lack of the rights to use them have limited PMs' ability to implement acquisition and sustainment strategies that are competitive throughout a program's life cycle.

Recent acquisition reform efforts have addressed this problem by emphasizing the importance of both managing intellectual property (IP) and adopting an open, modular approach to program design. For example:

- Better Buying Power 2.0 (April 2013) identified "enforcing open system architectures and managing technical data rights" as important strategies for promoting effective competition in Department of Defense (DoD) acquisitions.

---

**Decker** is a professor of Systems Engineering at the Huntsville, Alabama, campus of the Defense Acquisition University (DAU) and the director of the DAU Technology Transition Learning Center of Excellence. His experience includes more than 30 years in government and industry defense programs leading efforts in research, development, acquisition, and test and evaluation. **Nelson** is a principal research scientist with the Resource Analysis Division of CNA Corp. She has 30 years of experience as an economic and financial analyst, including 15 years as a full-time university faculty member and 15 years as an economic consultant to federal and state agencies, nonprofits and small businesses.

- Interim DoD Instruction (DoDI) 5000.02, “Operation of the Defense Acquisition System” (November 2013) added provisions requiring PMs to:
  - Establish and maintain an IP strategy to identify and manage the full spectrum of IP and related issues throughout a program’s life cycle
  - Apply open systems approaches in product designs, where feasible and cost effective

The long-run success of these acquisition reforms requires (among other things) a common understanding of the ways in which initial decisions on program architecture, data deliverables and data rights licenses affect the potential for competitive procurement and sustainment in the future. In this article, the authors explore a significant linkage in this interdependence: the connections between program architecture, data rights and sustainment strategies. We first outline Open Systems Architecture (OSA) as a general policy goal, and then illustrate its implications in the context of both consumer choices and DoD acquisitions.

