

www.dau.mil | November-December 2017



*Defense*

# AT&L

Acquisition, Technology and Logistics

A PUBLICATION OF THE DEFENSE ACQUISITION UNIVERSITY



## Product Support Should-Cost Opportunities

**How to Write a Good  
Risk Statement**

**AcqDemo Aids  
Acquisition  
Mission Success**

**SPECIAL SECTION:  
IT/Cybersecurity**

# CONTENTS

## 2



### **Product-Support Should-Cost Opportunities O&S Strategies to Boost Affordability**

*Marty Sherman and Bill Kobren*

Should-Cost savings opportunities exist in both product-focused and process-focused operating and support activities and throughout all phases of a program's life cycle.

## 10



### **How to Write a Good Risk Statement**

*James Thompson and Stephen Stump*

Well-structured risk statements help all stakeholders better understand program risks, and they facilitate system engineering plans and communications.

## 14



### **AcqDemo Aids Acquisition Mission Success**

*Scott Wortman*

The Acquisition Workforce Personnel Demonstration project evaluates employee contributions to mission success, rather than tenure. This helps improve acquisition performance.

## 19



### **Streamlining the Contract Award Process**

*Interview With Army Contract Writing  
Product Manager LTC Rob Wolfe*

*Gregory B. Gonzalez*

The Army Contract Writing System and the Army Contracting Command in Illinois implemented several innovative methods to speed initial contract awards. Their ideas can be used by other program managers.

## 26



### **Tabletop Exercises for Added Value in Affordable Acquisition**

*Eugene A. Razzetti*

Tabletops help improve team responses to disaster preparedness and emergency planning. They can help improve program management.



33



### The Quest for Defense Cybersecurity

*John A. Shaud, Michael G. Lilienthal, Scott Thompson and David Brown*

Many major weapons programs have difficulty negotiating the many directives and guidance to develop cybersecurity requirements and strategy. Here's a way forward.

39



### Safeguarding Federal Data

*Janel C. Wallace, J.D.*

Following multiple successful cyberattacks, DoD program managers must become familiar with emerging new rules for safeguarding federal information.

44



### Better Communications on IT Spending Risks

*Robert D. Frum, DCS*

There are ways to consider a broader range of possible outcomes when making information technology investments.

ALSO

38

### MDAP/MAIS Program Manager Changes

48

### Statement of Ownership



Defense

AT&amp;L

Vol XLVI

No. 6, DAU 259

Published by the

DEFENSE ACQUISITION UNIVERSITY

*Under Secretary of Defense for Acquisition, Technology, and Logistics*  
Ellen Lord

*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

*Art Director*  
Tia Gray

*Online Content Editor*  
Collie J. Johnson

*Copy Editor/  
Circulation Manager*  
Debbie Gonzalez

*Production Manager*  
Frances Battle

*Editorial Support*  
Noelia Gamboa  
Michael Shoemaker

*Online Support*  
Nina Austin

**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/publications/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 fax or e-mail the subscription form in this issue, or download the form at <<http://dau.dodlive.mil/files/2015/04/Online-Subscription.pdf>>.

#### Privacy Act/Freedom of Information Act

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

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

#### POSTMASTER, send address changes to:

DEFENSE AT&L  
DEFENSE ACQUISITION UNIVERSITY  
ATTN: DAU PRESS STE 3  
9820 BELVOIR ROAD  
FT BELVOIR VA 22060-5565

#### Disclaimer

*Defense AT&L* magazine promotes the free exchange of ideas. The views expressed are those of the authors and do not reflect the official policy or position of Defense Acquisition University, the Department of Defense, or the United States Government. Articles are in the public domain and may be reprinted or posted on the Internet. When reprinting or posting, please credit the authors and *Defense AT&L*.

Some photos appearing in this publication may be digitally enhanced.



# PRODUCT SUPPORT **Should-Cost** Opportunities

## O&S Strategies to Boost Affordability

Marty Sherman ■ Bill Kobren

**M**uch has been written about “Should Cost” in recent years. Department of Defense (DoD) policy and guidance are replete with both requirements and examples. Yet product support and sustainment Should Cost remains a mystery to many in the acquisition workforce. Let’s shed some light on the subject.

Start with what we know. Should Cost is defined in policy (DoD Instruction [DoDI] 5000.02, Enclosure 2) as “a management tool designed to proactively target cost reduction and drive productivity improvement into programs. Should Cost management challenges managers to identify and achieve savings below budgeted most-likely costs.” Or as the *DAU Glossary* indicates “... a program’s “Should Cost” target represents what the program manager believes the program ought to cost if identified cost saving initiatives are achieved.”

That’s all well and good, but what does that mean for my product support and sustainment strategy? And, perhaps more importantly, how exactly do I identify and implement Should-Cost opportunities for my program?


A great place to start is Chapter 4 of the *Defense Acquisition Guidebook* (DAG), available on the DAU website at <https://shortcut.dau.mil/DAG/CH4>. Here program managers, product support managers, and life-cycle logisticians will find detailed information on operating and support (O&S) Should-Cost initiatives for every phase of the life cycle.

The DAG identifies not just the what, but the how, reminding us in paragraph 3.2.4.1.3 that “the PM [program manager] should record all O&S Should-Cost initiatives in the life cycle sustainment plan (LCSP)” and that “O&S Should Cost initiatives are a way for the program to meet established O&S Cost affordability constraints. However, the PM should not stop developing and implementing O&S Should Cost initiatives if/when the O&S Will Cost estimate is lower than the O&S Cost Affordability constraint. PMs use O&S Should Cost initiatives as an ongoing way to improve the O&S Cost and performance of the system.”

---

**Sherman** is a learning director for product support integration in the Defense Acquisition University (DAU) Logistics and Sustainment Center at San Diego, California. **Kobren** is the director of the Logistics and Sustainment Center at DAU’s Fort Belvoir, Virginia, campus.





... [T]he magnitude of O&S cost makes it a particularly important target for programs planning to apply Should-Cost procedures and management.

The DAG also includes a number of notional examples, including: multi-vendor competition for supply support, investigating potential cost drivers based on design parameters, process improvements to reduce component repair times, and processes to evaluate whether O&S Should-Cost initiatives are delivering expected savings, among a range of others.

Additionally, Chapter 4 of the DoD *Operating and Support (O&S) Cost Management Guidebook* (<https://shortcut.dau.mil/JST/cost-guidebook>) provides an excellent overview of O&S Should Cost, along with a plethora of specific examples and in-depth information on analysis, development, documentation, oversight, tracking, assessment and reporting of O&S Should-Cost initiatives.

As the *O&S Cost Management Guidebook* reminds us, “the magnitude of O&S cost makes it a particularly important target for programs to apply Should Cost procedures and management. Since many drivers of O&S cost are determined by decisions made early in the acquisition process, program managers (PMs) and their staff need access to the best tools and practices available.” Several excellent examples of potential Should Cost enablers are addressed in detail in paragraph 4.2.1.6. Those examples and more will be discussed later in this article.

More generally speaking, analysis indicates the majority of O&S Should-Cost opportunities fall into the three broadly based areas of people, parts and fuel. If we apply the Pareto Principle, it would be logical to focus our Should-Cost energies there. How, you might ask. Great question.

A key step is to devise system acquisition and product support strategies that meets the warfighter’s performance requirements while minimizing and mitigating these areas. This can be achieved in several ways. From a product per-

spective, designing and fielding more reliable, maintainable, supportable, sustainable, suitable and transportable systems would by extension positively impact a range of other product support elements such as maintenance planning and management, supply support, packaging, handling storage and transportation (PHS&T), manpower and personnel, facilities and infrastructure, and training requirements. Result: Reduced O&S costs. Similarly, fuel, particularly petroleum-based fuel, is bulky, necessitating a large support infrastructure, transportation requirements and logistics footprint. Reductions in such requirements through fuel efficiency and alternative fuel initiatives can provide the same result: Reduced O&S costs. These efforts involve impacting the product by designing and developing supportable systems.

Processes can also be designed and developed to more effectively and efficiently support and sustain fielded systems. This includes a range of multidisciplinary sustaining engineering initiatives as well as improvements in management of the supply chain, product support, maintenance, information technology (IT) and data. Process-related examples include: a more responsive supply chain, robust deficiency reporting or proactive obsolescence mitigation processes.

To be successful, acquisition professionals need to adopt a holistic, interdisciplinary, truly life-cycle perspective, considering a diverse mix of product- and/or process-related initiatives such as but not limited to:

### **Product-Focused O&S Should-Cost Opportunities**

**Early, Upfront Investment in Reliability, Maintainability and Supportability.** Often, the greatest opportunities to save costs are manifested well before a weapon system is produced and deployed. Giving due consideration to reliability and maintainability and electing to pursue thoughtful trade decisions in the design affords the opportunity to reap tremendous life-cycle cost (LCC) savings. We like to talk about “upfront and early” since, notionally, 80 percent of O&S costs are determined during design development. Judicious investments in supportability analysis tools is key to enabling good trade decisions. Reliability centered maintenance (RCM) allows for determining the best trades between the cost for reliability in design and development versus cost on O&S. Condition based maintenance-plus (CBM+) can also complement RCM and identify cost effective monitoring and sensing systems to the cost of component failures and induced failures. The trades are not limited to selecting the components that provide the best reliability (cost considered). Maintainability-related trades also can yield significant cost savings.

**Failure Reporting, Analysis and Corrective Action System (FRACAS).** RCM and CBM+ are not simply cost-savings initiatives during initial maintenance planning. They have the potential to deliver additional savings throughout the life cycle. Most programs have some sort of FRACAS, which enables identifying potential changes in RCM plans. If

failure data indicate components are not reliable, consider inserting preventative maintenance to improve the mean time between failure and avoiding the cost associated with unexpected failures. You can also reduce forced removal times which will provide savings on unplanned maintenance and induced failures of other components. If FRACAS data indicate there are no failures, or there is significant remaining life during the current schedule for removals and/or inspections, then the period of use can be extended, saving considerable costs. This same activity can be applied to calibration items. Field and usage data can be used to identify the most likely candidates to transition from RCM to a CBM+ construct to minimize unnecessary maintenance and to reduce service costs. Each determination should be based on using an appropriate model feeding a cost benefit analysis.

**Prognostics and Health Management (PHM).** An integral part of CBM+, PHM is a comprehensive system for detecting and isolating failures as well as predicting remaining useful life for critical components. There are costs associated with implementing a PHM system—but much like RCM and CBM+, the benefits can be significant. The main cost benefit is due to a reduction in the assumed unscheduled and fixed-interval scheduled maintenance based on the precursor-to-failure and life-consumption monitoring PHM capabilities.

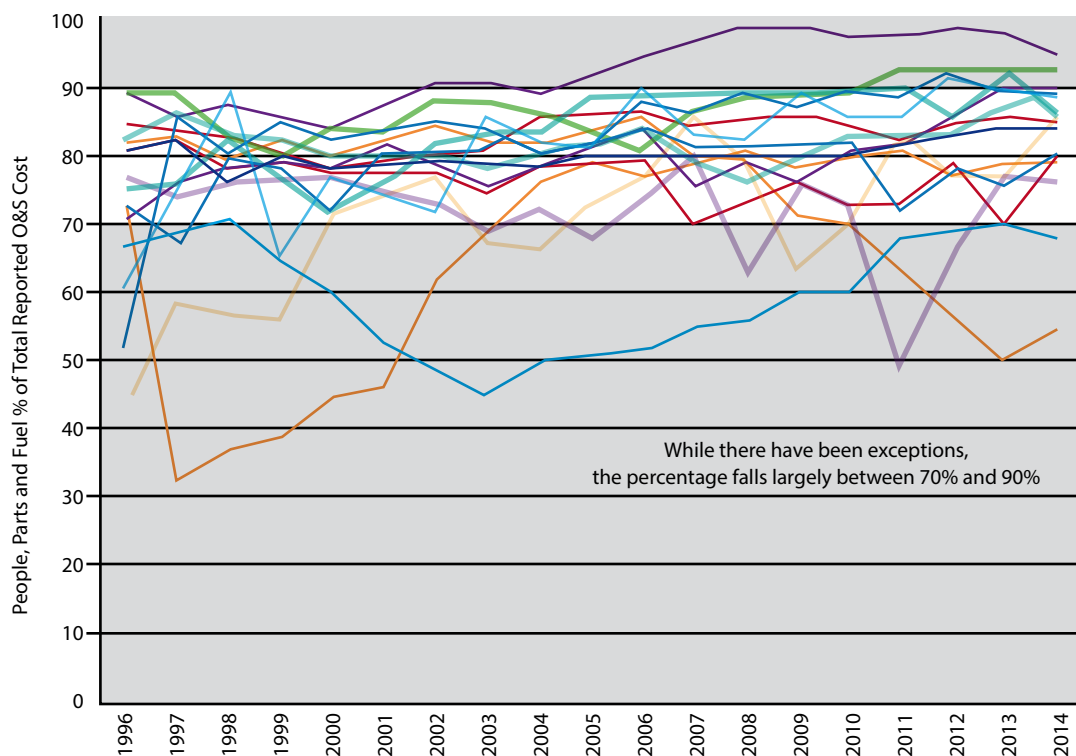
**Parts Standardization and Commonality.** As noted in the DoD *SD-19 Parts Management Guide*, the average total cost for adding a single new part into a system is about \$27,500. Giving preference to standard parts reduces the cost of cataloging new parts. Use of standard parts also leverages existing supply chains, with price breaks for bulk purchases and reduced inventory requirements. Giving preference to standard can reduce the likelihood of Diminishing Manufacturing Sources and Material Shortages (DMSMS) issues and resolution costs. Parts standardization can even reduce training costs and the

need for peculiar support equipment. The usual cost benefits of parts commonality extends to the use of common tools and support equipment.

**Value Engineering (VE).** VE is not an option; it is a requirement by statute and policy. Contractor-submitted Value Engineering Change Proposals (VECPs) are designed to lower a project's life-cycle cost to DoD while improving producibility, reliability, maintainability and, if properly executed, ultimate system availability. VECPs are applicable to all contract types, including performance based. If a VECP yields cost savings, it should be reported as Should-Cost savings. This a wonderful marriage of Continuous Process Improvement (CPI) and Should Cost. The Navy's Logistics Engineering Change Proposals (LECPs) seek to achieve similar benefits as VECPs, but with an emphasis on changes that will save on product support costs or enhanced logistics capabilities. Service life extensions, identification of replacement parts with better reliability/maintainability, changing maintenance tasks that reduce damage to equipment, consumption of material or hazardous wastes (HAZWASTE) generation are all VECPs/LECPs that can be reported as Should-Cost initiatives.

**Fuel and Energy Efficiencies.** Tremendous savings can be realized by eliminating or reducing energy needs or by seeking less-expensive energy alternatives. There are two primary, broad approaches: changes in practices and procedures and

**Figure 1. Distribution of Should-Cost Opportunities**



Source: DoD O&S Cost Management Guidebook, Figure 11—Percentage of total program O&S cost driven by people, parts, and fuel (inclusive of contractor logistics support and depot) since 1996 for 17 aircraft programs).

investments in technologies. Required operational checks, which consume energy without contributing to a warfighting mission, should be scrutinized. One aircraft eliminated a functional check flight in cases where a known good engine received from supply was installed and passed all ground checks. Can simulators and test procedures reasonably substitute actual operation? New technologies may include new means of propulsion (fuel cells, hybrid engines, and batteries), more fuel-efficient engines, lightweight and stronger materials, new designs, enhanced payloads and subsystems, and even directed energy weapons. The use of additive manufacturing (AM) technologies may allow for reduced fuel/energy requirements by reducing material moving through the supply chain.

**Hazardous Materials (HAZMAT)/HAZWASTE Management.** Designing, developing and fielding systems that are more sustainable and environmentally friendly saves money. There are numerous cost savings opportunities in HAZMAT and HAZWASTE. A requirement to perform maintenance without disturbing a low observable surface goes beyond improved availability due to reduced cure time requirements, but there is a dramatic reduction of HAZMAT and HAZWASTE produced in performing routine maintenance. The cost of PHS&T and disposal of HAZMAT/HAZWASTE in many cases may exceed the cost of engineering to find more sustainable alternatives.

**AM.** According to the Joint Technology Exchange Group (JTEG) “additive manufacturing also referred to as 3D printing, is a layer-by-layer technique of producing three-dimensional (3D) objects directly from a digital model. AM increasingly is used for maintenance and repair of damaged parts, particularly for products for which a long lead time or expense is associated with procurement of new parts. The ability to repair metal parts to near-new shape has significant advantages over manufacturing new parts, particularly large parts where only a small portion has been damaged.” Once AM policies, guidance, standards, engineering approval, and materiel disposition procedures are fully embedded into the DoD’s culture and Service manufacturing, maintenance, engineering, supply chain, and workforce training, AM has the long-run potential to be one of the most powerful product support Should-Cost enablers.

**Logistics Footprint Reductions.** Moving, storing, maintaining, packaging, protecting, managing, and sustaining stuff is expensive and often manpower intensive. Look for initiatives to reduce the so-called “tooth to tail” ratio. Leveraging “sense and respond” strategies, can facilitate strategic placement of shared pools of assets accessible and expedited through available distribution networks for identified needs. Just-in-time (JIT) inventory management, supported by readiness-based sparing and lean supply chains, can reduce the inventory. Judicious manning and equipping for on-site maintenance support will optimize readiness and reduce achievable footprint by applying appropriate models to big

data. Leveraging CBM+ and PHM can help, based on built-in test and troubleshooting capabilities, reduce test equipment, manpower and supply support needs. Moreover, targeted investments in reliability, availability, maintainability and supportability can improve system performance and readiness but also facilitate logistics footprint reductions to ultimately reduce life-cycle costs.

