the newsletter of
RELIABILITY, MAINTAINABILITY, & SUPPORTABILITY

December 2015 • Volume 19 • Issue No. 4

THIS EDITION

Published Quarterly

Sandra I. Erwin

DoD Mulls Changes to Weapons Maintenance Contracts

The Pentagon's top weapons buyer Frank Kendall hammers home to his staff the importance of "incentivizing" contractors to cut costs in every way possible.

One area where he hopes to squeeze significant savings is in weapons maintenance, a $170 billion a year business that is, by most accounts, fraught with inefficiency.

Kendall, who is undersecretary of defense for acquisition, technology and logistics, has directed procurement officials to investigate commercial-like approaches to maintaining equipment as an alternative to traditional contracts. The commercial method, known as "performance-based logistics," was in vogue in the 1990s but fell out of favor in recent years.

According to the consulting firm Deloitte LLP, the Defense Department could save up to $20 billion a year by switching many of its current support contracts to performance-based logistics, or PBL, arrangements.

Within the Pentagon's $170 billion logistics budget, $79.5 billion is for equipment maintenance, $68.4 billion is for spare parts and supplies and $23.1 billion goes to transportation. PBLs would offer savings of between 10 to 20 percent in the first two areas, Deloitte estimated.

To realize these savings, the Defense Department would have to switch the way it uses carrots and sticks. In a traditional transactional contract, the government pays for products or services delivered. In a PBL contract, a vendor is paid for a pre-agreed outcome that it must provide at a fixed price. For example, a PBL might require that a certain number of aircraft in a fighter wing be available to fly, for a set price per hour. Other PBLs deal with weapon components like sensors or engines. Many foreign militaries use PBLs for wholesale weapons maintenance and for operator training.

Critics of the current system argue that the Defense Department pays far more for equipment sustainment and experiences poorer service than if it used PBL contracts. This criticism, however, often falls on deaf ears. Fewer than 90 PBL contracts are in place today – less than half the number that existed in 2005. Few new PBLs are being pursued, and the military services are choosing to not renew some existing PBLs. Deloitte analysts, who conducted a study on performance-based logistics for the Pentagon two years ago, concluded that government buyers have soured on PBLs because these contracts are complex and not well understood.

Kendall agreed that PBLs can be a steep learning curve. A key struggle for managers is to define performance and determine if the price offered by the contractor is fair. "We will define performance in a way that is relevant to the operational community and reward people for doing a better job," Kendall told an industry conference. "Contract types that are tailored for doing that are the essence," he said. "Our research shows it works in some cases but it doesn't work in cases when people have not written a good contract and haven't enforced that contract."

Russell A. Vacante, Ph.D.

Resiliency: A Feature of Reliability Design for "Systems of Systems"

Reliability is defined as "the ability of a system to perform its intended mission when operating for a designated period of time, or through a mission scenario (or series of scenarios), in a realistic operating environment."[1] The subject of "resiliency" and its relationship to reliability, however, has recently been brought to my attention.

A review of engineering literature reveals the concept of "resiliency" as "the act of rebounding or springing back."[2] While I have on occasion thought about the ability of systems to recover after encountering a service disruption, for example, a desktop computer shutting down due to a virus, I seldom considered the need for a system to rapidly recover as a reliability issue. The concept of

1 Blanchard Benjamin S., Fabrycky, Wolter J., Systems Engineering Analysis, Fifth Edition, Prentice Hall, p.362.

2 SeeBok, Resilience Engineering, available at: http://sebokwiki.org/wiki/Resilience_Engineering, visited 11/22/15.

continued on page 7

GOOD NEWS FROM FLORIDA INSTITUTE OF TECHNOLOGY AND THE RMS PARTNERSHIP

The RMSP has established a new partnership with the Florida Institute of Technology (FIT) that promises real benefits to its members!

In cooperation with FIT, the RMSP will now offer Continuing Education Units (CEU) of credit for training in reliability, maintainability, and sustainability. These courses will be provided both online and onsite.

Professional logisticians will be able use the courses to meet annual training requirements, as well as, for professional development. A short description of training courses are available at *www.rmspartnership.org*.

Requests for training can be discussed with Dr. Russell A. Vacante at: president@rmspartnership.org

Kendall suggested that the Pentagon will sign more PBL deals in the future, but it could take time to train the government workforce how to write these contracts. "I'm a firm believer in incentivizing industry. We just have to be smart about how we lay those incentives out."