### Open Systems Architecture as a Policy Goal

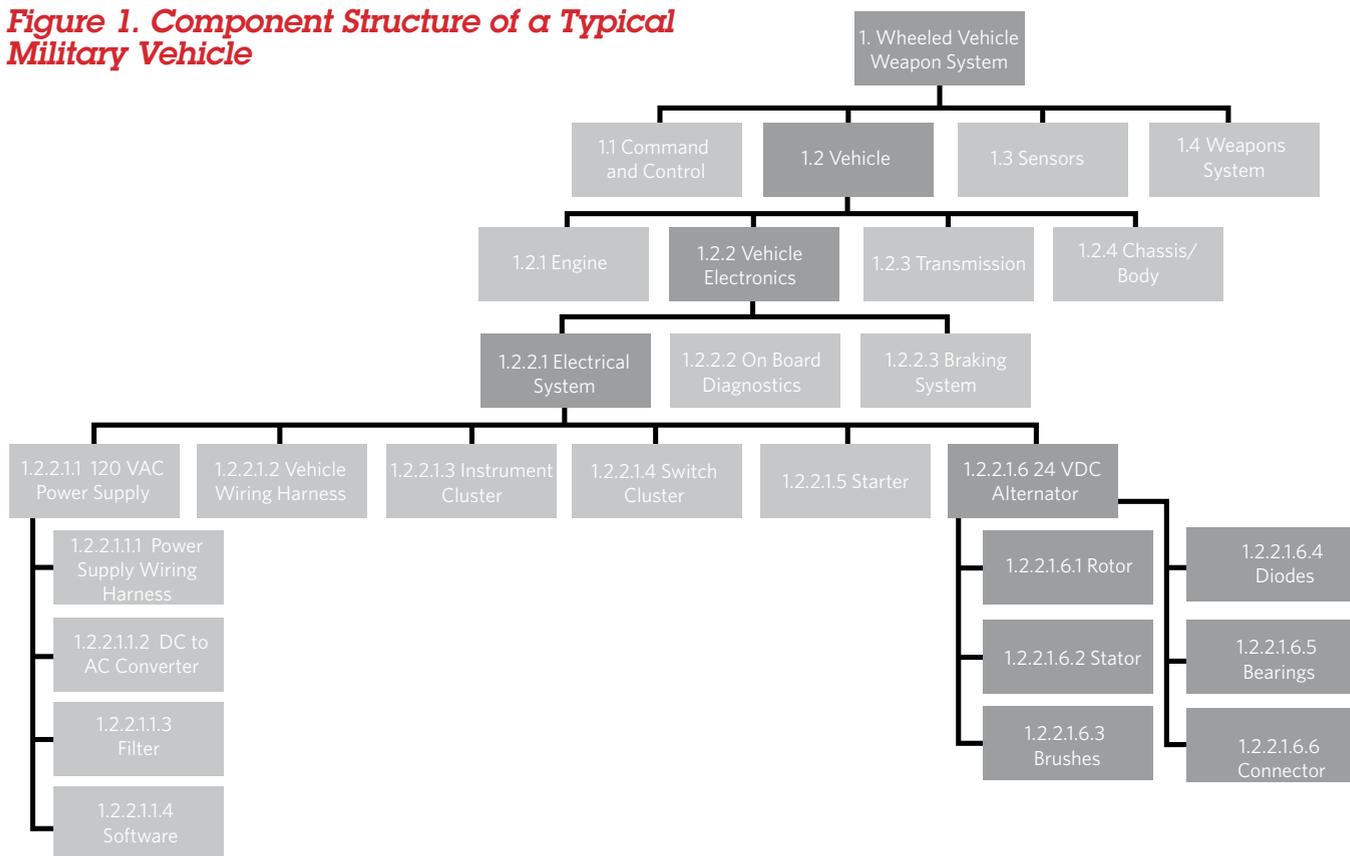
The general objective of OSA is to enable a PM to rely on “one or more qualified third parties to add, modify, replace, remove, and/or provide support for a component of a system” throughout a program’s life cycle (*DoD Open Systems Architecture Contract Guidebook for Program Managers*, p. viii). Reaching this goal depends upon the engineering approach adopted, as

well as the business strategies selected for sustainment and procurement. From an engineering perspective, OSA requires a system that is modular in design, “where functionality is partitioned into discrete, cohesive, and self-contained units with well-defined interfaces that permit substitution of such units with similar components or products from alternate sources with minimum impact on existing units” (*OSA Contract Guidebook*, pp. 137-138). A fully open architecture has interfaces that are public, published and nonproprietary. From a business perspective, OSA requires data (and data rights) strategies that support competition throughout a program’s life cycle, enabling the PM not only to control the cost of the initial system, but also to integrate technological innovations as they become available. In short, OSA is a policy designed to help the government to avoid “vendor lock” (i.e., where only one vendor can respond to the government’s needs).

### Alternator Failure in the Family Automobile

A complete description of OSA requirements and implications is beyond this article’s scope. However, a familiar scenario—the choice of maintenance options for a typical family car—helps identify the types of questions that must be answered when pursuing an OSA strategy. Furthermore, analyzing the linkages between program design, data rights and market forces in this simple context illustrates the types of issues that PMs need to consider as they refine their acquisitions and sustainment strategies for the next generation of DoD weapons systems.

**Figure 1. Component Structure of a Typical Military Vehicle**



Our analysis starts with a description of a vehicle as a system with a specific architecture. Figure 1 is a partial Work Breakdown Structure (WBS) for a typical military vehicle, identifying the components of the major systems and illustrating the hierarchy among them. We assume that a family car would have a similar component structure.

Experienced car owners know that flickering dashboard lights, dim headlights and a “Check Engine” light are symptoms of a failing alternator—component 1.2.2.1.6 in Figure 1. In principle, a car owner who notices such indicators can either buy a brand new car or choose among three basic maintenance strategies:

- Option 1: Take the car back to the dealer for repair.
- Option 2: Buy a new alternator (or get one at a junkyard) and install it (or have a third party install it).
- Option 3: Remove the alternator, rebuild it, test it and reinstall it (or have a third party do so).