## Process-Focused O&S Should-Cost Opportunities

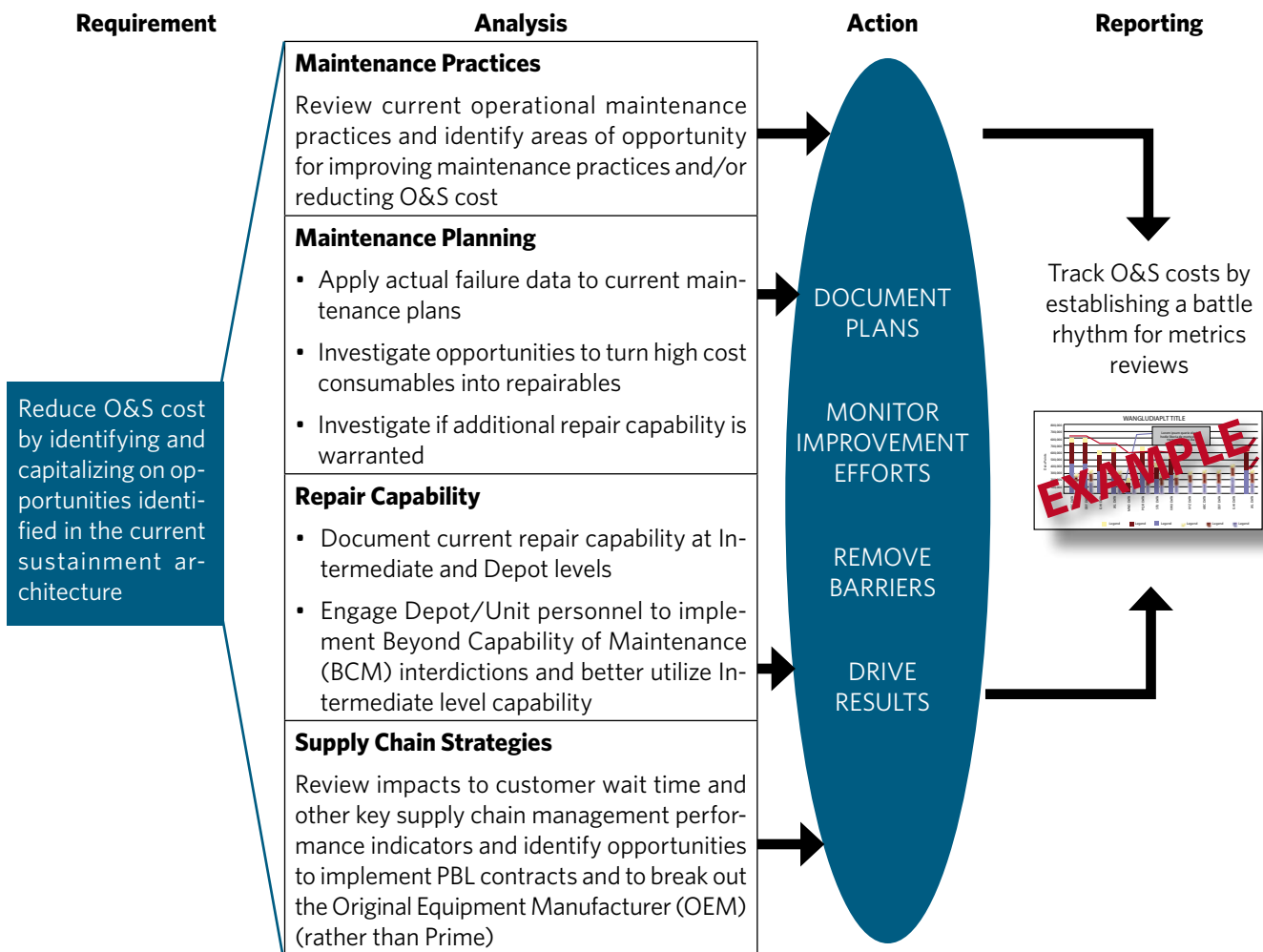
**Long-Term Performance Based Logistics (PBL) Product Support Strategies.** According to a Nov. 22, 2013, memo from the Assistant Secretary of Defense for Logistics and Materiel Readiness titled “PBL Comprehensive Guidance” and the 2016 DoD *PBL Guidebook*, “PBL is synonymous with performance-based life 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. ... PBL arrangements, on the other hand, are tied to Warfighter outcomes and integrate the various product support activities (e.g., supply support, sustaining engineering, maintenance, etc.) of the supply chain with appropriate incentives and metrics. In addition, PBL focuses on combining best practices of both Government and industry.” Sounds a lot like a golden O&S Should-Cost enabler, doesn’t it?

**Supply Chain Management (SCM) Efficiencies.** SCM often is procured as a service or deliverable. Knowing the supply chain from end-to-end enables the identification of Should-Cost opportunities. The most common way to look at the supply chain is in the context of the “three Vs,” which directly aligns with process-focused Should-Cost efforts.

- **Velocity.** How fast does material flow through the supply chain? Time can be money, so increase velocity through supply chain simplification—reduce nodes (use direct vendor delivery) and co-locate product providers. JIT inventory management and CPI methodologies for lean supply chains emphasize flow. For DoD, this can include transportation and maintenance improvements such as repair turnaround time reductions or “factory to foxhole” measures.
- **Visibility.** This is not just knowing what the supply chain looks like, but being able to pulse it at any point and any time to determine the supply chain’s health. Using technologies such as Radio Frequency Identification (RFID) and Item Unique Identification (IUID) can provide the data to reduce inventory levels and improve the supply chains’ efficiency and cost effectiveness. Use Manufacturing Resources Planning and Enterprise Resource Planning applications to better understand resource needs.
- **Variability.** How robust is the supply chain; can it absorb fluctuations in demand? Exploring options to buying access to inventory rather than holding large amounts of spares can result in significant savings. This is best done when the supply chain can be very responsive to demand changes.



**Figure 2. Identifying O&S Should-Cost Opportunities**



Source: DoD O&S Cost Management Guidebook, Figure 3—Example process for identifying Should-Cost initiatives that target O&S cost reduction.

**Inventory Management.** Any number of heuristics can be used to determine the right amount of inventory and reorder points. Simply asking to determine the amount of needed inventory and how much excess you have can be very revealing. Often, it can be found that excess inventory is carried for two reasons, “Just Because,” or “Just in Case.” While this may provide a certain amount of comfort, it is one of the most expensive forms of availability insurance. The cost of storage, security, climate control, obsolescence, and lost opportunity can be tremendous. This applies to parts, consumables, tools, support equipment and plant account. Are IUID, RFID and Serialized Item Management (SIM) being leveraged to reduce program and/or platform costs? IUD can contribute to improved total asset visibility, and RFID can give us true in-transit asset visibility when properly applied. Most SIMs provide tracking and status information. Is this being used to determine excess opportunities, directives issuance status, and ready-for-issue (RFI) versus non-RFI condition?

**PHS&T.** This has been the source of numerous potential cost savings initiatives. Examine support data to identify

items subject to damage during transportation, to determine if a minor cost for additional protective packaging can reduce component damage like the glass in the F-18 heads up display. Make sure items are properly stored to retain their useful life. For example, tire rubber should be stored upright, not stacked.

**Proactive DMSMS Strategies.** Proactive DMSMS management leads to early identification of DMSMS and related obsolescence issues, potentially increasing your ability to head off. The more lead time, the greater the likelihood of more lower-cost options to resolve DMSMS and obsolescence issues. Late recognition of an issue means an expensive redesign. Consider a technology refreshment strategy that replaces items before they become obsolete. (This is especially suitable for commercial off-the-shelf electronics and data processing equipment). Technology refreshment also avoids the need to pay for an out-of-cycle redesign. Although categorized under process-focused Should-Cost opportunities, DMSMS could arguably just as easily fall under product-focused area.

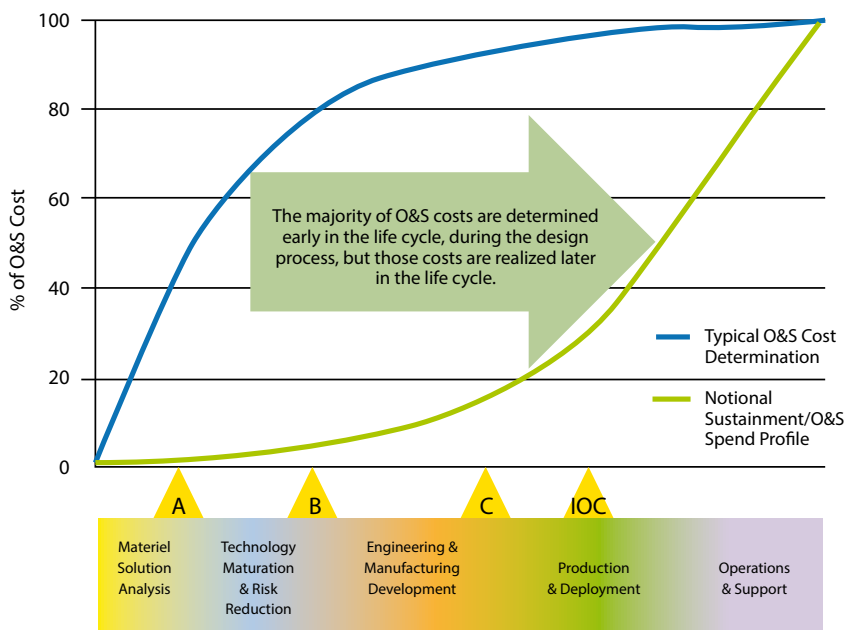
### Contract Type (and Associated Incentives).

It is important to know what you are incentivizing with the contract type used. Selecting the most appropriate contract type for the position in the life cycle and the associated risk can save a tremendous amount. If you have been buying logistics support as “time and material” and you have enough historical data to develop averages and identify trends, it may be advantageous to shift to a fixed-price construct. This is very much the case when shifting from a transactional construct to PBL product-support arrangements. Many articles have emphasized the benefits of paying for performance rather than for failures and the opportunities created for both customer and provider identification of ways to reduce resource consumption. Often a major modification gives rise to an impulse to go from a firm fixed-price contract for support to a cost-plus contract. Programs should instead consider stepping back to a fixed-price incentive firm target contract and leverage applicable historical data. For more insights into incentivizing performance, see the in-depth “Incentives—Motivating Achievement of Desired Product Support Outcomes” ACQuipedia article <https://shortcut.dau.mil/acq/psi-mado>.

**Proactive System Disposal, Demilitarization, and Material Disposition Planning.** As DoD Manual 4160.21, Volume 1, indicates, it is important to “treat the disposal of DoD property as an integral part of DoD Supply Chain Management; ensure that disposal actions and costs are a part of each stage of the supply chain management of items and that disposal of property is a planned event at all levels of (your) organization.” Expected outcomes include “... protecting national security interests, minimizing environmental mishaps, satisfying valid needs by extended use of property, permitting authorized donations, obtaining optimum monetary return to the U.S. Government, and minimizing abandonment or destruction of property.” All that affords tangible and viable O&S Should-Cost opportunities.

**Public-Private Partnering (PPP).** This partnering creates opportunities to leverage the best capabilities of organic and industry providers to realize synergy. Partners are able to take advantage of their strengths while mitigating weaknesses and gaps in their competencies. This can reduce overall cost, by assigning responsibilities to the organization that can most cost effectively provide that support. This cooperative arrangement also can result in joint efficiency improvements. The transparency can enable cost elements to be challenged. Specific benefits of PPPs can include: access to expertise (both sustaining engineering and maintenance), support decisions that are not made in a vacuum, more cost effective supply chains, and ac-

**Figure 3. Time Between O&S Decisions and Cost Results**



Source: DoD O&S Cost Management Guidebook, Figure 4—“Time delay between decisions affecting O&S cost and the realization of those costs.”

**Note:** A,B,C = acquisition milestones/decision points; IOC = initial operational capability.

cess to skilled artisans, technical expertise, best commercial practices, as well as state-of-the-art equipment and facilities.

**Integrated Product Life-Cycle Management (PLM) in an Integrated Data/Decision Environment (IDE).** PLM manages the entire life cycle of a product—from inception through disposal. An IDE or PLM system allows every program activity to create, store, access, manipulate and exchange digital data. It enables transparency and provides the opportunity to “see” potential cost-saving initiatives and facilitates better articulation of investment costs, unintended cost impacts, direct savings and related and/or second-order savings. Because boundaries are crossed, applicable stakeholders can see into the processes and products associated with the platform. And synergy is realized through integrated enterprise constructs, while the supply chain(s) are better managed. The IDE is more than just an IT system. It is key to Weapon System Configuration Management; providing traceability, thereby reducing costs associated with management of change proposals and upgrades. The IDE should also provide Product Data Management, ensuring there is system completeness, accuracy and validity to support initial and ongoing supportability analysis and associate all weapons system information with a configuration item, assembly, or end item. Finally, the IDE provides the foundation for trade decisions and optimal design solutions involving affordability and Should-Cost implications. An IDE allows the key players involved in the Should-Cost efforts to communicate and understand how their respective functional areas affect the trade studies and drive down will-cost estimates.

**Data Analytics.** Big data are out there. However, are the data being leveraged? DoD is a data-rich environment, but translating this into actionable information and enabling systems optimization is where “the rubber meets the road.” Data analytics and associated tools can be used to scrutinize the supply chain and evaluate supplier performance relative to timeliness, quantity, quality and pricing. This may create opportunities to reduce supply support and PHS&T and costs. Data analytics also can be used to optimize depot maintenance and planned maintenance scheduling—not just to reduce equipment down time but to realize efficiencies in resource allocations and reduce redundant and overlapping activities. Data analytics can point to areas where assignment of a depot technician to a lower-level maintenance organization may allow for numerous cost saving interdictions “beyond capability of maintenance.” All of these can translate into future Should-Cost wins.

**IT Refresh Rates.** Often, we look at historical refresh rates or standard refresh rates that broadly apply to software. This is the easiest and least time-consuming way to form a determination. A deeper analysis may find that a longer refresh cycle is appropriate in a particular operating environment, given the stability of the system to which it is applied or the nature of the software itself. The longer cycle could save on significant procurement and deployment expenses as well as potential integration issues. Software sustainment strategies are increasingly important in weapon system product support and, by extension, in product support Should-Cost opportunities.

**CPI.** Most organizations have a CPI methodology in place to guide projects and events. Whether the organization uses Lean, Six Sigma, Theory of Constraints, Total Quality Management or some combination thereof, consideration should be given to aligning Should-Cost efforts with it. Should Cost can be viewed as a particular subset of an overall CPI construct in

that it is an improvement effort aimed at initiatives that specifically result in cost savings (as opposed to making quality improvements or reducing cycle time).

Say what you will about logisticians and product support managers—if you want to truly tackle your program’s LCCs and deliver some tangible, high-impact Should-Cost wins, you inevitably must address O&S costs through innovative product support initiatives. You very quickly will realize that those wins must come either in product or process. Product initiatives very often revolve around designing, developing and fielding reliable, maintainable, supportable, transportable and energy-efficient systems. Process initiatives very often involve efficient and effective supply chains, rapid identification, turnaround and return to service of failed items, maintenance process efficiencies, reduced manpower requirements, and the like.

As the *DoD Product Support Manager’s Guidebook* pointedly reminds us, “PMs (and by extension, PSMs and Life Cycle Logisticians) pursue two primary support objectives. First, the weapon system must be designed to deliver the required warfighting capability and be affordable. Second, the product support solution must be efficient and effective, and it must reduce the demand for product support while meeting Warfighter requirements. When developing and implementing a product support strategy, the goal is to balance and integrate the support activities necessary to meet these two objectives.”

We would contend that delivering tangible, measurable O&S Should-Cost wins is, quite simply, one of the best ways to demonstrate successful achievement of these outcomes. &

The authors can be contacted at [martin.sherman@dau.mil](mailto:martin.sherman@dau.mil) and [bill.kobren@dau.mil](mailto:bill.kobren@dau.mil).

Expand Your Network

- Available 24/7
- More than 40 different acquisition-related Communities of Practice and Special Interest Areas
- Access to policies, guidance, tools, and references
- Automatic notification of new content (by subscription only)
- Ability to tap into the wisdom of the community
- Interact, share resources, ideas, and experiences with fellow practitioners across DoD and industry

**Acquisition Community Connection (ACC)**  
Where the Defense Acquisition Workforce Meets to Share Knowledge  
<https://acc.dau.mil>





# HOW TO WRITE a Good Risk Statement

James Thompson ■ Stephen Stump

**T**he recently released *Department of Defense Risk, Issue, and Opportunity Management (DoD RIO) Guide for Defense Acquisition Programs* discusses the importance of communicating risks through the use of structured risk statements. It describes how well-structured risk statements help all stakeholders better understand the program risks and enhance system engineering planning and communications. This article expands on that discussion and shares some of our more frequent recommendations for programs to improve risk statements.

---

**Thompson** is the director of Major Program Support in the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD[SE]). He is the lead for independent technical risk assessments, providing support to major defense acquisition programs, and informing relevant technical authorities and communities regarding best practices for systems engineering. **Stump** is the Land Expeditionary Warfare Program Support Team lead in the ODASD(SE).



A risk statement summarizes a potential problem that needs to be addressed. The statement communicates the potential adverse event or condition and its consequences on program objectives should the risk be realized. The statement informs other members of the extended program team, program leadership and stakeholders to make them aware and possibly help them make decisions in consideration of the risk.

A clear risk statement ensures that people across organizational boundaries or geographically distributed groups, such as in a system of systems, possess a common understanding of the problem. Poorly written risk statements do not achieve these goals and can be counterproductive. This article further discusses the elements of a good risk statement, various acceptable

formats, and examples of weak risk statements, showing how they can be improved.

### **Elements of a Good Risk Statement**

The recently published *DoD RIO Guide* indicates a good risk statement will include two or, potentially, three elements: the potential event or condition, the consequences and, if known, the cause of the event.