After a contract is awarded, government managers have to make sure the contractor is living up to the promises, and must punish non-performers, he said. "Everyone who has a contract ought to be worried about losing that contract next time around. If you are going to do a PBL, you have to do it correctly. You have to define the metrics of success."

Defense procurement experts warn that Kendall might be underestimating the challenge of using performance-based contracts, even if, in theory, they make financial sense.

"PBL contracts have a lot of potential to save money," said defense budget analyst Todd Harrison, of the Center for Strategic and Budgetary Assessments. "If you do the contract right, it creates better incentives for the contractor."

The rub, though, is that these contracts demand a considerable level of trust between government managers and suppliers. Defense officials have to let contractors decide how the work should be done, as long as they deliver the performance that was agreed upon, Harrison observed. The government also has less control over the contractor's profits, which can irk some officials. "If aircraft don't break as much, the company can make more money. Right now, under traditional contracts, we pay contractors every time something breaks," said Harrison. Contractors make more money the more the equipment breaks down under the conventional contracting system, so there is no incentive for the contractor to invest in more reliable components. "PBL turns this on its head. It gives a company incentive to improve parts. They get paid the same but repair less. ... It's a matter of setting up the incentives right."

Defense Department officials have a hard time wrapping their heads around this, said Harrison, because industry will come to them with a bid price, and the government is not sure if it is getting a good deal. "They want to know the cost, not the price, so they can determine how much profit the company is making," he said. "The point I would make to the Defense Department is that it shouldn't concern itself with the actual cost, all that matters to you is the price you pay. If the company can deliver the service you want at a price you're willing to pay, who cares what profit margins they're making as long as you're getting what you paid for, at a fair price."

Another caveat that could stall PBLs is that contractors expect these deals to be multiyear contracts. Companies will not want to invest in improvements that are going to pay off outside the window of their contract. Both the Defense Department and Congress have wavered on the merits of multiyear contracts. They question whether long-term deals promote complacency. The reality is that there is limited competition in the defense market, and the Pentagon has to accept that, said Harrison. The original manufacturer of a weapon system is going to always have a huge advantage. "Especially in highly regulated systems, not anyone can build parts," he said. If competition is artificially created by allowing vendors to bid based on buying parts from the OEM and selling them to the government, that just adds a middleman. "How's that supposed to save money?" Harrison asked. "When there's a natural monopoly, the Defense Department is better off giving OEMs incentives to lower cost, and long-term incentives." The Pentagon has to figure out how to pay more for higher levels of equipment readiness and less for lower levels of readiness, and write a contract accordingly, he said.

Al Banghart, senior adviser at Deloitte Consulting LLP, has been working with the Pentagon's procurement office for years, and led a study that quantified the savings that could be wrung from PBL deals. He is seeing signs from Kendall's office that there is high-level support for PBL contracts.

The recent publication of the "Department of Defense PBL Guidebook" is proof of that, he said. "Until just last month, program offices did not have any substantive tools to help guide

them through the PBL deployment process," said Banghart. "Today, as a result of inside-the-Beltway actions, they have a professional guide/workshop manual."

Training the workforce on PBLs is "critical," he said. "The performance-based strategy is substantially different from contemporary logistics practices. It is more complex, and it is not intuitive." In addition to classroom training, procurement professionals will need to be involved in actual PBL contract negotiations and executions before they become comfortable, he said.

Contractors that intend to play in the PBL arena also have to make major investments, said Banghart. First they must invest in the personnel resources and time to work with the government to establish a performance based arrangement, he said. The costs to industry to bid on a PBL arrangement are higher than going after a single transactional contract. But over the life of a weapon system, transactional logistics require hundreds and often thousands of contract actions, whereas systems maintained under PBL arrangements will have just a handful. "By itself, the elimination of the bureaucracy associated with legacy transactional logistics contracting make PBLs a desirable option," he said.

Suppliers also have to drive down costs in order to boost profits, said Banghart. Commercial firms do this in two primary ways: improving equipment quality to minimize the number of repairs required and adjusting repair production lines processes to make them more efficient. "And oh, by the way, this is exactly what the government wants industry to do," he added.

A potential obstacle for PBLs is that many government officials do not trust contractors, and are wary of over-privatization. "There's a debate within the Army about contractor logistics support," said Lt. Gen. Raymond Mason, Army deputy chief of staff for logistics. "Where's the right balance?" he asked. "In some cases, our assessment is that we have gone too far contracting out certain skill sets and capabilities." The Army has a huge stake in the logistics market because it owns several major maintenance depots, and it has to worry about keeping them viable, without necessarily competing with the private sector, said Mason. "We want to specialize in certain areas in our depots, not duplicate," he said. "We have to have a cultural change for greater cooperation with industry. The problem is we have commanders who want to keep contractors at arm's length because they are concerned about political and legal issues," he said. "I don't have a perfect solution for that. It's education."