Consider the scope of information required for each of the car maintenance options mentioned above.

**Option 1:** If the owner relies on the dealer for repairs, he or she needs little more than an operator’s manual that explains how to interpret warning lights and gauges. Since such manuals are standard equipment—with a cost built into the sale price of the vehicle—the owner generally will have ready access to the information needed to pursue this strategy at no additional charge.

If no further maintenance information is available—or if the car’s warranty requires that all maintenance be done by authorized dealers—the manufacturer is treating the vehicle essentially as a closed system.

**Option 2:** If the owner wishes to buy a new alternator and install it (or have a third party install it), then more information is needed, including complete specifications for a replacement

## OSA requires a system that is modular in design, “where functionality is partitioned into discrete, cohesive, and self-contained units with well-defined interfaces that permit substitution of such units with similar components or products from alternate sources with minimum impact on existing units.”

The relative merits of these options depend on many factors, including:

- The owner’s general knowledge of car repairs
- Competing claims on the owner’s time and budget
- The owner’s access to information about the specific alternator and its interface with the specific make and model of car in question
- The owner’s access to the tools necessary to perform the repairs
- The availability on the open market of replacement alternators, replacement alternator parts and a detailed repair manual

Many of these factors—like market conditions or the owner’s familiarity with car repairs—are determined by factors that have nothing to do with the terms of the original contract negotiated between the current owner and the car dealership. However, the availability of the information needed to follow a given maintenance strategy may well have been determined on the day the car was purchased. For an automobile, access to essential information—and permission to use it—will depend not only on the reporting mechanisms built into the car’s dashboard but also on the terms of the original sales agreement for the vehicle.

alternator and instructions on how to remove, replace and test a new one. More formally, the information required by the public for this maintenance strategy includes:

- All data listed for Option 1
- Full “form, fit and function” data for the existing alternator, such as
  - Mechanical interface (mounting, volume)
  - Electrical interface
  - Power interface (pulley size, shape)
  - Performance specifications, including
    - Power output (voltage, amperage, allowable ranges)
    - Efficiency
    - Acceptable range of revolutions per minute
    - Thermal environment/heat dissipation
- Repair instructions
  - Remove and replace directions
  - Test directions
  - Description of tools/test equipment required

If the manufacturer provides this information to the public at little or no cost, the manufacturer can be said to follow an OSA approach to the design of the electrical system (i.e., component 1.2.2.1)—at least insofar as the alternator

is concerned. This approach enables the owner (or a third party) to use publicly available data to identify and install a suitable replacement component but does not necessarily provide the information required to disassemble the alternator itself and perform repairs.

**Option 3:** A possible third approach is for either the owner or a third party to remove and repair or rebuild the alternator. This maintenance strategy would involve troubleshooting the alternator to determine what is faulty, disassembling it, replacing the defective part(s), reassembling, testing and reinstalling it in the vehicle. For this strategy to work, the technician would need to be able to buy appropriate parts from either the vehicle manufacturer or a parts supplier and have access to more extensive information, including:

### Lessons for DoD Program Offices

Within DoD, a program's life cycle sustainment strategy identifies the maintenance option(s) chosen both for the system as a whole and for its separate subsystems. Although the details differ, the choice of a sustainment strategy for a DoD program follows the same basic logic as the choice of maintenance strategy for the family car. In both cases, success depends on possession of and licenses for essential technical data and/or software. For DoD programs, the availability of this information will depend upon the specific technical data and software actually delivered, the terms of contracts negotiated between a given program office and its various suppliers, and the general legal framework provided by the United States Code and the Code of Federal Regulations (C.F.R.). For a more complete description of the rights to which the federal government is

## Although the details differ, the choice of a sustainment strategy for a DoD program follows the same basic logic as the choice of maintenance strategy for the family car.