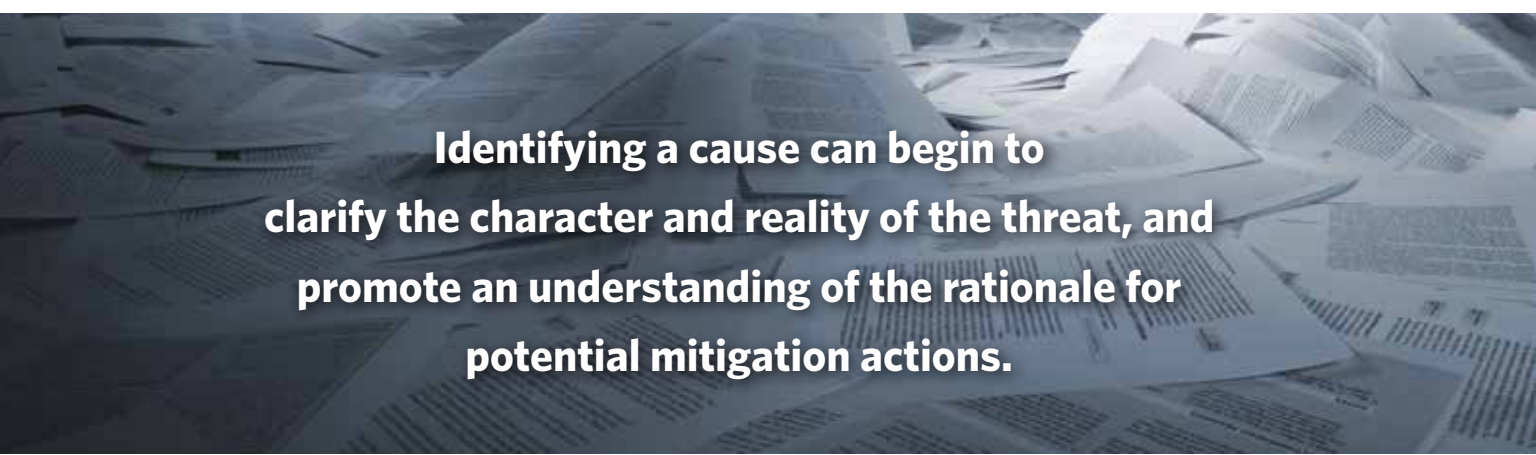
The potential event is a future possible happening that could have an impact on the program objectives. In short, the uncertain event describes something that can go wrong. It might be associated with design or development, technology failure, supplier problem, or any other item that might cause an undesirable condition that will impact program objectives.

If either the root cause or the proximate cause is known, it is helpful to describe it in the risk statement. Including the cause helps clarify what is driving the risk and later will help the program develop a mitigation plan. The mitigation aimed at reducing likelihood may address the proximate cause rather than the root cause. For example, the batteries Program X uses are not reliable and keep failing, so the program manager (PM) elects to switch to a different supplier. In this case, the proximate cause is that batteries keep failing reliability and the solution is to replace them with different batteries. Theoretically, the root cause might have been a bad production process, sloppy quality control, bad specifications, or bad design, etc., or a combination of these causes. These are important factors to investigate if you are the battery manufacturer or a battery PM, but the Program X PM does not address them because the solution to “proximate” cause (bad battery) is to buy from a different source.

increase or the aircraft maneuvering envelope will be reduced (consequence).

This example provides no reason for the concern that wing properties may not be achieved, which leaves open whether this is simply one passing concern among many possibilities or a causal factor posing an actual threat to objectives prompted by observation or known circumstances. Identifying a cause can begin to clarify the character and reality of the threat, and promote an understanding of the rationale for potential mitigation actions. The modified risk statement below provides a proximate cause for the risk. In addition, the modified statement more fully characterizes the impact to the design:

If the program cannot achieve the anticipated structural properties of the wing skin material (uncertain condition) due to the difficulty of controlling processing variables



## Identifying a cause can begin to clarify the character and reality of the threat, and promote an understanding of the rationale for potential mitigation actions.

Finally, the consequences are the impact the event or condition will have on a program, usually expressed in terms of cost, schedule, or performance. This part of the statement describes the outcome for the program if the risk event or condition is realized.

### Risk Statement Format

There are several generally accepted ways to write a risk statement. While the *DoD RIO Guide* highlights the “if-then” construct, there are other equally acceptable methods of defining the key elements of potential event or condition, consequences, and cause (if known). The guide suggests a program adopt one approach and instill a disciplined practice of using that approach. Here are a few approaches to consider:

■ **The “if-then” format** presents the possible risk event or condition (“if”) and the potential outcome or consequence(s) (“then”). If some event or condition occurs, then a specific negative impact or consequence to program objectives will result.

*Example:* If the program cannot achieve the anticipated wing skin structural properties (condition), then wing weight will

(cause), then the wing design will be 400 pounds heavier or the aircraft maneuvering envelope will be reduced (from 7.0 g [gravitation force] to 6.0 g) (consequences).

■ **Another approach is the “condition-consequence” format.** In this format, the “consequence” is the possible outcome of the existing “condition,” which has the following structure: A condition causing concern or uncertainty exists; therefore, a negative impact or consequence to a program objective may result.

*Example:* To date, the program is achieving lower-than-expected structural properties (condition) due to processing anomalies with the selected wing skin material (cause); therefore, a heavier wing design or a reduced high-g maneuver capability (7.0 g to 6.0 g) may result (consequences).

■ **A third approach adds a “because” to the statement construct, producing a “because-event-consequence” format.** This leads to statements with the following structure: “Because” of a fact or existing condition, “an event” may occur, resulting in a negative impact or “consequence” to a program objective.



*Example:* Because the program is experiencing processing difficulties with the wing skin material (cause), the anticipated structural properties may not be achieved (event or condition), resulting in a heavier wing design or a reduced high-g maneuver capability (7.0 g to 6.0 g) (consequences).

Whatever statement structures the program uses, the key objective is to clearly identify the event or condition, consequences, and cause (if known) without being overly complex. A risk statement should be specific and detailed enough to contribute to effective communication.

A clear risk statement can help clarify the “risk” as the actual threat to achieving project objectives. This avoids focusing on non-risks arising from confusion with causes, impacts, or even mitigation actions. Failure to distinguish between these elements will inevitably drive nonproductive efforts. Consistently using a structured language format can help reduce this confusion.

### Weak Risk Statements

Poorly written risk statements do not promote understanding or support productive action. Weak statements may be overly general, circular or self-evident. They may confuse risk with cause or consequences, or they may not describe consequences accurately. For example, a program may identify a risk as “inadequate staffing” when in fact the inadequate staffing should be considered a cause that may pose a variety of risks or consequences such as reduced quality, delays, or even workforce turnover.


The following are examples of poorly formed risk statements with a rationale for why they are inadequate.

- Makes an overly general observation:
  - **Weak:** *Supplier quality problems may cause program delays.* This statement lends no actionable insight into underlying or existing causal conditions and provides only vague impact on program objectives. In contrast, the statement below is more informative.
  - **Stronger:** Because wiring insulation from Supplier A does not meet specifications, it may be necessary to replace wiring in prototype units, resulting in a 30-day delay to start of testing and a day-to-day slip in completing the phase.  
This statement identifies the cause as the anomalous material delivered by a specific supplier, the nature of the uncertain event, and the contingent impact to program schedule. This more complete articulation of the problem points to additional analyses on potential mitigation steps and alternatives.
- Identifies an issue rather than a risk:
  - **Weak:** *Fatigue cracks discovered in already delivered vehicles may shorten service life unless remedied.*  
This statement describes an issue, not a risk. There is no uncertainty about the likelihood of occurrence. The

statement depicts an event that already has occurred, causing a problem with consequences that must be evaluated and addressed.

- Diverts focus from the program’s controllable activities:
  - **Weak:** *If the program’s funding is withheld due to poor test results, then the program schedule will be jeopardized.*  
In this case, the potential for curtailed funding is a consequence of the program’s poor test results, which should be the focus of attention but is not directly or centrally addressed in the risk statement.
  - **Stronger:** If the vehicle reliability test performance continues to be below XX mean time between failures during test, then the resulting schedule delay to fix failures could cause a 6-month extension of the overall program schedule and increase cost.
- Separates an actual risk from inadequate execution or poor quality effort:
  - **Weak:** *If the design analysis does not account for the range of expected environmental conditions, then the design may not function in the field.*  
This is not an actual risk because it is known that a design that neglects to account for operating environments will have negative consequences for system performance. In effect, this is saying, “If we don’t use sound engineering practices, our product will suffer.” Such inadequate analysis is an issue that should be preemptively avoided or corrected.
- Announces an unavoidable programmatic event and consequence as a risk:
  - **Weak:** *If a 5 percent budget reduction is imposed on our program due to announced departmental budget constraints, we will have to renegotiate the contract.*  
This statement is weak because no mitigation action can be provided for this predicted fact-of-life event, and when it occurs, it will be an issue, not a risk. It is a discrete event outside of the program office’s control.

### Summary

An important element of risk management is a clear articulation of the risks. The key requirement for a good risk statement is that it clearly identifies the event or condition, the consequences on program objectives, and cause (if known). Disciplined use of structured formats can help in describing a risk, produce more effective risk statements, and avoid weak statements that lead to confusion. Risks should be monitored and statements updated (a living document/plan) as the program progresses and gains knowledge. The *DoD RIO Guide* (<https://www.acq.osd.mil/se/pg/guidance.html>) provides additional information on risk and the nature of potential risk drivers as the program moves across life-cycle phases. 

The authors may be contacted through [james.j.thompson3.civ@mail.mil](mailto:james.j.thompson3.civ@mail.mil) and [stephen.a.stump.civ@mail.mil](mailto:stephen.a.stump.civ@mail.mil).

# AcqDemo Aids Acquisition Mission Success

Scott Wortman

It has been proven time and again that the Department of Defense (DoD) Acquisition Workforce Personnel Demonstration (AcqDemo) project enhances civilian personnel management policies and procedures to meet the needs of the acquisition workforce more effectively, ultimately yielding improved acquisition outcomes.

AcqDemo provides an inherently flexible human resource pay and personnel management system that recognizes and rewards employees based upon their contributions to mission accomplishment, and supports their personal and professional development, all while improving retention across the participating organizations. The Human Capital Initiatives (HCI) Directorate, under the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]), manages the AcqDemo program across DoD. Seeking to improve efficiencies and flexibilities, HCI has recently collaborated with stakeholders to streamline processes and make significant improvements to AcqDemo.

These improvements, planned for introduction in the fall 2017, will simplify the contribution assessment process and enhance quality and professionalism of the Acquisition Workforce in the participating organizations. The added flexibilities in hiring, compensation, recognition, educational qualification screening, and the availability of sabbaticals will increase the quality of the workforce environment and make DoD more competitive with the private sector as an employer of talented acquisition professionals. The AcqDemo improvements and flexibilities will empower organizations

**Wortman** is AcqDemo program manager for the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics' Human Capital Initiatives at Fort Belvoir, Virginia.



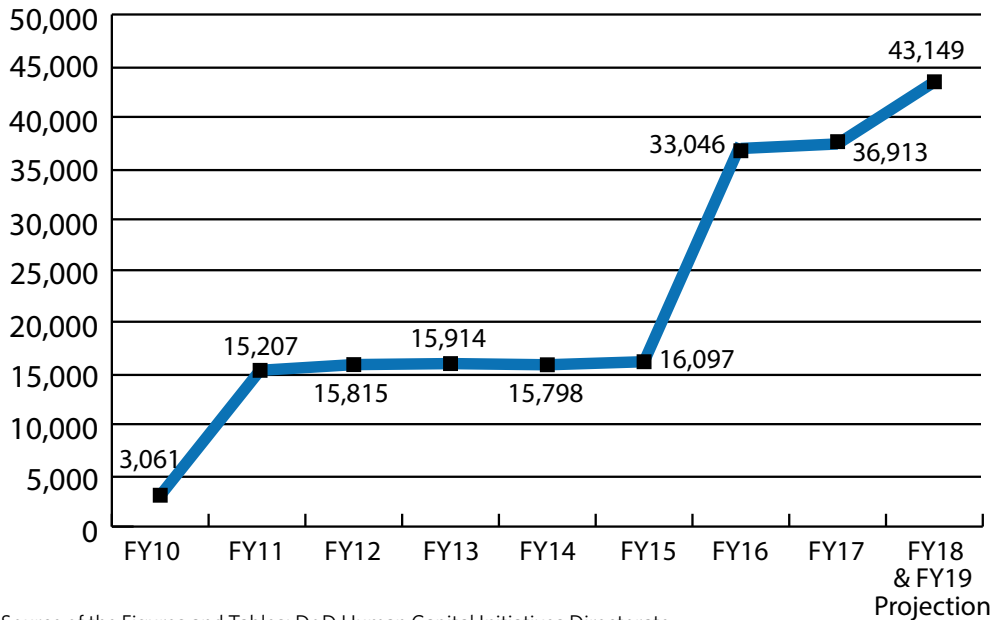
and managers to exercise more effective management of the acquisition workforce. The updated AcqDemo will benefit the participating DoD Acquisition Organizations, Acquisition Managers and the Acquisition Workforce. This is a classic case of a “good thing that just got better.”

**AcqDemo Background**

In 1996, Congress authorized the DoD to conduct a personnel demonstration project for the civilian acquisition workforce, aptly named AcqDemo. The initial intent of AcqDemo was to enhance the effectiveness of personnel programs and processes across the DoD Acquisition community. This was accomplished by using a Contribution-Based Compensation and Appraisal System (CCAS) that tied employee’s compensation directly to their contributions. CCAS also empowered managers at the lowest level with increased flexibilities in recruitment, staffing, classification, performance management and employee development. The introduction of AcqDemo provided a dramatically different way of recognizing employee contributions vice the very inflexible General Schedule (GS) system that based salary increases on performance and longevity. In the GS system, civilian personnel are neither rewarded nor recognized for their contributions to the organization’s mission.

Currently, AcqDemo has more than 37,000 participants and is forecast to number more than 43,000 by Fiscal Year (FY) 2019. Expansion has been continuous across DoD, and the number of participants doubled in FY 2016. Figure 1 shows the increase of the number of participants by fiscal year.

**Figure 1. AcqDemo Growth and Expansion in Numbers of Participants**



Source of the Figures and Tables: DoD Human Capital Initiatives Directorate.

**AcqDemo Structure and Flexibility**

There are two features of AcqDemo that make the project unique and advantageous for both employees and supervisors:

- Broadband pay ranges are utilized to classify employees.
- Employee appraisal system, which ties compensation to contribution to the organizational mission.

The broadband pay ranges provide significant flexibility for management to reassign employees to new positions within the AcqDemo project. When employees enter AcqDemo, they are assigned to one of three broad career paths based on their occupation: business management and technical management professional (NH), technical management support (NJ), or administrative support (NK). As shown in Table 1, the NH and NJ career paths each have four pay bands, and the NK career path has three pay bands. Each pay band corresponds to two or more GS grades, which is why the pay bands are referred to as broadbands. When employees enter AcqDemo, their supervisors have compensation-setting flexibility—they can establish the new employee’s initial pay at any point within the broadband. Broadbands afford the greatest personnel management flexibility by granting supervisors the authority to reassign within the same broadband without changes in pay or job description.

Pay is linked to contribution through a process that evaluates the relative contribution to mission for each employee on a numerical scale that equates to pay. Pay Pools perform this evaluation, which is informed by employee self-assessments and direct supervisor appraisals.

**Table 1. Broadband Ranges**

BUSINESS AND TECHNICAL MANAGEMENT PROFESSIONAL (NH)			
I (GS 1-4)	II (GS 5-11)	III (GS 12-13)	IV (GS 14-15)
TECHNICAL MANAGEMENT SUPPORT (NJ)			
I (GS 1-4)	II (GS 5-8)	III (GS 9-11)	IV (GS 12-13)
ADMINISTRATIVE SUPPORT (NK)			
I (GS 1-4)	II (GS 5-7)	III (GS 8-10)	



## Coming AcqDemo Improvements

The original AcqDemo Project Plan included streamlined hiring and appointment authorities; a Voluntary Emeritus Program; broadbands; simplified classification and appraisal criteria (six factors); revised reduction-in-force procedures; CCAS; academic degree and certification training; and sabbaticals. The soon-to-be-published *Federal Register* notice features major improvements such as streamlined contribution factors (six to three); simplified accelerated hiring; CCAS updates; modified appointment authorities; simplified classification process; enhanced academic degree and certification training; expanded candidate selection processes; modified Reduction in Force (RIF) process; student relocation incentives; and the Voluntary Emeritus Program. Most of the changes being introduced are flexibilities available to an organization that the organization must elect to utilize before incorporating them into the organization's process. Please consult your organization to see which flexibilities are available for your use.

## Performance Appraisal Enhancements

Upon publication of the *Federal Register* notice, the HCI Acq-Demo Program Office will roll out the major enhancements in the FY 2018 performance cycle. The greatest enhancement is the reduction of the number of "contribution factors" in the CCAS—six to three (as shown in Figure 2). The reduction of factors is a highly anticipated change driven by feedback from the AcqDemo user community. The streamlining of factors helps employees and supervisors by eliminating factor redundancies and overlaps without forfeiting the key contribution factors. Figure 2 maps the contribution factors from the old to the new system.

A performance assessment has also been added to the new AcqDemo design. Although performance has always been a part of Acq-Demo, the design has been contribution focused. To appropriately capture performance, AcqDemo will incorporate a separate performance assessment, which uses the same criteria for evaluating contribu-

**Figure 2. Six Classification Factors Into Three New Factors**



tion, and enables employees to see the bigger picture during the appraisal period. The three levels of the performance criteria will be averaged and compared to the Performance Appraisal Quality Levels (as shown in Table 2), which will determine the rating of record (e.g., outstanding, full successful or unacceptable).

## Recruitment and Staffing Enhancements

Direct hire authority gives managers and human resource professionals the option of making an on-the-spot tentative offer to candidates at recruiting events. If the candidate has the degree required by the Office of Personnel Management (OPM) and/or DoD standards covering acquisition or acquisition support positions, then he or she is eligible to receive a job offer. This includes the authority to appoint student interns and veteran candidates for acquisition positions in the critical acquisition career fields of business and technical management or technical management support, thereby increasing managers' ability to identify and hire the best candidate.

**Table 2. Performance Appraisal Quality Levels**

Performance Appraisal Level	Performance Appraisal Level Quality Criteria
Level 5—Outstanding	An employee's quality of performance exhibited in achieving his/her contribution results substantially and consistently surpasses the factor-specific expected contribution criteria and the employee's contribution plan goals and objectives.
Level 3—Fully Successful	An employee's performance consistently achieves, and sometimes exceeds, the factor-specific expected contribution criteria and his/her contribution plan goals and objectives.
Level 1—Unacceptable	An employee's performance fails to meet the expectations for quality of work and the required results for the goals and objectives set forth in his/her contribution plan for the appraisal cycle.

Additional hiring flexibilities include:

- Scholastic achievement appointment—available to a wider range of candidates.
- Rule of Many—when there are 25 or fewer candidates for a position, the hiring manager, who knows the subject matter better than Human Resources personnel, will have the option of reviewing all the candidates to find the skills needed.
- Voluntary Emeritus Program—opens opportunities to military and civilian retirees who supported the Acquisition Workforce but were not in positions designated under the Defense Acquisition Workforce Improvement Act (DAWIA).

Also expanded supervisory and managerial probationary periods will afford adequate probationary periods so that current managers with significant responsibility for major programs can assess candidates for full-time position assignments. If

- Salary inequities exist between supervisory and non-supervisory employees' basic pay.
- It is difficult to fill team lead positions.
- Organizational level, scope and value of position warrant additional compensation.