One industry executive who asked to not be quoted by name said he is skeptical about the future of PBLs. While Kendall officially endorses this approach, his influence might not trickle down into the lower tiers of the procurement bureaucracy, where government-industry relations are a bit more tense. "Extended contracts needed to make PBLs work conflict with Pentagon policy for shorter contracts to increase opportunities for competition," the executive said. He said Kendall's strong emphasis on competition is "anathema to PBL, which depends on trust and partnership to work. Without a strong champion in the Pentagon, acquisition professionals have little incentive to take on PBLs." ●

Article reprinted with permission of the author. NDIA 5-7-2014.

ABOUT THE AUTHOR

Sandra Erwin *is the editor of the National Defense Industrial Association's National Defense Magazine, a leading defense industry publication covering defense policy, technology and business trends. Erwin was named editor in January 1999. Prior to becoming editor, she was the magazine's executive editor, and before that, associate editor and editorial coordinator.*

She has extensively covered Department of Defense acquisition policy and programs, defense technology and weapon systems, military logistics, defense industry trends and issues affecting the defense industrial base. She has in-depth experience covering military information technology, tactical communications and defense energy reforms.

Erwin writes frequently about defense procurement issues such as acquisition and contracting reform, and foreign military sales. She is a resident of Arlington, Va., received her Bachelor of Arts degree in Political Science from Coe College, Cedar Rapids, Iowa, and pursued graduate-level studies in Political Science at the University of Maryland, College Park. She also received a publications specialist degree from George Washington University, Washington, D.C.

Lincoln Hallen

A Sharing of Information

"Sharing isn't always the right thing—like when its chicken pox."

On the other hand, sharing data as part of the Government-Industry Data Exchange Program (GIDEP) is an important and meaningful enterprise. GIDEP is a joint service program that enhances the partnership between government and industry seeking to reduce or eliminate expenditures of resources by facilitating the exchange of information.

It looks like data and information are interchangeable. However, you need to distinguish between data and information. If you strictly define *data*, it refers to facts and statistics collected together for reference or analysis. Data is distinct information that is formatted in a special way. The results of the references or analyses can become useful *information*. Hence, if a company decides to submit a maintenance report, data on a counterfeit part, a reliability analysis, or a white paper about most anything, it becomes useful data that others can mine with other data to develop information that may save millions of dollars in time and resources. GIDEP reported that the cumulative utilization savings from all users since 1964 is over $2.2 billion.

GIDEP is used by the US Army, Navy, Air Force, NASA, Defense Logistics Agency, Defense Contract Management Agency, Department of Energy, Canadian Department of National Defence and many industry partners.

"Flowers and pricker bushes grow out of the same dirt."

When GIDEP started in the 1960s it had limited usage and meaning. It was a parts repository that many of us started using to see what problems may exist with some part or piece of equipment. We also looked for reports for possible reliability estimates of similar equipment. Now, with the expanded knowledge of diminishing sources of parts and material shortages, GIDEP has become a key focal point for the housing and subsequent mining of large amounts of data.

"There are a lot of different ways to get to the top of the jungle gym."

There are a number of data types that are in the GIDEP database:

Failure Experience Data provides a means to exchange information about nonconforming and suspect counterfeit items in government and industry systems. These documents (ALERTS, Safe Alerts, Problem Advisories and some Agency Action Notices) inform the participants that a problem situation exists and help prevent usage of problem products.

Product Information Data contains mainly Product Change Notices issued by the semiconductor manufacturers that affect the form, fit, function or the production processes of a product.

Diminishing Manufacturing Sources and Material Shortages (DMSMS) notices originate when a part manufacturer announces that a part or a production line will be discontinued. This information is downloaded, augmented with value-added data, and then stored in GIDEP as Product Information Data. DMSMS also occurs at the module, component, equipment or other system indenture levels and includes microcircuits, brake pads, fasteners, software, valves, filters and more.

Metrology covers a wide range of measurement related subjects. The major emphasis for GIDEP is on calibration procedures and technical manuals. The Army, Navy and Air Force metrology centers are the major contributors of calibration procedures to the GIDEP database.

Engineering Data is a repository of documents and reports generated during the life cycle of parts, components, assemblies or systems from concept and acquisition to operation and disposal. Such data can be on, but not limited to, research development, testing, production, management procurement or any logistic support operation. Members have exchanged information to help avoid costs and additional labor, and even spawn ideas to bring about new methods or techniques for better, leaner business practices.