- All information required for Options 1 and 2
- "Form, fit and function" (FFF) data (including performance specifications) for the internal parts of the alternator, such as
  - Electrical parts such as diodes, boards, brushes and connectors
  - Mechanical parts such as bearings, rotors and stators
- Alternator repair procedure details
  - Problem diagnosis
  - Disassembly/reassembly directions
  - Test directions
  - Description of tools/test equipment required

In other words, the technician would need detailed information about the internal workings of the alternator in order to make the needed repairs. If the manufacturer provides this information to the public at little or no cost, the manufacturer can be said to follow an OSA approach to the design of the alternator itself (i.e., component 1.2.2.1.6).

Table 1 provides a comparison of the information and parts requirements for the basic options discussed thus far. The question of how to repair a faulty alternator is only one of many that buyers must consider when deciding how they plan to maintain and repair their purchase. In each case, the set of options available to buyers (and their respective costs and benefits) will depend, in part, on the extent to which manufacturers have adopted an OSA approach to vehicle design and sales practices.

entitled to, see Section 2.8.7.6.5 of the *Defense Acquisition Guidebook* (<https://dag.dau.mil>).

The task of choosing a maintenance strategy for a military vehicle can be used to illustrate the common elements of the two planning problems. As with the privately owned automobile, there are three basic options to consider for a specific component such as an alternator:

- Option 1: Have the original equipment manufacturer (OEM) provide all maintenance (for major systems, this option is seldom chosen).
- Option 2: Treat the vehicle's alternator as a "Line Replaceable Unit" (LRU), a "black box" component of the electrical system and plan for maintenance, replacement and upgrades at this level.
- Option 3: Treat the vehicle's alternator as a repairable component and plan for access to the spare parts, tools and data needed for removal, repair, installation and testing.

Once again, these three options imply different data and data rights requirements.

**Option 1:** Even if the OEM provides all maintenance (including repairs and upgrades) over the vehicle's life cycle, military users will need basic information about vehicle operations and maintenance requirements. Under the Defense Federal Acquisition Regulation Supplement (DFARS), required operation, maintenance, installation, and training (OMIT) data are

**Table 1. Information and Parts Requirements for Car Maintenance Strategies**

|   | <b>Option 1:<br/>Dealer<br/>Service</b> | <b>Option 2:<br/>Alternator<br/>as an LRU</b> | <b>Option 3:<br/>Alternator as<br/>Reparable</b> |
|---|---|---|--|
| Operator's Manual                             | ✓                                       | ✓   | ✓  |
| Source of spare alternators                   |   | ✓   | ✓  |
| FFF data for alternator                       |   | ✓   | ✓  |
| Alternator installation and test instructions |   |   | ✓  |
| Sources of alternator parts                   |   |   | ✓  |
| FFF data for alternator parts                 |   |   | ✓  |
| Alternator repair and test instructions       |   |   | ✓  |

delivered with unlimited rights. The government can also specify the standards (military or commercial) that certain systems and/or subsystems must meet.

**Option 2:** Removal and replacement of LRUs (such as an alternator) can be performed by the OEM, government workforce or third-party contractors:

- If system development followed OSA design principles down to an LRU level of detail:
  - The government would require FFF data for each LRU as well as FFF data concerning the interface between each LRU and the rest of the vehicle. Under standard DFARS contract clauses, these data would be delivered with unlimited rights. This information is normally incorporated into interface control documents (ICDs) developed by the vehicle designer, whether the design was paid for by the government or by the contractor.
  - As in Option 1, the government would have unlimited rights to OMIT data delivered with the vehicle.
- To enable this approach, the government must define the LRUs for the vehicle in the request for proposal (RFP) and require delivery of FFF data (ICDs) for each LRU.
- Usefulness of this strategy also will depend on existence of competing LRU suppliers and qualified support contractors.
- Unless additional data are delivered, government personnel and support contractors (other than the OEM) do not have sufficient information to repair the LRUs.