The Very High Score provision allows for current scores in the NH, NJ, NK career paths to be raised above the current maximum of 100 (NH), 83 (NJ), and 61 (NK) to 115, 95, and 70, respectively; increasing managers' flexibility in rewarding employees whose contributions are at the very top of the pay band.

Accelerated Compensation for Developmental Positions permits employees to receive evaluations twice a year, at the mid-year point and at the end of the appraisal cycle with the target of accelerating compensation when the employee contribution and performance exceed expectations.

## **Accelerated Compensation for Developmental Positions permits employees to receive evaluations twice a year, at the midyear point and at the end of the appraisal cycle ...**



the probationary supervisor doesn't work out in the position of increased responsibility, the organization can move him or her back to the previous supervisory or nonsupervisory position.

Reductions in force will now be based on performance rather than a longevity-based system.

Expanded detail and temporary promotion authority enables managers to fill open positions at a higher level of responsibility with existing employees beyond the current 120-day limit, for as much as 1 year within a 24-month period. For example, if an employee's supervisor is on extended leave, that employee in a lower broadband level may be temporarily promoted to a higher level of responsibility, with a higher salary, for 6 months. At the end of that period, if circumstances require, that employee could be temporarily promoted for another 6 months within the 24-month period.

### **Additional New Features**

Supervisory and team-lead cash differentials provide local commanders with an additional tool to incentivize and compensate supervisors and team leaders as defined by the OPM General Schedule Supervisory Guide or Leader Grade Evaluation Guide. Organizations can offer 5 to 10 percent over a person's base salary. Supervisory and team-lead cash differentials are applied under the following circumstances:

Special act awards of \$25,000 allows Service Acquisition Executives to award employees up to \$25,000; a significant increase over the current \$10,000 limit.

Another exciting update is the student intern relocation incentive, which will give local commanders or their designees the ability to approve relocation for new student interns whose worksite is in a different geographic location from the college/university in which they are enrolled or their permanent home residence. This incentive targets top talent for student internships and increases the opportunity for a follow-on hiring after graduation.

The sabbatical provision is open to all eligible employees with 7 years of federal civilian service completed. This provision expands the existing sabbatical provision, requiring a post-sabbatical service requirement 3 times the length of the employee sabbatical.

With all the changes taking place, we want organizations under AcqDemo to be able to incorporate the newly implemented enhancements, policy changes and software into their personnel procedures and practices as required to support their mission requirements. Communications and training on the new improvements have already begun and

we soon will provide additional information to your AcqDemo representative.

### Join AcqDemo

We at HCI would like to invite all eligible acquisition organizations that have not yet opted to join AcqDemo to check out the improved AcqDemo and to see if it will be a good fit for your organization and your acquisition professionals. To participate, your organization must be listed in Table 1 of Appendix B of the AcqDemo *Federal Register* notice. If your organization is listed, the workforce must meet the following criteria: "at least one-third of the workforce participating in the demonstration project consist of members of the acquisition workforce; and at least two-thirds of the workforce participating in the demonstration project consist of members of the acquisition workforce and supporting personnel assigned to work directly with the acquisition workforce." (National Defense Authorization Act of 2004). For organizations that would like their bargaining unions to join the program, a written agreement between the organization and the union representing the workforce prior to joining AcqDemo is required to cover participation in and implementation of the demonstration project.

We are very pleased to help you determine the eligibility of your organization and if your agency is interested, we encourage you to contact the DoD AcqDemo Program Office via e-mail [AcqDemo.Contact@hci.mil](mailto:AcqDemo.Contact@hci.mil) or your AcqDemo component representative.

AcqDemo is a proven and innovative solution. Recent growth that has more than doubled the number of employees par-

ticipating in AcqDemo indicates that more acquisition organizations are realizing that they need AcqDemo to be competitive with the private sector, other demonstration projects, and other federal agencies in attracting and retaining a high-quality workforce. AcqDemo's appointment and performance appraisal-related flexibilities are intended to help organizations achieve their mission by ensuring that they have a highly qualified and motivated workforce and by making them more agile and adept in responding to evolving mission needs or changes in the environment.

### About HCI

René Thomas-Rizzo, a member of the Senior Executive Service, leads the HCI organization. She is the principal adviser to and senior leader on behalf of, the USD(AT&L) on all DoD-wide acquisition workforce strategy, policy and initiatives for the 160,000-plus member Acquisition Workforce (AWF).

HCI is responsible for assisting the USD(AT&L) in carrying out statutory powers, functions, and duties of the Secretary of Defense with respect to the Defense AWF and as it relates to DAWIA. In the increasingly fast-paced world of changing threats and evolving technologies, the DoD AWF supports the DoD objective to ensure our warfighters are ready to fight today and in the future. To accomplish this mission, the Office of the USD(AT&L) has put into place AcqDemo as an opportunity to provide a civilian personnel management system that meets the needs of the Acquisition, Technology, and Logistics community. &

The author can be contacted at [scott.wortman@hci.mil](mailto:scott.wortman@hci.mil).

## 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!







# Streamlining the Contract Award Process

Gregory B. Gonzalez

A longstanding challenge and source of interminable frustration for Department of Defense (DoD) program managers (PMs) is the often excessive timeline associated with conducting a source selection and awarding a contract.

PMs either can reluctantly accept the lengthy timeline or use innovation and resources available to them to streamline that process. The sooner a contract is awarded, the quicker a PM can get to the work of product development, testing and deployment to the warfighter.

The program management office (PMO) for the Army Contract Writing System (ACWS), in concert with the Army Contracting Command—Rock Island (ACC-RI) in Illinois, implemented several innovative methods to significantly reduce the timeline required to award the initial ACWS contract. The ideas for efficiency and innovations outlined below can be used by other PMs to streamline their own contract award processes with similar effect.

In the following question-and-answer (Q&A) interview, LTC Rob Wolfe, product manager for the ACWS program, explains some of the most impactful efficiencies that he and his team implemented to facilitate a source-selection decision and contract award in just 11 months after release of the request for proposals (RFP). Contracting activity baseline goals for that process often take more than twice as much time.

---

**Gonzalez** is the senior acquisition consultant to the product manager of the U.S. Army's Contract Writing System in the Program Executive Office of the Army Enterprise Information Systems in Alexandria, Virginia. He is a retired Army colonel with more than 25 years of Department of Defense acquisition experience.



**Q: Does the Army Contracting Enterprise recognize that the contract award process needs to be reduced—and if so, what are they doing about it?**

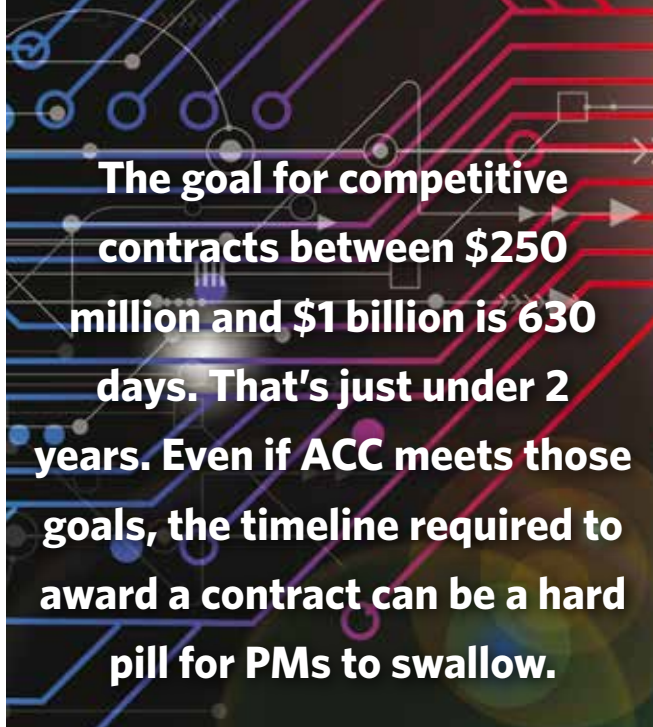
**A:** Sure. I believe they do. The Army Contracting Enterprise has long recognized the need to reduce what they refer to as Procurement Action Lead Time (PALT). PALT is the timeline required to achieve all work in which a contracting activity is engaged to award a contract. This work includes acceptance of a complete and actionable requirements package, release of a RFP, and conduct of a source selection culminating in the award of a contract. As an example, the commanding general of the Army Contracting Command (ACC) distributed a memorandum on Jan. 18, 2017, to the ACC workforce. The memo established a PALT baseline, by dollar threshold and acquisition type, and encouraged the workforce to achieve these baselines unless unusual circumstances are involved. This is great news, but for PMs, even the timeline goals for the PALT baselines can seem excessive to PMs. For example, the PALT baseline for a competitive contract estimated at between \$50 million and \$250 million is 600 days. The goal for competitive contracts between \$250 million and \$1 billion is 630 days. That's just under 2 years. Even if ACC meets those goals, the timeline required to award a contract can be a hard pill for PMs to swallow.

**Q: How did the ACWS program reduce the PALT timeline as it worked toward awarding a contract?**

**A:** Well, before we released the development RFP in April 2016, our team began looking for ways to improve the efficiency of the PALT process. Their initial efforts focused on listing all PALT activities in an Integrated Master Schedule (IMS) so their start times and durations could be identified and analyzed. They soon realized that many of the events that were originally planned to be conducted in a serial manner could be sequenced so that one event could start shortly after the other, with both then conducted in parallel. There are three great examples of this.

The initial plan called for using one team that would evaluate written proposals and then evaluate the live software demonstrations in sequential order. The staff decided it would be more efficient to form a separate live demonstration evaluation team and to conduct the live demonstrations in parallel with proposal evaluations. The live demonstration evaluation team had to be created from functional personnel, because the PMO didn't have sufficient staff, but use of this second team saved roughly 2 months of schedule.

The second efficiency initiative streamlined the evaluation report review cycles. During the Source Selection Evaluation Board (SSEB), there were two occasions when the SSEB chair, the Contracting Officer (KO) from ACC-RI, and attorney from Army Materiel Command were required to review evaluation reports. Normally these types of reports are done in sequential order (SSEB chair, legal, then KO,) and often from separate



locations. The ACWS team decided that it would be much more efficient to bring together all three personnel in one room for a weeklong review session. We made a compelling case to leadership to permit the KO and attorney to travel from their home stations and dedicate an entire week to one program. The results were extremely productive. The days (and nights) were long, but each set of reviews was completed in less than a week. If done serially from separate locations, this same process could have taken several weeks.

The final example involved the Source Selection Advisory Council (SSAC) and Source Selection Authority (SSA) updates. Typically, the source-selection process requires the SSEB Chair to update the SSAC and SSA at specific points along the source-selection path. These updates normally are conducted first for the SSAC, then a second is conducted for the SSA. Since these meetings require significant preparation, coordination and often travel, the program saved substantial time and resources by executing them jointly. With agreement of the SSA, the ACWS program conducted all SSAC and SSA updates together in one forum, saving potentially weeks of schedule. This joint update process continued well into the source selection until the SSAC conducted its comparative analysis work, which was conducted without the SSA present.

There are other efficiencies, but those discussed above were the most impactful.

**Q: What was the single most valuable time-saving initiative the ACWS team implemented during the PALT process?**

**A:** Without a doubt, the best decision we made was to co-locate our KO with the SSEB chair and the SSEB team. I will acknowledge that doing this is something that all programs

may not be able to do, but if they are able to make it happen, it will make a world of difference. The KO's duty station was at ACC-RI and the source selection evaluation took place at Fort Belvoir, Virginia. The KO agreed to an extended temporary duty assignment (TDY) in the National Capital Region (NCR). The TDY period began just days before the offerors' proposals were submitted to the government and lasted until the conclusion of discussions 180 days later. Because the KO worked in the same space with the SSEB team, he was able to follow and discuss key issues and provide immediate feedback. He became a trusted member of the team. The KO's daily presence on site saved months of long-distance coordination, e-mail exchanges, and phone conversations during which clarity and efficiency would have been the first victims. At the conclusion of discussions and while the offerors prepared their final proposals, the KO went back to his duty station at Rock Island. He returned to the NCR with the attorney, in a TDY status, to conduct the final evaluation report legal and reviews.

If PMs are not able to make any other changes to the PALT process, I recommend co-locating with the KO as that one thing.

**Q: Conducting formal discussions with offerors during a source selection can be very time consuming. Was the ACWS team able to implement any efficiencies in that process?**

**A:** Yes, we were. We learned very early in the source-selection process that communicating with offerors was a necessary but tedious and lengthy endeavor that often led to misunderstanding. Our first eye-opening experience took place shortly after the offerors submitted their initial proposals to the government.
























































































The KO needed to clarify a point in the proposals regarding past performance so he sent one e-mail to the applicable offerors. That single e-mail resulted in 50 e-mail exchanges between the KO and the offerors. If a similar ratio were experienced for each comment or question that had to be discussed with the offerors, the process could result in thousands of e-mail exchanges. We just knew that we could never support a process that was so inefficient and that could generate a seemingly endless trove of e-mails and questions. We had to find a more efficient way to communicate with the offerors.

We implemented a better solution during formal discussions with the offerors. Formal discussions typically are very time consuming because they involve an inefficient process wherein industry prepares questions and then, metaphorically speaking, throws them over the fence to the KO for an answer. The government team then prepares responses and throws them back to industry. This same process can be repeated hundreds of times, often without providing a sufficient or clear outcome.

Our solution was to conduct two separate, one-on-one discussions with each offeror team. The purpose of the first one-on-one discussion was to ensure each offeror's understanding of the Evaluation Notices (ENs) generated from evaluation of the initial proposals. Each offeror team met with the KO, the SSEB chair, and the technical factor and subfactor leads. Offerors asked questions and the team provided direct and clear responses. The KO directed the entire process. The purpose of the second meeting was for the offerors to respond to the ENs and to ensure that the government understood those responses.

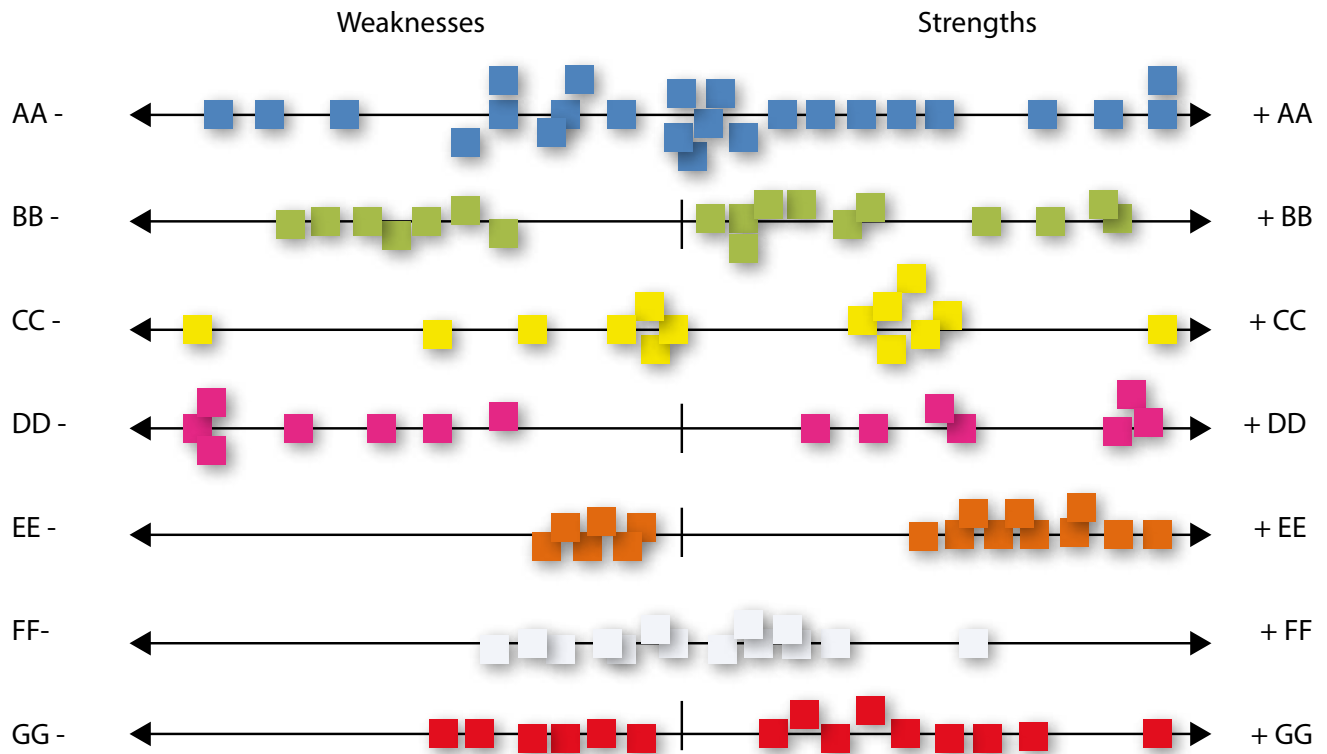
Each meeting took between 2 to 5 hours, depending on the number of questions. This same process when executed in the

Figure 1. Example of Board 1

	AA		BB		CC		DD		EE		FF		GG	
	S	W	S	W	S	W	S	W	S	W	S	W	S	W
Price														
Technical Capability														
														
														
														
Management Capability														
Past Performance														
Small Business														

Source of Figures: ACWS Product Management Office.

**Figure 2. Example of Board 2**



typical fashion could last months with less favorable results. Several of the offerors said they had never experienced a more positive exchange because it provided the clarity they needed to better prepare their final proposals.

Because he felt the offerors were well prepared to make necessary changes to their original proposals, the SSEB chair felt comfortable requiring all offerors to submit final proposals within 30 days after discussions were ended. For the ACWS team, it was a period of intense activity but well worth the effort for the results and schedule savings it enabled.

**Q: What, if anything, did you do to make the proposal evaluation process more efficient?**

**A:** I knew that to be able to meet the aggressive schedule goal we set for ourselves to complete the source-selection process and award the contract within 11 months we had to establish a reasonable limit for the time the SSEB team could evaluate each proposal. That goal was set at 2 weeks. The first week was spent reading the proposal thoroughly, taking notes and formulating responses. The second week was used to caucus and draft the initial reports. The only way the SSEB team could meet this tight timeline was for the members to prepare themselves in advance. We spent several weeks on that preparation.