Reliability/Maintainability Data consist of technical reports on various reliability concepts, practical maintenance operations and engineering tools for making reliability or maintainability decisions. There are a number of Failure Analysis Reports on parts suspected to be counterfeit.

"You can sit around and wait for a ride, or you can start walking."

As a participant or user of GIDEP, you become a part of a growing and important resource for government and industry. Because of users, two key features have developed within GIDEP: Suspect Counterfeit Parts and Obsolescence Management.

Suspect Counterfeit: The counterfeiting of components and assemblies found by government and industry has increased notably during the past decade. GIDEP contains data on equipment, parts, and assemblies that are suspected to be counterfeit. GIDEP members provide formal fact-based reports on items received that after visual inspections and in many cases extensive testing and analysis, are suspected to be counterfeit.

GIDEP can be a key to mitigating this risk by informing members of suspect

counterfeit incidents as well as providing a process for reporting them. Counterfeit parts are not only a problem with the military and related industry, a Consumer Reports news item published November 17, 2014 reported that 'counterfeit' tires pose a consumer risk and that tested Chinese tires underperform and could prove dangerous if the product should prove to be defective.

"Before you trade sandwiches, check between the bread."

Obsolescence Management: Manufacturers are regularly discontinuing production of selected products. GIDEP is the DOD central repository of DMSMS Notices regarding discontinued products. The DMSMS Knowledge Sharing Portal (DKSP), in cooperation with GIDEP and hosted by the Defense Acquisition University, provides a single entry point for DMSMS support by providing access to a full array of centralized informational services working with both government and commercial entities. The DKSP homepage is located at *http://www.dmsms.org.*

The continuing issue of DMSMS has opened the door for counterfeit products to enter the supply chains of the military and their industry partners. By being a member of GIDEP, you are part of a community that is tackling this critical issue. To gain access and become a member of GIDEP, go to *www.gidep.org.*

"Half the fun of pizza is sharing it." ●

N.B., All italic quotes are from Really Important Stuff My Kids Have Taught Me *by Cynthia Copeland Lewis, Workman Publishing, New York, 1994*

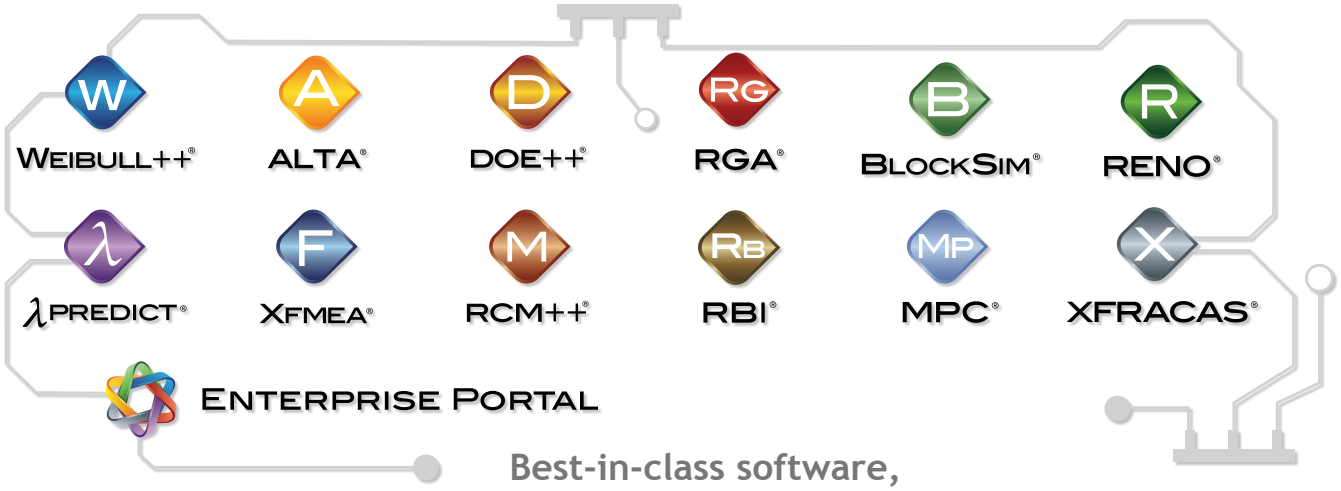
ABOUT THE AUTHOR

Lincoln Hallen *is an independent logistics consultant based in the Washington, D.C. area. Mr. Hallen has more than fifty years of experience in systems engineering, logistics support engineering and computer science. He teaches various courses in logistics for industry and government activities.*

Mr. Hallen is an active member of the Counsel of Logistic Engineer Professionals, a member of The Management of In-Service Reliability, Cost & Effectiveness (MIRCE), a member of the RMS Partnership, a representative to the Government/Industry Data Exchange Program, and a member of the Parts Standardization Management Committee. He is the author of many articles on logistics, space logistics engineering and computer systems. He has published a nationally distributed computer book, has university degrees in mathematics and business administration and technical training in aviation electronics, missile systems, and logistics engineering.