**Option 3:** The life-cycle sustainment and acquisition strategies provide for the repair or upgrade of the individual LRUs, plus the maintenance options discussed in Options 1 and 2. This would be required of an architecture that is open down to the individual part level.

- The government must require delivery of technical data for each part that could be repaired or replaced.
- If the government paid for the development of the vehicle, the government would be entitled to unlimited rights for all

data delivered under the contract. If the contractor developed, at its expense, some or all of the vehicle, it has the option of asserting limited rights for the data associated with the portion it developed outside the government contract or of asserting restricted rights for software developed exclusively at private expense. The contractor must clearly segregate the data pertaining to the exclusively privately funded development from that associated with the government-funded effort.

In addition, the system's acquisition strategy may include the plans to upgrade the system in the future to provide additional capabilities and address new requirements. The ability to incorporate new or improved technology is frequently part of the acquisition strategy. Using our alternator example, if industry developed new, low-friction bearings for the alternator (thereby reducing fuel consumption), how would the PM desire

to take advantage of this new technology? The choice—buy new alternators or buy new bearings and rebuild the existing alternators with government assets—will determine what technical data are required to be delivered to enable the desired upgrade approach.

The PM may elect to treat some components as consumables, as nongovernment repaired LRUs, or components that will not be upgraded or modified, while other components of the system are considered "repairable" or able to be modified by the government or support contractors. Once this determination is made by the PM and the PM's integrated product team members, the technical data and software delivery requirements can be determined. It is not sufficient to simply require the delivery of a general Technical Data Package (TDP), as this does not necessarily contain the technical data and software that will be required for the sustainment strategy chosen. (MIL-STD [Military Standard] 31000A provides a definition of the contents of a TDP.)

To implement an open systems architecture, the PM—together with the systems engineer(s)—must incorporate several different (and sometimes competing) requirements in the analysis of alternative systems architectures:

- Life-cycle sustainment strategy
- Acquisition strategy (including plans for upgrading and adding capabilities)
- Existing military and commercial standards
- The level at which the government wants to implement an OSA (may be different for different components of the system)

Additional information and guidance can be found in the *OSA Contract Guidebook*, available at the Defense Acquisition University/Acquisition Community Connection website (<https://acc.dau.mil/osaguidebook>). 

The authors can be contacted at [william.decker@dau.mil](mailto:william.decker@dau.mil) and [nelsonjb@cna.org](mailto:nelsonjb@cna.org).

# Securing Cyber Acquisitions

Michael Cook

Technology touches the lives of almost everyone in today's world. Our society has embraced all forms of emerging technologies and has thrived from the benefits provided. Personal and professional cellphones have proliferated and enriched the lives of typical Americans. Social networking provides 24-hour access to data and information between friends and strangers alike.

Technology also has played a significant role in the world's economy and in the control and management of America's critical infrastructure, including the power grid, logistics and supply lines and the water supply system. The aggregate of technology that allows these capabilities is encompassed within the definition of cyber and is inherent in most of our acquisitions today.

Yet, with all the benefits of technology, there are many emerging dangers that we are only beginning to identify and that we struggle to address. Acquisition professionals have witnessed the challenges firsthand. Issues such as protecting the integrity and confidentiality of data as well as the critical U.S. defense infrastructure are today at the political forefront. Other nations actively seek to steal our capabilities in order to close the cyber gap we now enjoy. Many reports and articles point to the desires of other nations to expand their influence in the world arena. One way to do this is to gain access to the technological developments that the United States has spent so handsomely to acquire over the years.

---

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



Unfortunately, we are not competing on a level playing field with other nations. We have laws that prevent us from actively stealing trade secrets, intellectual property and military technology; other nations do not. One of the most significant issues that Information Technology (IT) professionals constantly strive to address is information assurance and the protection of sensitive data and associated cyber assets.