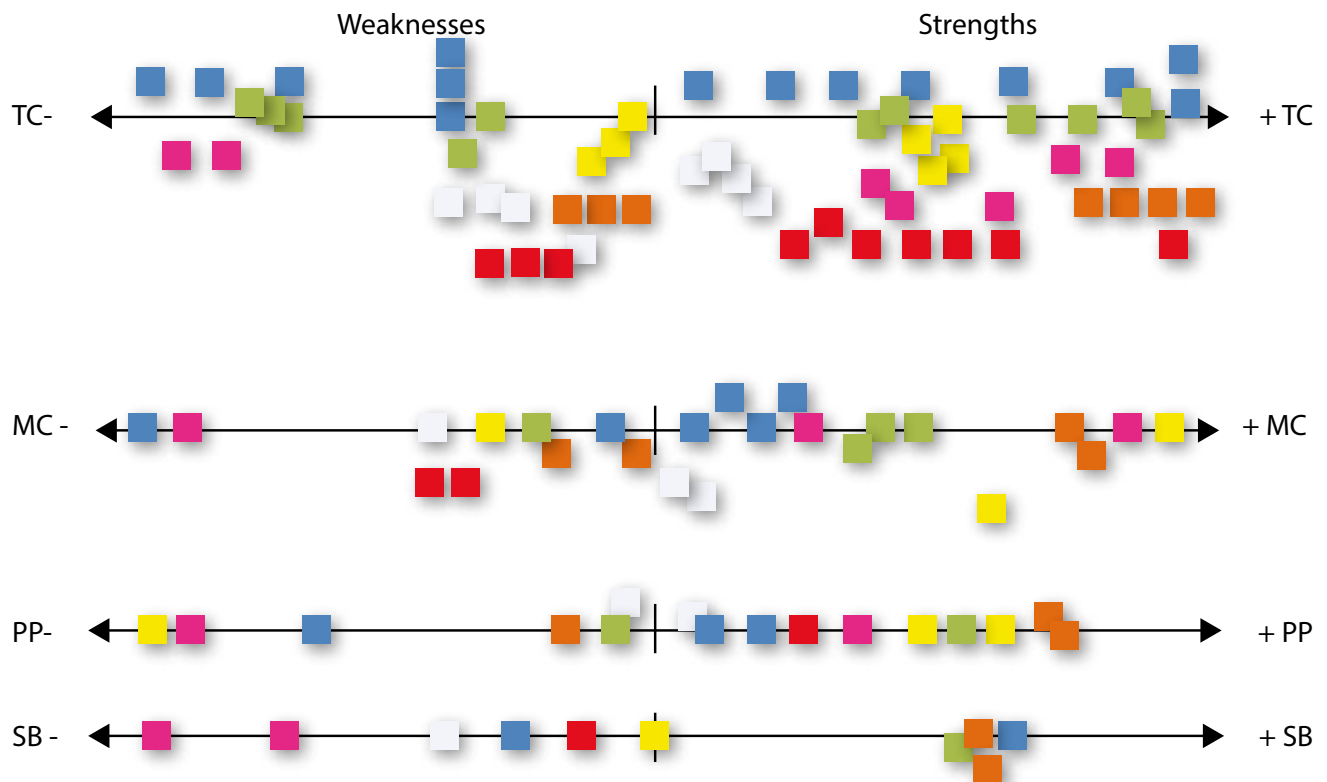
The first thing we did was to conduct an exercise in which every SSEB team member contributed to the development of a

proposal evaluation guide. Team members studied the definitions of adjectival ratings and findings and how they relate to the evaluation. They each prepared a list of authorized references (from Sections L and M) that they would use in their evaluation reports. They also developed a notional list of activities, relevant to their areas of evaluation, that they believed would “meet” the evaluation criteria. This served to ground each of the team members and help them understand the center mark from which strengths and weaknesses could be determined. We conducted these and other, similar exercises to ensure that the evaluators were in the right frame of mind and ready to do their work as soon as they received proposals.

There were several areas of the proposals we needed to evaluate, but for which we didn’t have a government subject-matter expert (SME) to include on the SSEB team. To solve this problem, we used contractor SMEs with specific skills to augment the SSEB team as nonvoting, “technical advisers.” The input from these SMEs proved invaluable and allowed the government team members to meet schedule and focus on writing reports.

Another decision we made before kicking off proposal evaluations was to adjust the time we allowed for the teams to complete the first evaluation. Instead of 2 weeks, we planned for the teams to take twice that time to allow them to develop their battle rhythm. We then invited the attorney from ACC-RI to meet with the SSEB teams immediately after the teams completed evaluating the initial proposal. The purpose of the

**Figure 3. Example of Board 3**



attorney's meeting was to assess their process and findings. This legal guidance and feedback helped the teams understand how all follow-on ENs needed to be written and did much to ensure the team started out on the right track. This saved time that otherwise would have been required for rework later.

**Q: Bringing together SSAC to conduct a comparative analysis of the proposals requires detailed planning. Can you describe how you planned for the SSAC comparative analysis and how your planning made the best use of the SSAC's time?**

**A:** The ACWS SSAC members were very senior. Because of their seniority and the level of responsibility of their primary jobs, they could only afford to dedicate 2 days for this activity. We had to come up with a process, in advance of their meetings, that would be effective and agreeable to all the members so they could conduct a thorough comparison in a relative short time and arrive at the right recommendation. The concept the PMO team developed was very similar to a scrum in an Agile process. Our process was simple, but highly effective because it allowed SSAC members to quickly organize data into visual patterns of strengths and weaknesses and to discuss their relative values. The process involved three steps using three separate scrum boards.

Step 1 was to identify discriminators (strengths and weakness) by offeror and organize them by evaluation factors. The KO asked each SSAC member individually to list discriminators

that he/she identified during review of the evaluation reports. Additional facilitators recorded these discriminators on colored "sticky" notes, one color for each offeror, and placed them on Board 1. The sticky notes were divided into two columns for each offeror: one for strengths and one for weaknesses.

After each SSAC member provided input, Board 1 looked something like Figure 1. Board 1 allowed the SSAC members to view the initial side-by-side comparison of strengths and weaknesses of each proposal. Figure 1 does not include any source-selection information and the number of offerors does not reflect the actual numbers of offerors in the ACWS source election.

During Step 2, the KO, under the direction of the SSAC members, transferred the colored sticky notes from Board 1 to Board 2, one at a time, by offeror. Board 2 included one row for each offeror that was a continuum with a minus sign to the left, a center mark in the middle, and a plus sign on the right. As the SSAC members transferred sticky notes from Board 1 to Board 2, they discussed the relative importance of each discriminator and placed it in the agreed-to order of importance on the continuum. After the sticky notes (discriminators) for one offeror were all transferred to Board 2, the group started transferring notes for the second offeror, and so on. At the end of Step 2, Board 2 included a listing of relative importance of the strengths and weaknesses of each offeror. At this point, patterns began to emerge that the SSAC could discuss. Figure 2 shows an example of what



Board 2 looked like (no source-selection data were used to create this example).


Step 3 was to arrange discriminators for all offerors by evaluation factor. The board required for this step included a row for each of the four evaluation factors: Technical Capability, Management Capability, Past Performance, and Small Business. The evaluation factors were placed from top to bottom in the same order of importance listed in the RFP. In this step, the SSAC members transferred the sticky notes from one of the offerors from Board 2 to Board 3 and placed them in the rows that corresponded to their appropriate evaluation factors. As they transferred the sticky notes, they took care to maintain the same relative position of importance on the continuum. The sticky notes from the first offeror transferred to Board 3 became the baseline from which the group would judge the importance of every other offeror's discriminator as they were transferred from Board 2 to Board 3.

The result of Step 3 was a visual tool that displayed the strengths and weaknesses of each Offeror, by evaluation factor, arranged in the order of importance as determined by the SSAC members and how they stacked up to the other Offerors. An example of what Board 3 looked like is included in Figure 3. No actual source-selection data were used to create this example.

Once the SSAC identified which stood out among the others, it was then easy to compare the cost of that proposal against the capability provided in that proposal and to make a recommendation as to the best value decision for the Army.

**Q: What was the final result of the efficiency initiatives that your team put into practice during the ACWS Source Selection?**

**A:** Well, I'm pleased to say that all the effort the team put into planning an aggressive source selection schedule, combined with the implementation of numerous efficiency initiatives that helped us stay on schedule, all resulted in a final SSA decision just over 8 months after proposal receipt, and contract award after only 11 months. I am convinced that if my team had accepted the status quo, this same process could have taken twice that long.

All PMs know that there are variables they can't control in the source-selection process. But with careful planning, a commitment to reduce PALT, and cooperation from the contracting community, the SSEB timeline can be significantly reduced, allowing PMs a greater likelihood of remaining within their cost and schedule baselines. 

The author can be contacted at [gregory.b.gonzalez.ctr@mail.mil](mailto:gregory.b.gonzalez.ctr@mail.mil).



DAU is continually looking for new topics, tools and resources to help you succeed on the job.

**HOW DO WE KNOW WHAT YOU NEED?  
YOU TELL US!**

**VISIT**

<https://www.dau.mil/tools/t/Request-a-New-Tool>  
Take a quick two-question survey on the topics, tools and resources you need.

# *Defense ARJ* and *Defense AT&L*

## Online-only for individual subscribers



# NEW

Online presence for  
easier use on mobile and desktop devices:  
<https://www.dau.mil/library/defense-arl>  
<https://www.dau.mil/library/arj>

Please subscribe or resubscribe so you will not miss out on accessing 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.

Type "Add to LISTSERV" in the subject line.

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







# Tabletop Exercises

## for Added Value in Affordable Acquisition

Eugene A. Razzetti

A tabletop exercise is an activity in which key personnel assigned high-level roles and responsibilities are gathered to deliberate various simulated emergency or rapid response situations. While tabletops frequently are used to improve team responses to disaster preparedness and emergency planning, they also can contribute to less time-critical challenges, such as program management.

Tabletop exercises can enable program managers (PMs) to:

- Evaluate all phases of programs, including emergency responses.
- Identify equipment design deficiencies or tactical shortcomings.
- Test or validate recently changed or modified strategies or tactics.
- Clarify objectives, roles, and responsibilities.
- Obtain feedback and recommendations from key participants, especially operators.
- Improve coordination.
- Develop metrics for use during program execution and actual operations.
- Identify/validate training requirements.
- Assess capabilities and identify needed personnel and material resources.
- Develop draft Concepts of Operations (CONOPS) and Techniques, Tactics, and Procedures (TTP) for further modification and improvement.
- Address fact-of-life issues, such as cybersecurity and antiterrorism/force protection.

### Tabletop Versus Wargame

Most members of the military understand wargames, and that's fine. Many senior officers have participated in them, which also is fine. Wargames, however, can be too hard to schedule, prepare for and fund—especially if lots of realism and participation are needed. Tabletops are easier, faster and, in their own way, can be just as productive.

Table 1 summarizes the similarities and differences between tabletop exercises and wargames. PMs can use tabletops to focus on the requirement for platforms, strategies, and uncertain sets of tactics and procedures, rather than the actual employment of each. Tabletop “play” focuses on validation of risks, needs and approaches, keeping in mind always the realities of retaliation by the adversary.

---

**Razzetti**, a retired U.S. Navy captain, is a management consultant, auditor and military analyst. He is the author of five management books, including “Hardening by Auditing—A Handbook for Measurably and Immediately Improving the Security Management of Any Organization,” and he has served on the advisory boards of two business schools.



PMs, desperate for time and funds, but not so desperate that they want to be pushed in the wrong direction, can accomplish a great deal with a tabletop.

### Setting Up a Relevant Tabletop

Figure 1 provides an overview of the tabletop development and implementation process discussed in this article. The value of the tabletop is a direct result of the amount of preparation that goes into it.

Preparation first, prediction later: PMs can see from Figure 1 that a tabletop exercise requires nothing that would not be essential to any sound Department of Defense (DoD) program. Neither does the tabletop pursue or discover any intelligence that does not have direct, measurable worth. Predictions reached as a result of tabletop are only as valuable as the preparation by all participants.

Conduct of the tabletop, over and above normal workaday management practices, can lead to validation or minor program modification, major engineering or organizational changes, or possibly program cancellation.

In the July-August 2017 issue of *Defense AT&L*, I wrote about the “Ethical Imperative and the Courage to Cancel.” A tabletop exercise as outlined in this article may provide PMs with just such an imperative, and a strong, defensible justification to cancel.

At the outset, the PM must ask several questions: What do I want to learn from the players? What do I want to convey to the players? How can the tabletop exercise optimally assure its goals and objectives? How do the participants reinforce each other? How is necessary information optimally exchanged? Does my program adequately address anti-terrorism, force protection, and crisis response? The final question should now be considered an indispensable element of any DoD program.

### Tabletop Objectives

The objective of the tabletop is support of the program itself; identification of material and non-material gaps and overlaps within the program as they relate to the successful completion of the mission; development of courses of (corrective) action (COA) based on threat and risk identification and assessment; and determination of the optimal function alignment of assigned forces in the command structure, as they pertain to roles and responsibilities, and finally, determination of optimal training and qualification approaches and strategies.

### Key Assumptions

Although the following are not all-inclusive, they are key assumptions for PMs and exercise planners and facilitators:

- The tabletop process will identify (if only at the early stages) the need for a robust Command, Control, Communications, Computers, Intelligence, Surveillance, and Recognizance (C4ISR) approach.

**Table 1. Tabletop Versus Wargame**

Areas of Tabletop Activity	Wargame	Tabletop
Program management and improvement	✓	✓
Adaptive to program stakeholder requirements	✓	✓
Strategy and concept development	✓	✓
Preliminary validation of operations and/or tactics	✓	✓
Logistic resupply	✓	✓
Evaluate preparedness	✓	✓
Threat and risk assessment	✓	✓
Needs assessment (e.g., training)	✓	✓
Define performance metrics and measures of effectiveness	✓	✓
Resources management	✓	✓
Disaster preparedness	✓	✓
Doctrine/checklist development	✓	✓
Pre-post incident evaluation and “hot wash-up”	✓	✓
Decisions	✓	✓
Conclusions, action plans, milestones, assignment of responsibilities, feedback	✓	✓
Two-sided, opposing, umpired maneuver	✓	
Actual Armed Forces elements participating	✓	
Computer modeled simulations	✓	

Table by the author.

- There will be a need for an anti-terrorism/force protection (AT/FP) capability, if only to protect own forces, regardless of the location or projected scenario.
- Operating forces will be subject to attack, and time on station will increase vulnerability.
- Regardless of the specific mission, operations not adequately planned or supported will take longer and increase force vulnerability, whereas well-planned and -supported operations will leave forces vulnerable for shorter periods, and therefore less vulnerable.
- Forces will operate from forward operating bases, where only limited resupply and maintenance can take place.
- Analyses resulting from the tabletop may, of necessity, be qualitative. There likely will not be sufficient data to all quantitative analyses, especially when projecting new equipment, strategy, or tactics.
- Risks (threats and vulnerabilities) that are identified and assessed will be reevaluated after a notional course of corrective action has been identified. Please see my article on

Risk Management in the July-August 2016 issue of *Defense AT&L*. In it, I employ the Formula: Risk = Threat x Criticality x Vulnerability.

- For the purposes of this tabletop, budgeting decisions are more important than warfighting decisions.
- Findings and recommendations for corrective action will be divided into three categories:
  - Material (technology-related)
  - Non-materiel (CONOPS, operational plans)
  - Functional alignment (operational chains of command)

Game play and analyses must identify areas of potential synergy and innovation (explained below).

### Tactical Situations Needed

Threats, vulnerabilities, mission criticalities, (i.e., risks), and COAs cannot be assessed in the abstract. Findings and recommendations without real-world frames of reference would not be credible or supportable, despite the best efforts of subject-matter experts.

Tactical Situations (TACSITs) are scenarios based on real-world conditions used to shape and forecast future operations. Modeling can be used when there is insufficient data or knowledge.

Figure 2 describes the creation and continuing improvement of TACSITs. As with almost any project, an ongoing feedback loop will increase productivity and potential contribution.

TACSITs should contain the scenario outline, the missions of the command(s) involved, the threat assessment, and the risk assessment (risk spreadsheets with standardized criteria).

TACSIT areas of focus should include (but are not limited to):

- Operational
  - Force selection
  - Exploiting the geography and the environment
  - Integrating platforms/exploiting capabilities
  - Tactical decision-making
  - Ability to rapidly assess changing tactical situations
- Command
  - Delegating authority (need for and ability to)
  - Lines of communication
  - Establishing information requirements for decision-making (i.e., The Commander's "Dashboard")

**Figure 1. Tabletop Development and Use**

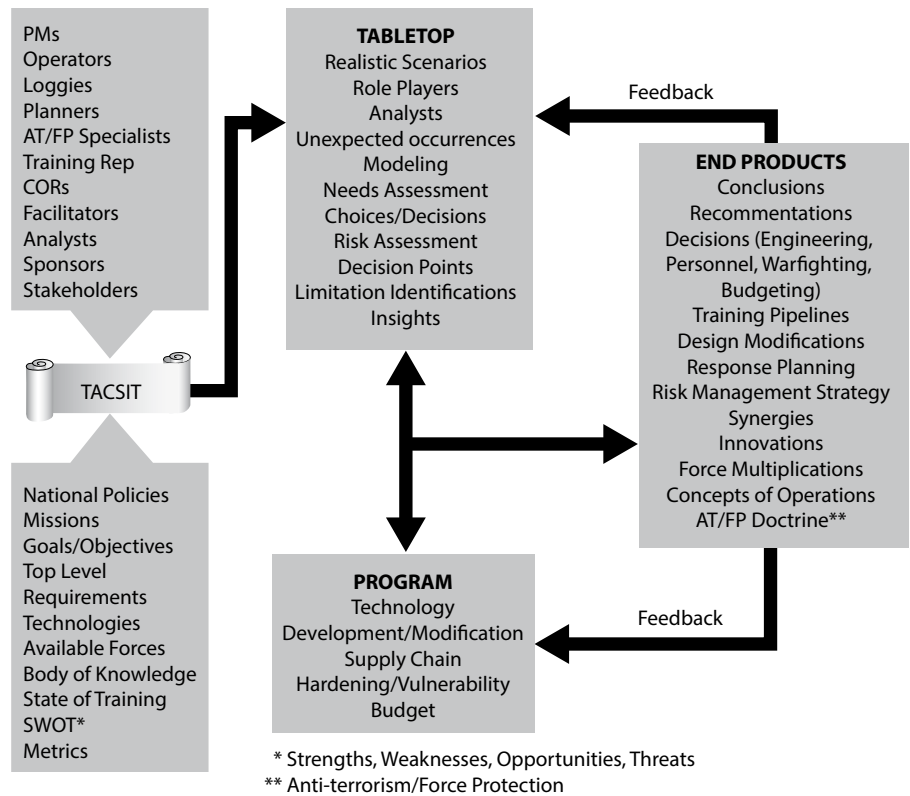


Figure by the author.