THE SYNTHESIS PLATFORM®

Upgrade to Version 10 today!



Best-in-class software, integrated reliability solutions

The **Synthesis Platform** provides **intelligent integration** between reliability program activities and tools, while simultaneously **facilitating effective cooperation** across engineering teams of any size.

Version 10 offers new features in individual Synthesis applications and significant platform enhancements, such as:

- **Option to implement a Synthesis Enterprise Portal (SEP) website**
- **Integrated Project Planner for reliability milestones and tasks**
- **Easier to Find and Filter analyses, with more graphical Dashboard overviews**
- **Display and track Key Performance Indicators (KPIs)**
- **Automated Watches and Alerts for actions and metrics**

http://Synthesis.ReliaSoft.com/version10.htm

ReliaSoft®

Editorial, from page 1

resiliency, as a sub discipline within the reliability community, has gone unnoticed most likely since neither the technology nor the threat to systems has yet advanced to the point of causing major disruption beyond the parameters of defining reliability.

Exponential advances in software technology and the resulting increased dependency upon it has made communications, record keeping, storage and access to banking, and other related technical functions to commerce and national security, extremely efficient, rapid and interdependent. In the not too distant past, many of these systems were designed and configured as being independent or standalone. An auxiliary backup power source was often provided for critical systems associated with hospitals, transportation infrastructure and military equipment to prevent long-term service disruption.

Advances in software technology, however, has allowed a proliferation of "systems of systems" to occur. While these systems of systems are realizing improved efficiencies, these advancements come with unintended consequences. For instance, a single point of failure can result in widespread outages. Even more disconcerting is the fact that as the complexity of systems of systems architecture increases so does the vulnerability at which a single point or multiple points of failure can occur. In the past, a single piece of equipment or single system failure could be brought back online with one or more auxiliary units. A "systems of systems" network, however, can be so large and complex that one or multiple points of failure can result in devastating loss of network function that cannot be remedied with use of one or more auxiliary units. Recent breaches in cyber security, including breaches within the defense department, banking industry, stock market and human resource computers serve as just a few examples of how vulnerable and dysfunctional "systems of systems" can be and the degree to which critical human activity can be adversely impacted.

The above suggests that in order to achieve the intended mission reliability for "systems of systems," resiliency design must be integral to any "systems of systems" reliability program plan. The importance of incorporating resiliency as part of the life cycle design process grows exponentially with the increase in complexity levels of "systems of systems."

Twenty-first century "systems of systems" or networks that are resilient have the ability of self-diagnosis that provides for a rapid return to functionality at a single point of failure. They also have the ability to adopt corrective actions that protect the entire network from future similar failures from one or more outside intrusions. Resilient systems must, in addition to rebounding rapidly to a failure caused by an outside attack, have protective measures in place for similar points of vulnerability throughout the entire systems of systems configuration. Resiliency confronts the issue of the cyber security component of systems of systems that have become highly dependent on software technology.

Resiliency requirements should be elevated to a higher priority within the reliability program when designing systems of systems. Cyber security specialists who understand the importance of resiliency and its' relationship to achieving mission reliability should be integrated into the reliability, maintainability and supportability (RMS) and logistics total life cycle team.

Continued discussion pertaining to the resiliency for "systems of systems" will occur within future issues of the RMS Partnerships' professional journal (published bi-annually). Interested authors are asked to send their articles to our journal editor Jim Rodenkirch at rodenkirch_llc@msn.com. ●

RMS/LOGISTICS & SYSTEMS ENGINEERING ON-SITE SHORT-COURSE OFFERINGS

Provide Us Your Training Requirements and the RMS Partnership will provide tailored training that will exceed your expectations. For Additional Information contact Russ Vacante at *president@rmspartnership.org*

INTERESTED IN CONTRIBUTING?

If you are interested in sharing your knowledge in future editions, please contact Russ Vacante at:

president@rmspartnership.org

Articles can range from one page to five pages and should be of general interest to our members.