Traditionally, managers have sought to protect data, to ensure that it is not accessed or tampered with. IT managers have implemented numerous mitigation strategies to prevent hackers, competitors and rogue agents from gaining access to technology data and information systems. However, the industry's philosophy has shifted recently as the focus has expanded.

The IT industry has come to learn that denying access to data and IT systems is not enough. Foreign states and agents now are motivated by socioeconomic and political interests to expand the breadth and width of network attacks on public infrastructure, critical supply lines and installations that house and process food and water sources. Today's modern hacker has developed the desire and motivation and technical proficiency for gaining access to large networks critical to national and political interests.

Malware is released into the environment daily to carry out these attacks. Malicious code has been a common method, specifically through one system that connects with others. The industry has seen much debate concerning many attacks on our critical infrastructure, attacks via supervisory control and data acquisition (SCADA) systems as well as other types of industrial control systems. Inherent vulnerabilities, and therefore risks, are associated with SCADA systems that have saturated the infrastructure management industry throughout the world. Although SCADA systems are prevalent, industry professionals have not focused on securing them from attack.

Over time, these vulnerabilities have been discovered and exploited, in many cases without the knowledge of those tasked with managing the systems. The predominant point of view for many years appears to have been that SCADA systems can be ignored because other systems, networks and data are more important and require the professionals' attention and focus. Unfortunately, a large-scale attack stemming from malicious code could spread rapidly from one network to another among the networks considered noncritical. The resulting vulnerabilities present the added risk of the attack spreading to larger, critical networks that monitor and control the nation's critical infrastructure.

This becomes even more significant when one realizes that many of our facilities are supported by commercial providers for key services such as fire monitoring. A facility's remote fire-monitoring system may not be considered when acquiring a cyber system, but once that system is installed the facility becomes vulnerable if the fire-monitoring system is

hacked and reports normal conditions even while the building is engulfed in flames—thereby rendering the cyber system useless.

Fortunately, a number of SCADA industry standards can be implemented to mitigate the vulnerabilities within these systems. And recent events and advances in technological capabilities have made that mitigation critical to our national and economic interests. Unfortunately for the United States and many other countries, it appears many systems have failed to implement the best practices.

However, we now seem to be taking these vulnerabilities more seriously, from a defensive as well as an offensive standpoint. Members of the cyber and acquisition communities are familiar with the Stuxnet malware that reportedly destroyed 1,000 centrifuges that were being used by Iran to enrich uranium. The Stuxnet deployment renewed interest in protecting SCADA systems and in defending against cyberattacks on our critical networks. Essentially, our nation acknowledged that cyber was an area of warfare that could be both used against our enemies and used by our enemies against us.

There has been a paradigm shift in how we view network and cyber acquisitions. There is a growing awareness of attacks on cyber systems and critical infrastructure.

Another significant issue is the rapid development and evolution of the technology used for our cyber acquisitions. Mitigation efforts against current threats and vulnerabilities often come much later than the identification of those threats, leaving the industry struggling to play catch-up. Even more dangerous are threats and vulnerabilities that are not identified until serious damage has been done. Moreover, in today's daunting economic environment, many organizations look at cyber budgets as areas to cut back. And many top-level managers and members of the acquisition community do not understand the importance of funding and developing a robust cyber capability with a strong information-assurance suite.

One strategy used by the Department of Defense (DoD) in recent years to mitigate cyber attacks has been contracting out the requirement to the IT industry and paying the private sector to protect critical cyber systems. The industry possesses a great deal of experience and talent and at times is better suited to perform the tasks associated with cyber defense than is the military. Unfortunately, the cost is high at a time when military budgets are shrinking and our economy is still recovering from a severe downturn. In addition, when it is decided to contract out for cybersecurity or network and data services, some control is lost. This poses a significant issue for our military and the sensitive and classified data associated with it. The challenge will come in finding partners that are receptive to a comfortable middle ground where the mission of the military is met and the contracted services are provided by industry.