- Information processing
- Crisis response

In the creation phase, planners need to exploit the geography and environment, as well as the political situations. Since any product or strategy must work in a variety of places and scenarios, it makes sense to create a representative number of TACSITs.

**Figure 2. Tactical Situation Development**

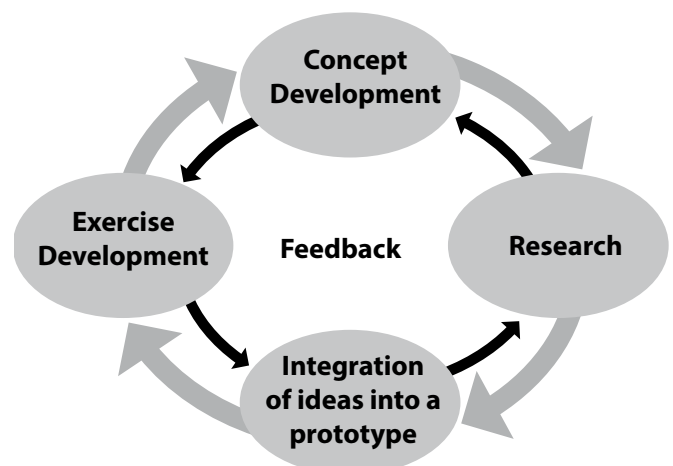


Figure by the author.

Several years ago, I helped develop TACSIT scenarios for West Africa, Iraq, Cambodia, Straits of Hormuz, Indonesia, Philippines, South Korea, and Montenegro, based on likely deployments of a joint or composite command.

Each location was an anticipated operating hot-spot region for the same contingency lead and support forces. Material solutions (new platforms and weapons) were barely in the design phase at that time. For that reason, the study group concentrated on Non-materiel (and) Functional Alignment solutions, and assessed their projected impact. We found that many problems for which new equipment was needed could, in fact, be mitigated to the same extent by realigning forces and rewriting operation orders and concepts of operations. It was in the rigorous development of non-materiel and functional alignment solutions that participants were better able to refine material solutions.

For example, movement of truck convoys in places like Iraq would be less vulnerable to attack if the current vehicles were replaced with some that offered increased armor protection and self-defense capabilities (materiel solution). However, routing those convoys around dangerous parts of town and late at night (rather than in full daylight) also reduced vulnerability to attack (non-materiel solution). Required implementation cost and time: Negligible.

Threats were identified, risks assessed, and COAs are notionalized. Risk assessment becomes risk management when participants evaluate the (projected) impact of the courses of action on the scenario.

### **Synergies—Making 1+1 = 2.5**

In the May-June 2009 issue of *Defense AT&L*, I wrote about Synergy and Innovation. Synergy is the combined or cooperative action of two or more stimuli for an enhanced effect, and that the whole becomes greater than the sum of its parts. Synergy can be quantified in subjective and objective metrics. Innovation is the introduction of something new or different, or the introduction of new things or methods. PMs want innovation but may not recognize it.

PMs must develop a synergy mindset that says 1 and 1 must equal 2.5 or it's not worth doing. The identification, quantification, and implementation of synergies are a vital part of the tabletop exercise.

Representative synergies to look for include enhanced survivability; force multiplication; operational reach; and consolidation of like processes. See Table 2.

### **Training Needs Analysis and Assessment**

Tabletop participants must (literally and figuratively) come to the table knowing what they need to look at and who needs what. PMs must know what all tabletop participants need to learn and understand, otherwise problems will go unaddressed and the tabletop will fall short of its goals. Nowhere

is this more important than in determining training needs. The completed tabletop should address individual and team training needs and qualifications, as well as their respective pipeline schooling.

Once identified, COAs should be categorized and collected for further discussion and the assignment of responsibilities as appropriate.

Materiel solutions require technological introduction/expansion of equipment, platforms, vehicles, computer systems, etc. Their introduction in the tabletop is the next step after nationalizing in special science and technology committees or workshops.

Non-materiel solutions do not require development of additional technologies, and presumably without excessive time and funding expenditures. Non-materiel solutions normally require internal reorganization, process development and documentation (e.g., CONOPs, standard operating procedures), and/or training, qualification, and the establishment of standards.

Functional Alignment Solutions are a special form of non-materiel solutions. These solutions may require component commanders to realign responsibilities. However, unlike the other non-materiel solutions, these may require approval at the highest DoD levels.

For purposes of illustration, we define "gap" as the difference between the level at which the capability is being performed currently and the level at which it must be performed to successfully accomplish the mission.

In addition to gaps, exercise participants should be alert to overlaps or redundancies; for example, when two subordinate commands establish separate logistics pipelines for the same parts, publish "almost identical" communication plans, or generate redundant reports.

Table 2 provides a notional listing of problems, the gaps that they create, and the attendant impediments to mission success; measurable, replicable metrics from which to judge improvement; and the potential synergy achieved through COA implementation. One example of each of the above three categories is shown for demonstration purposes. They are not the results of any particular study or exercise. Only one example of each of the three solution categories is shown.

A robust tabletop exercise enthusiastically planned and vigorously facilitated, would likely result in 100 identified shortcomings; and be considered a good day's work. Emphasis on the word "facilitated." The tabletop must not be allowed to get hung up or stray from the agenda.

A table like this, in which the categorized solutions are assigned tracking numbers, can serve as the baseline

**Table 2. Materiel, Non-Materiel and Functional Alignment Courses of Action (Fictional)**

Number	Capability Affected (Fictional)	Identified By	Gap	Course of Action	Metric	Synergies
Materiel 01	Navy Task Assigned (NTA) 6.2	Component commanders	Total Operational Authority (TOA) is below needed level and includes obsolescent equipment	Upgrade component command TOAs in numbers, suitability, and sustainment	Mission and on-station times (decrease)	Enhanced survivability, Force multiplication, operational reach, and like-process consolidation
Non-Materiel 01	NTA 6.4	Component commanders	High attrition of qualified officers/enlisted personnel with specific experience	Develop specializations and paths to promotion	Personnel numbers, qualities (increase)	Enhanced survivability force multiplication
Functional Alignment 01	NTA 6.5, 6.6	Component commanders	Anti-terrorism, Force protection training, not centralized or specific	Develop standardized training (e.g., train the trainer)	Personnel trained/qualified (increase)	Enhanced survivability force multiplication

Table by author.

documentation for the tabletop. Adding two columns marked “Assigned Responsibility” and “Completion Date” is all that is necessary for tracking and follow-up. The table then becomes a dynamic management tracking tool, rather than just a dry, ponderous, final report for the file cabinet, or (worse yet) the cloud.

Findings must be “actionable.” Esoteric or pie-in-the-sky musings on anyone’s part has no place in a world in which real threats require real solutions.

### What You Might Find Out

Here are some possible findings that may result from the tabletop:

- The design of the platform or system is too sophisticated, and the additional capabilities projected may not be required and/or may not be worth the increased time and funding requirements. This is often called “gold plating” a platform or piece of equipment.
- There is only limited stand-off chemical/biological detection capability and additional detection capabilities are needed.
- Construction engineers need lighter/stronger building materials to withstand projectiles and shrapnel.
- In-theater decisions are being made in the contiguous United States (CONUS), rather than by the in-theater commanders.
- Two (or more) subordinate commands in the operating area have created their own logistic pipelines for CONUS “reach-back.” One command can do all the requisitioning.
- The reporting superior of one of the in-theater commands has placed redundant reporting requirements on the subordinate. The superior can be copied on a report already in use.
- Personnel report to the theater of operations without sufficient general or specialized training and qualification.

Example: Port commanders and staffs report to ports of debarkation without necessary team training. This was a particularly challenging training problem when dealing with reservists recently called to active duty.

### Summary

Both wargames and tabletops can help PMs to know what they know and don’t know; and to find out what they don’t know they don’t know.

Wargames, however, can take a long time to prepare, schedule and execute. Further, they may focus too single-mindedly on the employment of specialized technologies and equipment, but assume too much about the structured programs that turn those technologies and equipment into reality, or trivialize the need for robust CONOPs and TTPs. A program may get the direction, threat and risk identification and analysis, and the actionable intelligence it needs from a tabletop exercise. Apply the program’s objectives to the tabletop. Then, craft realistic, facilitated, TACSIT scenarios; and play them out with qualified participants from all stakeholder organizations.

Look for every opportunity to identify and implement synergies. Make 1 + 1 equal 2.5 or seriously consider dropping pursuit of a program element.

Finally, generate and categorize courses of corrective action and assign metrics, milestones and responsibilities, and document them in a dynamic management tool.

Good luck!



The author can be contacted at [generazz@aol.com](mailto:generazz@aol.com).



[illegible]

## Want to help change the way DoD does business?

For more information and advice on how to submit your manuscript, check the writer's guidelines at <https://www.dau.mil/library/defense-atl/p/Writers-Guidelines> or contact the managing editor at [datl@dau.mil](mailto:datl@dau.mil).

If you're interested in having longer, scholarly articles considered for publication in the *Defense Acquisition Research Journal*, or if you're a subject-matter expert and would be willing to referee articles, contact the managing editor at [defensearj@dau.mil](mailto:defensearj@dau.mil). Be sure to check the guidelines for authors at <https://www.dau.mil/library/defense-atl/p/Writers-Guidelines>.





# THE QUEST for Defense Cybersecurity

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

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

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

---

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

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

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

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

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

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

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

## What Is Cybersecurity?

According to DoD Instruction (DoDI) 8500.01 (Cybersecurity), it is the “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” A 2015 RAND Corporation report on Air Force cybersecurity referenced

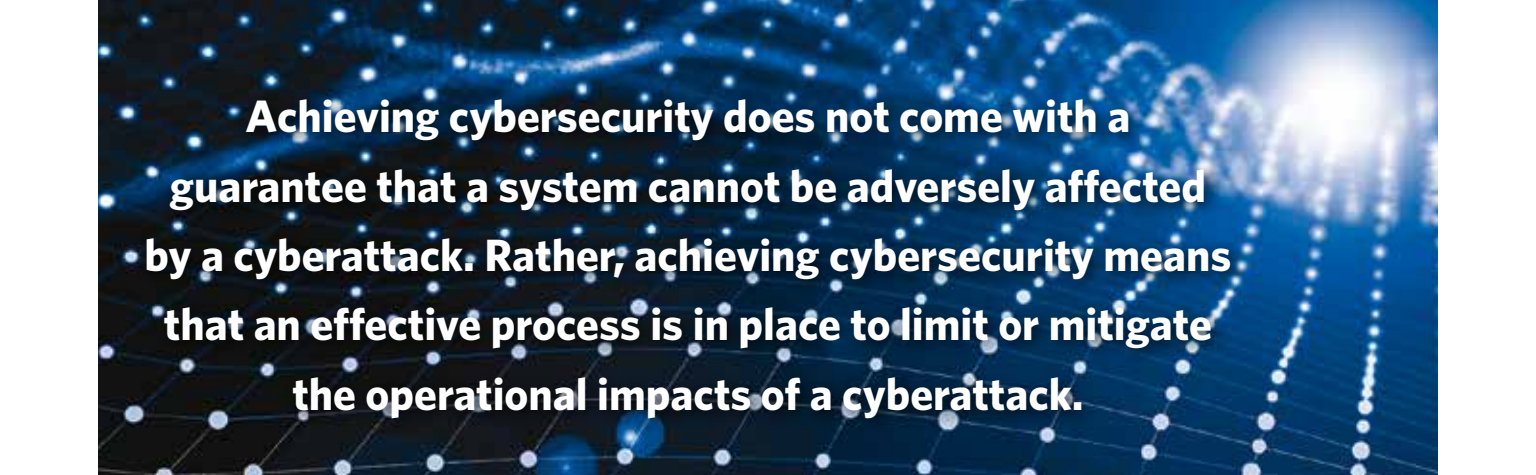
DoDI 8500.01 definition above, adding that cybersecurity is “limiting adversary intelligence exploitation to an acceptable level and ensuring an acceptable level of operational functionality (survivability) even when attacked offensively through cyberspace.” Cybersecurity should not be viewed as an end state. Achieving cybersecurity does not come with a guarantee that a system cannot be adversely affected by a cyberattack. Rather, achieving cybersecurity means that an effective process is in place to limit or mitigate the operational impacts of a cyberattack.

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

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

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





**Achieving cybersecurity does not come with a guarantee that a system cannot be adversely affected by a cyberattack. Rather, achieving cybersecurity means that an effective process is in place to limit or mitigate the operational impacts of a cyberattack.**

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

### **Looking at Our Theoretical Example**

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

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

What are the vulnerabilities of this very complex weapons system? Even in peacetime, the ship can expect routine cyberattacks on its communications pathways. In wartime, successful cyberattacks on its C4I, mission planning or other communications links could render this SoS ineffective or nonsurvivable. How can relevant vulnerabilities be identified? How should any

identified vulnerabilities be prioritized? What can be done to mitigate these vulnerabilities to provide the Jimmy Doolittle with cyber-resiliency?

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

### **First Main Focus: Start Early**

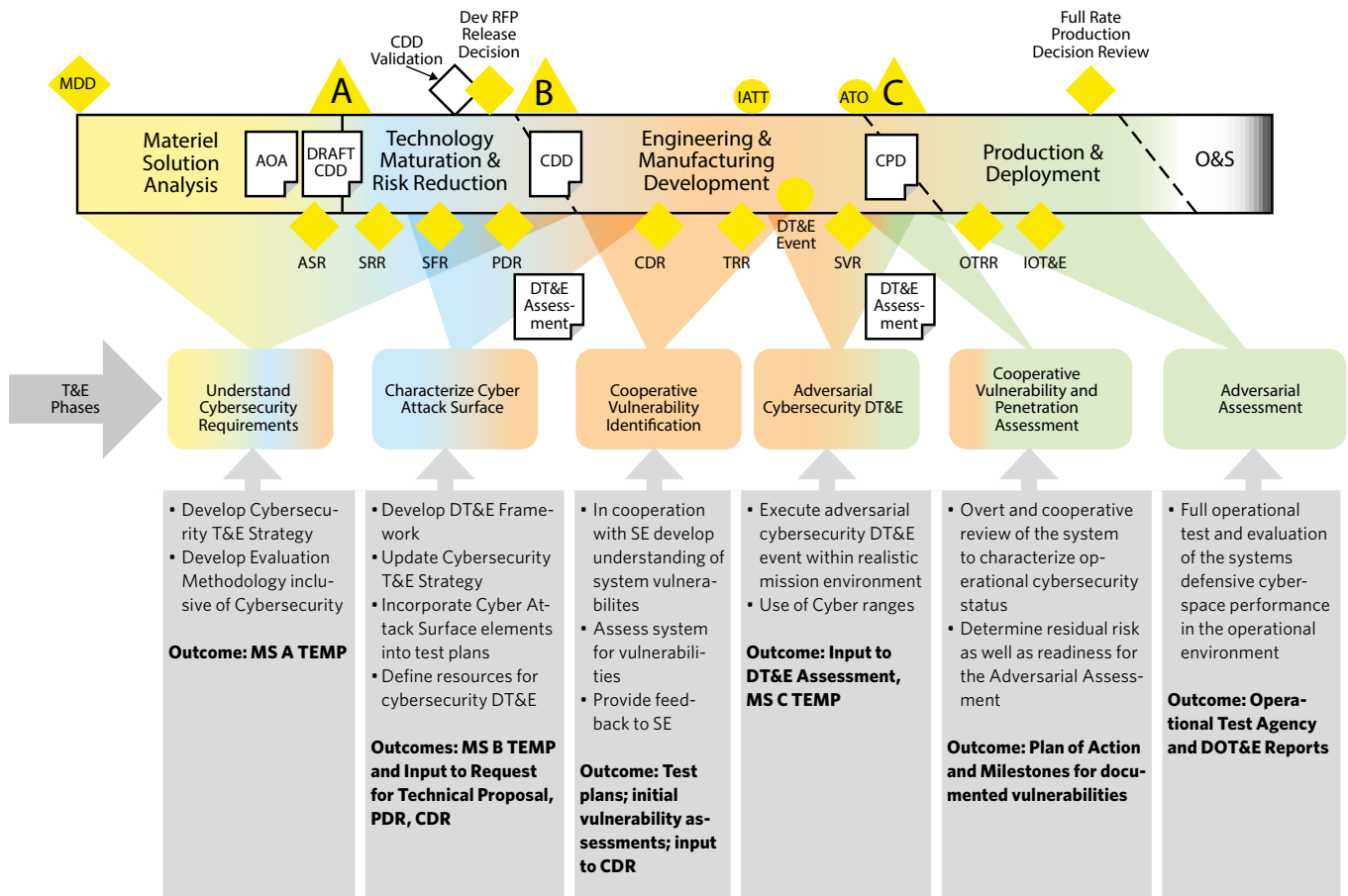
There were two primary focus areas to implement this process for cybersecurity.

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

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



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



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

#### Key to Abbreviations Used in Figure 1

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

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

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

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

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

## Second Main Focus: Test and Evaluation

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

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

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

The Doolittle COVA process directly supported the first three phases of the six-phase cybersecurity testing process: Understanding cybersecurity requirements; characterizing cyberattack surfaces; and identifying cooperative vulnerability. However, the results of the COVA also provided actionable and

credible inputs to the fourth phase: Adversarial cybersecurity developmental T&E.

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

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

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

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

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

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

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

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

## MDAP/MAIS Program Manager Changes

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

### **Army**

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

### **Navy/Marine Corps**

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

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

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

### **Air Force**

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


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

## Summary and Conclusion

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

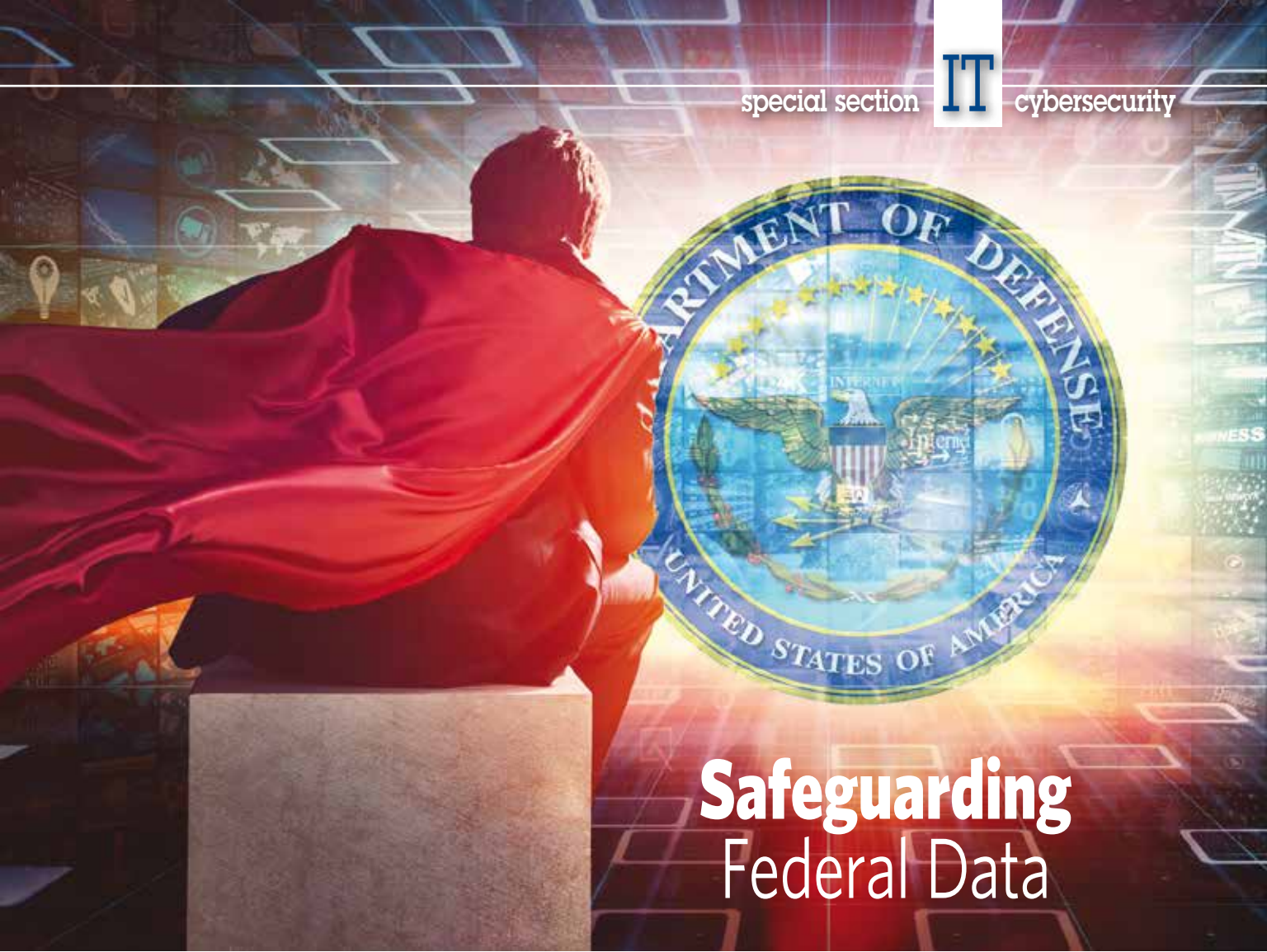
“The event was a ‘game changer’ in that it not only helped identify vulnerabilities but it tied them to mission risk and also helped with the culture change necessary to get our entire workforce behind this important topic. Getting our engineers, fleet, and program offices to understand exactly what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

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

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

The authors can be contacted at [JShaud@afa.org](mailto:JShaud@afa.org); [MLilienthal@ewa.com](mailto:MLilienthal@ewa.com); [SThompson@ewa.com](mailto:SThompson@ewa.com); and [DBrown@ewa.com](mailto:DBrown@ewa.com).





# Safeguarding Federal Data

*Janel C. Wallace, J.D.*

**R**ules for safeguarding information are increasing in number, as are cyberattacks on federal information. Everyone needs to know about the rules for safeguarding information so their agencies or businesses can comply with them and contracts can continue as planned.

These rules impact everyone, including small businesses, those delivering Federal Acquisition Regulation (FAR) Part 12 supplies and/or services, and contracts below the Simplified Acquisition Threshold (SAT) of \$150,000. This article discusses the FAR and other rules instituted to ensure the safeguarding of federal information.

## **FAR Changes**

FAR Subpart 4.19 and FAR Clause 52.204-21 became effective June 15, 2016. FAR Clause 52.204-21 is designed to require a contractor to safeguard some of its information systems as of the date of contract award. FAR Subpart 4.19 and FAR Clause 52.204-21 are attributable both to the changes made in the Federal Information Security Modernization Act of 2014, which provides for additional federal information security requirements, and the Office of Personnel and Management data breach that resulted in the theft of personnel records concerning

---

**Wallace** is a professor of Contract Management at the Defense Acquisition University at Fort Belvoir, Virginia. She is a U.S. Air Force veteran, a former litigation attorney, and a contract specialist. She holds a law degree from the University of North Dakota.



more than 20 million current and former federal employees and contractors.

The contractor information systems covered (“covered contractor information systems”) are defined in FAR Subpart 4.19. They include information systems that a contractor owns or operates that process, store or transmit federal contract information.

What does “federal contract information” mean, specifically? It is summarized as the kind of contract information that the government has no intention of releasing to the public. It is information provided by or generated for the government under a contract to develop a product for or service to the government. It excludes information provided by the government to the public or simple transactional information.

### **Application of the Rule**

FAR 52.204-21 should be added to a solicitation so that offerors are made aware of the safeguarding requirements that could apply to the contract. FAR 4.1903 requires insertion of FAR Clause 52.204-21 when a contractor or subcontractor at any tier may have federal contract information residing in or transiting through its information system. The focus of FAR 52.204-21 is on the information system(s) and not the information itself. That focus makes it unnecessary to specifically identify what information was created or compiled for the government or to decipher specifics about each set of information in a contract to determine its applicability to FAR 52.204-21.

Since the safeguarding requirements apply even in the case of a mere possibility of federal contract information residing in or transiting through a contractor’s or subcontractor’s information system, it is the responsibility of the government’s technical team to assess that possibility in drafting the contract requirements. The government’s technical team is relied upon instead of the contracting officer because the government team generally is more familiar with the information and information systems required by the contract.

Pursuant to FAR 7.105(b)(18), the acquisition plan must discuss compliance with FAR 4.19 when addressing the requirement’s security considerations if federal contract information may be residing or transiting through the contractor’s information systems.

### **Exceptions to the Rule**

Use of FAR 52.204-21 is not required when the procurement involves available, commercial off-the-shelf (COTS) items; the information has already been made public by the government; or when the information is simple transactional information such as that needed to process payments. COTS items were excluded as COTS is considered unlikely to include even the possibility of federal contract information residing or transiting through a contractor information system. The government inherently does not have an interest in protecting information

that is already available to the public. The government also does not have an interest in protecting simple transactional information since doing so may make the rule overbroad.

There are no exceptions to the safeguarding rule when contracts fall below the SAT because many acquisitions below the SAT may still involve a government interest that requires safeguarding. There are no exceptions to contracts falling under FAR Part 12 since information may need to be safeguarded despite the use of Part 12, particularly since Part 12 may utilize policies and procedures from other FAR parts.

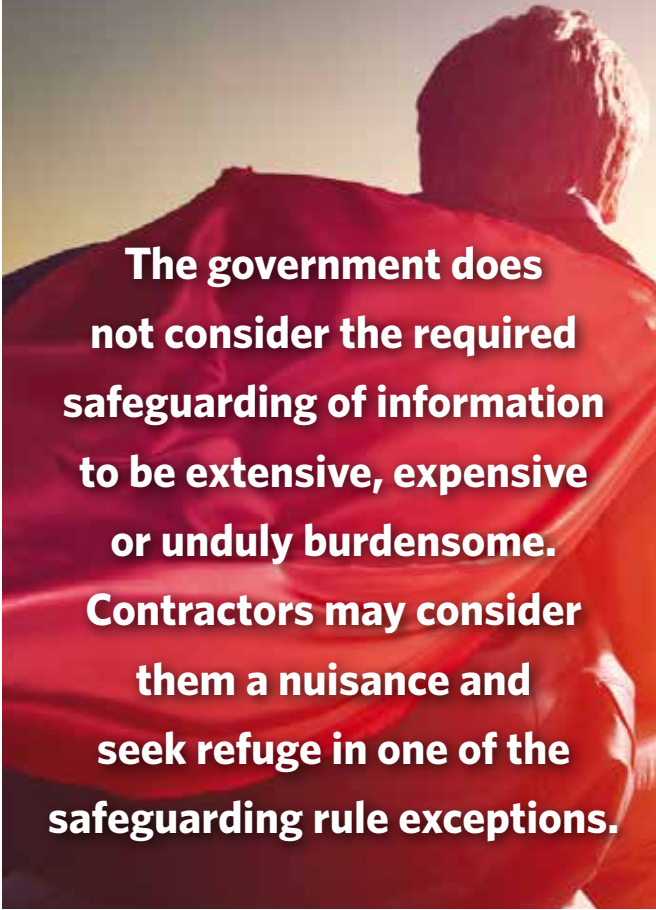
The government does not consider the required safeguarding of information to be extensive, expensive or unduly burdensome. Contractors may consider them a nuisance and seek refuge in one of the safeguarding rule exceptions. For instance, the COTS exception may result in contractors and subcontractors clamoring to categorize their supplies and/or services as COTS items to avoid the safeguard requirements. But contractors and subcontractors should realize that the government expects reduced prices for COTS supplies and services presumed to be sold in sufficiently large market quantities.

At present, it may not seem worthwhile for contractors to attempt to categorize their products or services as COTS. It may, however, become worthwhile as more stringent safeguarding requirements are developed.

### **Background**

Implementing FAR 4.19 and FAR Clause 52.204-21 are just two steps in a series of coordinated regulatory actions taken to strengthen protection of information systems. In May 2015, the National Archives and Records Administration (NARA), which was designated by Executive Order 13556 to implement the Controlled Unclassified Information (CUI) Program, issued a proposed rule to guide agencies and contractors in designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI that is not classified but also not intended for public disclosure. Only that information requiring safeguarding and dissemination controls pursuant to federal law or regulation and/or government-wide policy can be designated as CUI. Another focus of the CUI program is to prevent inconsistent markings and unnecessary restrictions.

On Sept. 14, 2016, NARA issued its final rule on CUI. NARA explained that the purpose of the program is to establish uniform requirements on how every agency handles each type of CUI. There are two types of CUI, basic and specified, which are now better defined. CUI that doesn’t provide specific protections in law, regulation or government-wide policy will fall into the basic category. The basic category provides the minimum controls and is where the majority of CUI will fall. NARA established and now maintains a CUI registry, which is the central location for guidance, policy, instructions and information pertaining to CUI.



**The government does not consider the required safeguarding of information to be extensive, expensive or unduly burdensome. Contractors may consider them a nuisance and seek refuge in one of the safeguarding rule exceptions.**

NARA and the National Institute of Standards and Technology (NIST) together developed guidelines on how controlled unclassified information should be protected when not under direct federal control. As a result, NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* was created in June 2015. NIST SP 800-171 provides agencies with recommended basic requirements for CUI. The FAR does not have direct references to NIST. However, it does require (in FAR 52.204-21) that contractors consider other safeguarding requirements applicable to the contract.

The Department of Defense (DoD), abiding by NARA's policy, implemented a rule through a revision of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. This revision resulted in a direct reference to the use of NIST SP 800-171 for systems that are not part of an information technology service or system operated on behalf of the government. The contractor is told in 252.204-7012 to implement NIST SP 800-171 no later than Dec. 31, 2017. A non-federal organization collecting or maintaining information on behalf of the government or operating or using systems on behalf of the government must follow the Federal Information Security Modernization Act, which includes the minimum security requirements of *Federal Information Processing Standards (FIPS) Publication 200* and SP NIST 800-53. Both are viewed as comparatively more burdensome than NIST SP 800-171. NIST SP 800-171 is a blend of NIST SP 800-53


and *FIPS Publication 200*. The use of NIST SP 800-171 may not satisfy the requirements of NIST SP 800-53 and *FIPS Publication 200*, which are more specific and stringent and do not generally apply to contractor systems.

The DoD interim rule also created DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," and DFARS 252.204-7009, "Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information." DFARS 252.204-7008 provides that, by submitting an offer, a contractor represents that it will implement the NIST SP 800-171 in effect at the time of the solicitation. DFARS 252.204-7008 also affords an offeror the opportunity to propose an approach that is different from any of the NIST SP 800-171 security requirements. If the different approach is approved by the DoD Chief Information Officer, it becomes part of the contract.

DFARS 252.204-7009 requires that a contractor agree to limit its use of cyber-incident information received from a third party in assisting or advising the government and not for any other purpose. In signing the contract, the contractor agrees to protect the information against disclosure or release and to ensure that its employees are subject to use and non-disclosure obligations prior to receiving access to the information. Penalties may be assessed against a contractor for violating the agreement. The third party reporter also would be empowered to seek civil damages and other remedies from a contractor that violates the agreement, making this clause exceptional by extending protection to a noncontractual party.

The safeguarding of information is not a new concept, particularly for the DoD, which issued an interim rule in February 2014 that resulted in creation of DFARS 204.74, "Disclosure of Information to Litigation Support Contractors." A final rule was issued on May 10, 2016, making it clear that a litigation support contractor will respond to a contracting officer's request upon completion of the litigation support by destroying or returning to the government all related litigation information in its possession. The final rule also makes it clear in DFARS 252.204-7014, "Limitations on the Use or Disclosure of Information by Litigation Support Contractors," that a contractor will not disclose any litigation information outside the contractor's organization without the contracting officer's written permission. "Sensitive information" is defined by DFARS 204.7401 and includes CUI of a commercial, financial, proprietary or privileged nature. Like the "federal contract information" definition of FAR 4.1901, "sensitive information" does not include information that is otherwise publicly available.

All the aforementioned DFARS clauses contain flow-down language requiring inclusion of each DFARS clause in subcontracts at any tier where required. FAR 52.204-21, although not specific to CUI like the aforementioned DFARS clauses, shares in the required flow-down language so that the



**If the impacts change due to more stringent regulation, there may be an adverse effect not only on small businesses but on the competitive environment.**

substance of the clause (including the flow-down language) must be inserted in subcontracts when the subcontractor might have federal contract information within or transmitted through its information system(s).

### **Review of Rule Comments**

The government responds to public comments on rule proposals. The responses to the then proposed rule 52.204-21 make it clear that more stringent rules are forthcoming on safeguarding information, particularly for CUI. Sixteen respondents commented on the FAR rule. The Civilian Agency Acquisition Council and Defense Acquisition Regulations Council (hereinafter referred to as “the Councils”) reviewed the comments as the councils were developing the final rule. Some of the considerations given to the comments are noteworthy. There were many concerns expressed in the comments about the proposed rule’s clarity. In responding, the councils opted for simplification in what apparently was an effort to avoid delay in implementing the rule. The councils opted to make the rule very broad, particularly as compared to its draft version, to avoid regulating in confusing specific terms.

The councils appeared to seek buy-in or acceptance of the idea that they simplified the rule enough to avoid hurting small businesses. The councils indicated their belief that the rule provides the most basic safeguards that a prudent business person would exercise even if the rule did not exist. A review of FAR Clause 52.204-21 appears to indicate that the minimum requirements are far from being egregiously prohibitive.

If the impacts change due to more stringent regulation, there may be an adverse effect not only on small businesses but on the competitive environment. In that case, there would be an increase in both the actual costs that offerors will pass on to the Federal Government and in costs directly attributed to decreased competition. The question then would shift to whether the information-safeguarding rules are worth the government’s overall cost of implementing and enforcing them. It may ultimately be left to the contracting officer’s discretion to determine whether the federal contract information involved needs the stringent safeguards or instead can be protected by the minimal safeguards of the current FAR 52.204-21.

Other comments on the FAR rule expressed concern that the rule would not be in conformity with the NIST’s requirements. One comment suggested that the councils wait pending the final NARA rules pursuant to Executive Order 13556. The councils recognized the validity of the concerns expressed but declined to await the final NARA rule. The Councils instead indicated that they would stipulate through FAR 52.204-21 that contractors are not relieved of the requirement to abide by any other specific safeguarding requirements (i.e., from the NIST), including those for CUI as established by Executive Order 13556.

Other areas of concern regarded the conveying of information via e-mail, voice, fax, text messages and blogs. The councils considered these communication media as being out of scope with the current rule. The focus was intended to be on the information systems as opposed to the information itself. This may be confusing to some, since the type of information conveyed would seem to define what information systems are covered. According to Title 44 U.S. Code Section 3502, an information system is defined in part as including information resources organized for processing, sharing and disseminating information. In considering what constitutes an information system, it would appear that e-mail, fax, text messages and blogs indirectly fall under the requirements of information systems from which they are delivered if the information sent might contain federal contract information. It is important to remember that it is the information system that is regulated rather than the information itself, and that a contractor must put forth a good faith effort to protect its systems.

### **Conclusion**

It is important to know how the rules for safeguarding information affect your agency regardless of whether the rule falls under NIST, DFARS or FAR. The councils made it clear that more stringent rules are on the horizon. The protection of federal information requires that we are neither too relaxed about disclosing our information nor too stringently regulatory. The balance may shift to one side or the other, depending upon the future level of cyberattacks and technology development. &

---

*The author can be contacted at [janel.wallace@dau.mil](mailto:janel.wallace@dau.mil).*

# FREE ONLINE SUBSCRIPTION

☐ *Defense ARJ*

*Defense AT&L* ☐

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

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

☐ *New Online Subscription*

☐ *Cancellation*

☐ *Change of E-mail Address*

Date

Last Name: \_\_\_\_\_

First Name: \_\_\_\_\_

Day/Work Phone: \_\_\_\_\_

E-mail Address: \_\_\_\_\_

Signature: (Required) \_\_\_\_\_

PLEASE FAX TO: 703-805-2917, or

E-MAIL TO: [datlonline@dau.mil](mailto:datlonline@dau.mil)

## **The Privacy Act and Freedom of Information Act**

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

# SUBSCRIPTION



# Better Communications on IT Spending Risks

Robert D. Frum, DCS

**W**hy are million-dollar information technology (IT) investment decisions based on single-point green, yellow, and red visual indicators, which are poorly defined and ineffective abstractions of the fundamental components of risk—probability and impact? Decisions are founded on a weak understanding of the risk without considering a range of possible outcomes for any choice of action.