When services are contracted out, critical tasks performed by the government include contract monitoring, oversight and maintenance. Experienced contracting officers and knowledgeable contracting representatives are important in this work. A critical tool of contracting is the contract itself—or related documents that identify the contract requirements.

As we have seen, many serious threats exist to our networks, systems and data, and these threats grow every day as technology continues expanding and developing. Rapid technological change and our inability to keep pace both ensure that the threats will continue to exceed proactive measures against them. However, the goal of those in the acquisition industry is to develop methods to protect the cyber space in the absence of our ability to stay ahead of technology. Regardless of whether the industry or government agencies develop the methods, the benefit will be experienced by everyone.

Threats to our networks and our data affect us all—socially, economically and politically. The focus must be to eliminate as many threats as possible and to acknowledge that vulnerabilities exist all around us, not just in large facilities that maintain network devices and store data. It, in fact, includes the support systems and software that run our critical national infrastructures and enable our cyber capabilities.

From the defense acquisition standpoint, a closer look is needed at the support systems when cyber capabilities are

acquired. Facility support systems such as remote monitoring and fire-suppression systems must be evaluated—along with the electrical power system's security.

Cyber systems require a comprehensive environmental analysis to be truly secure and hardened in a manner that will protect our cyber investment as well as provide the needed capability. This challenge requires that the information assurance effort be designed into the cyber acquisition. Although the current acquisition doctrine calls for early involvement on information assurance, we often find lacking either the expertise or a concentrated effort. The DoD needs to attract and develop more information-assurance professionals who possess the knowledge and skills associated not only with information assurance but with managing defense acquisition projects and programs—and who also are familiar with emerging technology.

A great deal of effort will be needed to perform this level of diligence; however, the acquisition community is not in this endeavor alone. As attention increasingly focuses on securing acquired cyber assets, the demand for enhanced security and protection will continue growing. As a result, the future will require a comprehensive environmental-analysis approach in cyber acquisitions. For the acquisition community, an early and proactive approach increasingly is imperative. &

The author can be reached at [cookm49@hotmail.com](mailto:cookm49@hotmail.com).

# PROGRAM MANAGERS e-TOOL KIT

<https://pmtoolkit.dau.mil/>

*The Program Managers e-Tool Kit provides the program management resources of the popular print Program Managers Tool Kit in a dynamic Web-based format.*

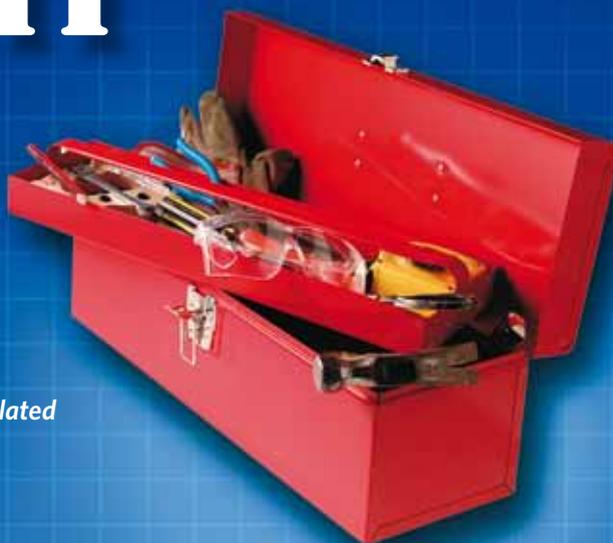
**The e-Tool Kit features:**

- ✓ Continual content updates
- ✓ Live policy links
- ✓ Links to informative ACQuipedia articles and related communities of practice.



Visit

<https://pmtoolkit.dau.mil/>  
today to explore this convenient tool!



# 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](mailto: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.

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.

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](mailto: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](http://www.dau.mil).



***Learn. Perform. Succeed.***