IT professionals can significantly improve how they assess and communicate program risk to business investment decision makers, who must allocate funds among competing priorities. We can reform our communication of risk to

---

**Frum**, a retired U.S. Army lieutenant colonel, is the Chief Information Officer in the Navy International Programs Office. He holds bachelor's degrees in Political Science and Computer Science, master's degrees in Business Administration and Management Information Systems, as well as a doctorate in Computer Science. He also is Level II certified in Information Technology under the Defense Acquisition Workforce Improvement Act and a certified Project Management Professional. The views expressed are the author's own and do not reflect those of the U.S. Navy or the Federal Government.



business leaders so we provide a range of estimated outcome values, within a confidence interval that reflects the inherent uncertainties of large, complex decisions.

Monte Carlo simulation prepared with standard Microsoft Excel is a low-cost, yet effective, method for quantifiably modelling risk. Displaying the simulation results graphically as a familiar management histogram chart overlaid with a risk expectancy line enables uncertainty to be precisely articulated within a confidence interval for better-informed decision making. Risk variable values can also be changed on the fly to support dynamic what-if analysis. The model presented by the author was developed from material taught by Derek E. Brink, a Certified Information Systems Security Professional, in Harvard University's Division of Continuing Education course "How to Assess and Communicate Risk in Information Security."

The stakes are high. The federal IT dashboard indicates that government-wide IT spending for fiscal year (FY)

2017 totals about \$81.6 billion. The site also specifies that for all major IT investments government-wide, 3.4 percent of the projects are considered to be high risk, and 23.2 percent are considered medium risk. The U.S. Government Accountability Office has issued several reports between 2011 and 2015 documenting failed major IT projects, including eight projects valued at more than \$8.5 billion. Improved risk analysis and communication would return substantial value. For example, if the cost of failed programs was reduced by merely 1 percent, this would amount to more than \$85 million saved on these eight projects alone.

The key or greatest facilitator of informed business decisions is communicating data uncertainty as a frequency and impact distribution, overlaid with an exceedance probability (EP) curve at the desired confidence level. The concept may seem complex, but the technique has been widely applied in financial, insurance, actuary, and catastrophe planning to estimate the probability that a certain level of loss will be exceeded over a given time.

I offer three assumptions regarding risk that show why I believe we must improve our assessment and communication of risk. These include:

- Risk is fundamentally determined by the likelihood of an undesirable event, and the impact of such an event.
- Risk in federal IT programs is mostly presented in qualitative terms of colors—red (high), yellow (medium) or green (low).
- Risk assessment and management are important activities for successful project management.

### A More Detailed Look

Risk determination depends upon the type of threat, weakness or vulnerability. However, framing risk based only on potential dangers does very little to enable value-based investment judgments. In fact, using technical jargon to present risk supports poor value judgments because there is no assessment of the odds that something bad actually will happen. As a result, decision makers often are left with only a binary choice of whether to commit resources. For example, the IT professional might describe a cyber-security risk as an unauthorized access breach that could expose employee records to compromise if stronger access management controls are not put into place. In the best-case scenario, the business leader is somewhat better informed and at worst has misleading value information on which to base decisions. Properly framing risk in terms of the probability and associated consequence magnitude allows evaluation of the level of uncertainty. Communicating the same cyber risk as a 10 percent probability that unauthorized access could result in an annual business cost of \$2 million enables the organization leaders to determine how much risk they are willing to mitigate at the corresponding cost.

Again, most risk in federal programs is presented as red, yellow or green. The color scheme is a risk representation convention described by the Department of Defense's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. The approach to relative risk levels attempts to assess risk based upon Likert scales ranging from "not likely" to "near certainty" and "minimal impact" to "critical impact." Likert scales are ordinal, meaning the data can be ranked but not accurately interpreted mathematically. In short, risk heat maps should be limited to the most basic risk prioritization. As a business investment decision support tool, the color-coded representation is ineffective for articulating quantified risk probability distributions for a range of possible outcomes for any meaningful choice of action.

Risk management seeks to define uncertainty as the probability of an event—and the business effect, positive or negative, of such an event. In terms of program and project management, risk is most often expressed for individual cost, schedule and performance variables in relationship to delivering the end product. Different disciplines such as research, engineering development, and logistics may each have its own perspective on project risk. But managing activity risk must not be confused with investment decisions that aggregate the effect of all variables to permit best-value business case investment analysis.

The subject-matter expert (SME) plays an essential role in determining risk. SMEs typically are more knowledgeable than others regarding uncertainty measures within their areas. Using the unauthorized access breach example, the cybersecurity SME might estimate the likelihood that the

## Figure 1. Risk Simulation Model

**Business impact risk = what is the risk that a longer project length will increase cost?**

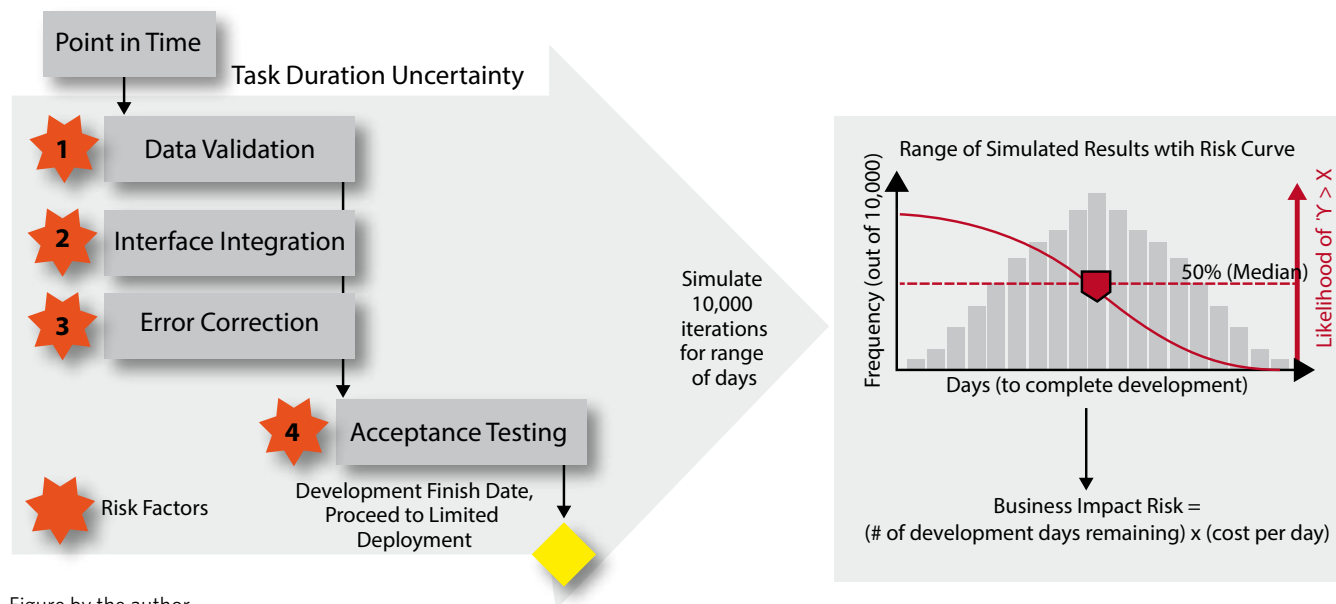


Figure by the author.



Figure 2. Project Risk Simulation

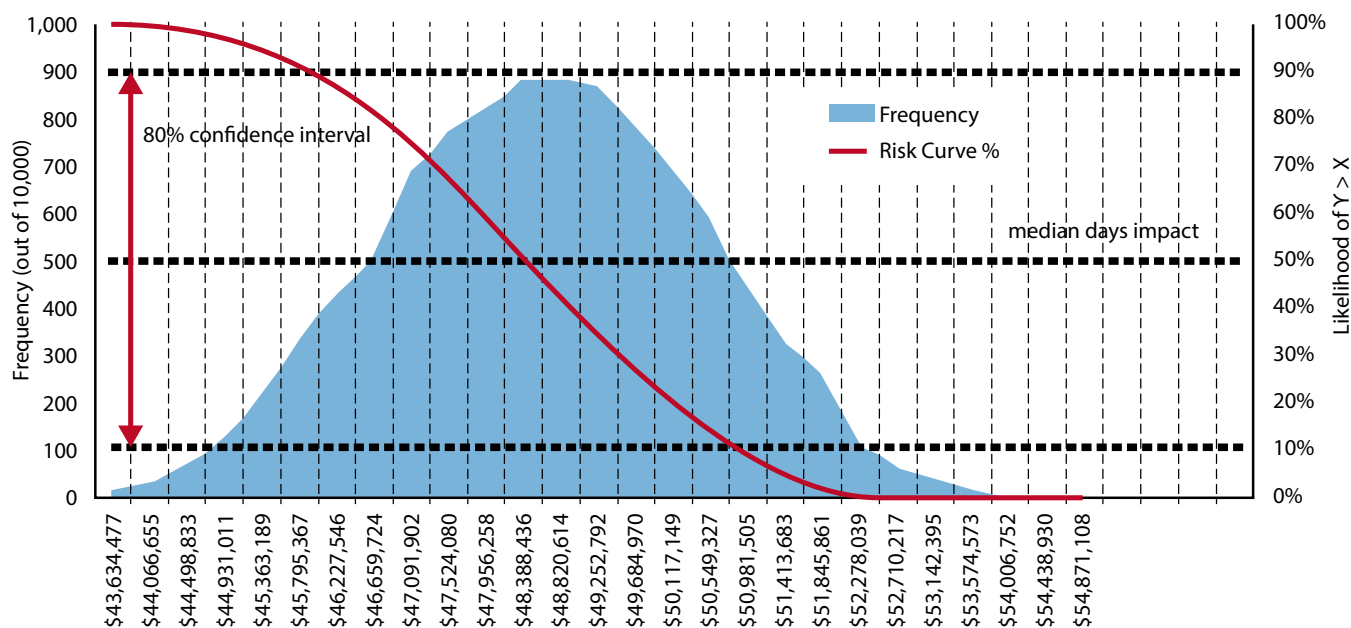


Figure by the author.

organization could experience between one and three unauthorized access breaches within the next 12 months, in line with the 2016 Ponemon Institute data breach study reporting about a 26 percent likelihood of a company having one or more data breaches involving at least 10,000 records in the following 24 months. The SME knowledge, supplemented with historical and industry data, provides a reasonable measurement of the factors of risk, while incorporating the inherent uncertainty. Typical—though insufficient—risk representation would then simply apply an annualized loss expectancy (ALE) calculation such as *annual loss = (likelihood of at least one breach) x (estimated number of breaches per year) x (estimated cost per breach)*. Given a breach cost estimated at \$100,000, an ALE statement would quantify the annual potential risk as an average of \$200,000. Based on this rudimentary cost analysis, risk then would be conventionally presented as red, yellow or green ordinal choices for the business leader to determine if the potential loss would be worth the financial investment needed to mitigate the risk.

Monte Carlo simulation is an excellent quantitative method for determining the likelihood of a potential loss within any of several designated intervals, over a range of values. Standard Microsoft Excel is more than adequate for creating simulation models and displaying possible scenario impact outcomes graphically as familiar charts. In the simulation model, the SMEs provide their estimates for the risk factors; specifically, providing the values for the upper and lower bounds, with a 90 percent certainty.

For example, consider a hypothetical software development project for which the business leader wants to assess the risk of the project's \$40 million budget and submits the Business

Impact Question: What is the risk that a longer development time will increase the overall project cost? Figure 1 illustrates the project simulation risk model, with four key risk variables that fundamentally determine the overall project duration. The model simulates the number of days to complete each factor. Factors 1, 2 and 3 are accomplished in parallel and must be completed before Factor 4 can begin; Factor 4 is then added to the highest of the three values. Daily cost is then applied to the resulting number of days.

Figure 3. Risk Simulation Chart

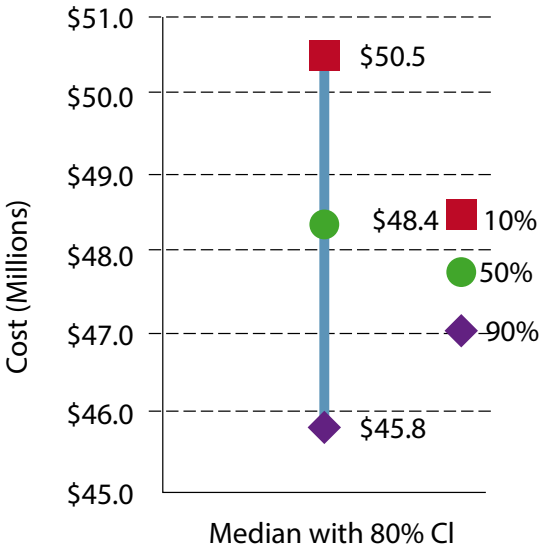


Figure by the author.

## SECTION 3685, TITLE 39, U.S.C. SHOWING OWNERSHIP, MANAGEMENT, AND CIRCULATION

*Defense AT&L* is published bimonthly at the Defense Acquisition University, Fort Belvoir, Va. 22060-5565. The university publishes six issues annually. The director of the DAU Press is Randy Weekes; the managing editor of *Defense AT&L* is Benjamin Tyree; and the publisher is the Defense Acquisition University Press. All are colocated at the following address: Defense Acquisition University, Attn: DAU Press, 9820 Belvoir Rd., Ste. 3, Fort Belvoir, VA 22060-5565.

### Average Number of Copies of Each Issue During the Preceding 12 Months

A. Total number of copies printed  
(net press run): \_\_\_\_\_ 3353  
B. Paid and/or requested circulation: \_\_\_\_\_ 3227  
1. Sales through dealers and carriers,  
street vendors, and counter sales: \_\_\_\_\_ 0  
2. Mail subscriptions paid and/or  
requested: \_\_\_\_\_ 3227  
C. Total paid and/or requested circulation: \_\_\_\_\_ 3227  
D. Free distribution by mail, carrier, or other  
means; samples, complimentary,  
and other free copies: \_\_\_\_\_ 71  
E. Total distribution: \_\_\_\_\_ 3298  
F. Copies not distributed: \_\_\_\_\_ 55  
G. Total: \_\_\_\_\_ 3553

### Actual Number of Copies of Single Issue Published Nearest to Filing Date

A. Total number of copies printed  
(net press run): \_\_\_\_\_ 3305  
B. Paid and/or requested circulation:  
1. Sales through dealers and carriers,  
street vendors, and counter sales: \_\_\_\_\_ 0  
2. Mail subscriptions paid and/or  
requested: \_\_\_\_\_ 3189  
C. Total paid and/or requested circulation: \_\_\_\_\_ 3189  
D. Free distribution by mail, carrier, or other  
means; samples, complimentary,  
and other free copies: \_\_\_\_\_ 46  
E. Total distribution: \_\_\_\_\_ 3235  
F. Copies not distributed: \_\_\_\_\_ 70  
G. Total: \_\_\_\_\_ 3305

The probability and impact simulation results for this hypothetical project are displayed in Figure 2, indicating that for 10,000 simulations there is a 90 percent likelihood that the annual cost will exceed about \$46 million and a 10 percent probability that the annual cost will exceed about \$50 million, with a median (50 percent likelihood) expected annual cost of about \$48 million. The values between 90 percent and 10 percent represent an 80 percent confidence interval, but any level of risk can be determined simply by examining the exceedance probability curve.

When communicating with business leaders, the same information could be presented as in Figure 3. Because Excel calculates 10,000 simulations of this model in about 1 second, leaders could quickly receive answers to “what if” sensitivity analysis questions that change the risk simulation variable values such as labor and material costs, purchase versus lease, number of units produced or purchased, workforce size and payment schedules. Creating an initial risk simulation model from existing Monte Carlo modeling templates took about a week, but subsequently building the model used in this example took only about 1 hour. The simulation model is clearly a significant improvement over ALE and red-yellow-green risk communication. First, simulation considers thousands of possible outcomes, not just the average outcome. Second, simulation assesses the likelihood of each outcome. Third, risk analysis can then be communicated as quantified values rather than hunches or guesses.

### Conclusions and Recommendations

Business leaders facing uncertainty for significant investments in complex and expensive IT projects require more than simple risk heat maps to inform their decisions. Accurate and meaningful communication of risk requires a quantitative measurement of business impact. Risk simulation provides an inexpensive yet effective method for reducing uncertainty, by quantifying probability and impact for a possible future event, within a specified time period, over a range of values, with a specified confidence level. Communicating risk as, “90 percent likelihood that the annual cost will exceed about \$46 million with a median (50 percent likelihood) annual cost of about \$48 million” is far more useful to making a better-informed business decision than simply stating that increased project cost is “Very Low, Low, Moderate, High, or Very High.”

To begin transitioning from risk matrix to risk simulation for investment circumstances I recommend the following:

- Schedule FY 2018 and FY 2019 for discussion, publishing guidance and creating training opportunities. Then, beginning in FY 2020, provide that Monte Carlo risk simulation become mandatory for all IT investment decisions exceeding \$1 million.
- Establish a library of basic simulation models and tutorials to facilitate rapid development for a variety of applications. &

The author can be contacted at [robert.frum@navy.mil](mailto:robert.frum@navy.mil).

## 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. For each article submitted, please include three to four keywords that can be used to facilitate Web and data base searches.

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

### Deadlines

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

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

### Audience

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

### Style

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

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

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

### Length

Articles should be 1,500-2,500 words.

### Format

Send submissions via e-mail as Microsoft Word attachments.

### Graphics

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

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

### Right to Use Illustrations

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

### Author Information

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

### Copyright

All articles require a signed Work of the U.S. Government/Copyright Release form, available at [https://www.dau.mil/library/defense-atl/Lists/PageContent/Attachments/6/DATLcopyright-release\\_032217.pdf](https://www.dau.mil/library/defense-atl/Lists/PageContent/Attachments/6/DATLcopyright-release_032217.pdf). 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, <https://www.dau.mil>.