Innovation In Sustainment: Business Processes Represent the Largest Opportunity for Innovation
Mr. Jeff Slayton

A New Data Acquisition Strategy and Operational Plan
Lt Col Christopher Monsey

Logistics Under Attack
Capt Alex Pagano

Leveraging Integrity and Trust: A Call for Values-Based Compliance in U.S. Air Force Aircraft Maintenance
Capt Dave Loska

Persistent Logistics: Posture, Sense and Respond in a World of Great Power Competition
Lt Gen Warren D. Berry

THE EXCEPTIONAL RELEASE
THE AIR FORCE PROFESSIONAL LOGISTICS JOURNAL / ISSUE 149
Table of Contents

4  LOA President’s Letter / Ret Col Scott Fike
8  Persistent Logistics: Posture, Sense and Respond in a World of Great Power Competition / Lt Gen Warren D. Berry
12 Editor’s Letter / Capt Dave Loska
13 Logistics Under Attack / Capt Alex Pagano
20  A New Data Acquisition Strategy and Operational Plan / Lt Col Christopher Monsey
42  Innovation in Sustainment: Business Processes Represent the Largest Opportunity for Innovation / Mr. Jeff Slayton
47  Leveraging Integrity and Trust: A Call for Values-Based Compliance in U.S. Air Force Aircraft Maintenance / Capt Dave Loska

EXECUTIVE BOARD
President
Scott Fike
president@loanational.org
Vice President
Jason Kalin
vp@loanational.org
Chief Financial Officer
Holly Gramkow
cfo@loanational.org
Chief Information Officer
Ryan VanArtsdalen
cio@loanational.org
Chief Operations Officer
Jondavid DuVall
coo@loanational.org
Executive Senior Advisor
Lt. Gen. Warren D. Berry

EXECUTIVE STAFF
Symposium Directors
Kenneth Banton (Chairman)
Dara Hobbs (Co-Director)
Jennifer Fletcher (Co-Director)
Membership Officer
Evin Greensfelder
Rachel Weiler (Assistant)
membership@loanational.org
LOA Historian
Jeffrey Decker
Charitable Program Officer
Tammy McElhaney
AOA Representatives
Zachary Matthews
Casey Klessinger
Chief Learning Officer
Jared “Boyd” Stewart
dlo@loanational.org
Board of Advisors
Judy Fedder, Lt Gen, USAF (Ret)
Kevin Sampels, Col, USAF (Ret)
Art Cameron, Brig Gen, (Ret)
Patricia Knighten
Legal Advisor
William Rogers
Public Affairs Officers
Jacqueline Jastrzebski
Alex Pagano
Civilian Ambassador
Joshua Gee
Van Mizak
Chapter Ambassador
Katie Wallace
Corporate Membership Officer
Tyner Apt-Hill
LOA University Dean
Jerry L. Ottinger II

THE EXCEPTIONAL RELEASE
Chief Editor
Dave Loska
dlo@loanational.org
Assistant Editor
Ms. Mary H. Parker
Managing Editors
Mr. Robert Bosworth
Montanna Ewers
Richard P. Schwing
Andrew Kibellus
Holly Gramkow
Nathan Elking
Lisa McCarthy
Corbin Aldridge
Nicholas Hufnagel
Alexander Barden
Damiqua “Champ” Champion
Director of Publishing,
Graphic Design & Art
Jenny Jones
Greetings Log Nation!

It’s hard to believe approximately four and a half months have passed since concluding yet another awesome National LOA Symposium in Oklahoma City! As I shared on the final day of the Symposium, I am extremely excited, honored, and humbled to be just one small part of a phenomenal National LOA leadership team…and, more broadly, our National LOA Enterprise! I’m looking forward to serving with each of you as we embark on a great 2020 LOA season! I am truly fortunate to join our National Executive Board team of Lt Col Jason Kain (VP), Maj Holly Gramkow (CFO), Capt Ryan VanArtsdalen (CIO), and Mr. JonDavid “JD” DuVall (COO). Together, with our National Board of Advisors and all of the Team National LOA Staff, our aim, as always, will be to serve every one of you and, in the process, strive to ensure you experience all that our great LOA organization has to offer. It is, after all, Y-O-U that makes L-O-A truly A-W-E-S-O-M-E.

Speaking of the October 2019 National LOA Symposium. Wow! From the LOA University to breakout sessions to the main stage and let’s not forget the Air Logistics Complex tours, it was chocked full of awesome and informational presentations. No surprise, right?! Thanks to the National Symposium Leadership Team of Col Gregory Lowe, Maj Holly Gramkow, and Ms. Lynda Lowin, and their amazing group of volunteers. I’d also like to thank our event planning team, EventPower. Lastly, a huge thanks to our Corporate/Industry partners, for without their support, our Symposia would simply put be a challenge to execute. Bottom line, thanks to all who make our annual National Symposia awesome each and every year! And, if you hadn’t heard, our 2020 National Symposium will be held in Salt Lake City (SLC), led by our newly selected 2020 National Symposium Team of Col Kenneth Benton, Lt Col Dana Hobbs and Ms. Jennifer Fletcher. Congrats to Team 2020, and thanks for leading us to SLC!

When we as L-O-A grow, we prosper. When we prosper, we excite. When we excite, we explode. When we contagiously explode, there’s nothing to stop us….we grow….we mentor more, learn more, outreach more, problem-solve more, thought lead more, spark more, innovate more, think more, TESSERACT more…

So, what lies ahead for our Log Nation? Our symposium highlighted the wide-ranging challenges that we are experiencing today, such as worn-out aircraft and archaic IT systems. But, we are countering these issues head-on by strike teaming, thought-leading, sparking, pitching, using apps and websites, sprinting, scrumming—and let’s not forget TESSERACT-ing! I.e., there’s an abundance of ways in which to tap into and persistently and purposefully harness and leverage our collective LOA logistics energies and synergies— together with our industry partners, academic colleagues, sister services, and others. There’s an abundance of ways to get after the challenges. And the Log Nation is all over this!

Speaking of harnessing, we have 80+ LOA chapters that in their own right can be Log Nation spark tanks — or think tanks — or perhaps internationally-dispersed TESSERACT labs. Case in point, we witnessed our inaugural A4-sponsored Think Tank out briefs on stage last year at the 2019 LOA Symposium. With continued Senior Leader and O-6 (or equivalent) Chapter Advisor enthusiasm and support, what a great way to professionally develop our up and coming Log Nation leaders….by innovating – sparking – thinking – TESSERACT-ing, and more. All to say, the theories are proven, the constraints are not insurmountable and are identifiable, and hard-to-achieve results are, of course, possible, knowing that at times “getting there” may be more of an art than a science.

As we usher in 2020, amongst all the sparking, thought-leading and oh….generating a sortie, loading a pallet or munition or weapon, sourcing a part, or acquiring a new system — the list is long — would you Tap someone on the Shoulder and ask if they’d like to get in on this good thing – this thing we call L-O-A! And let’s not forget, “shoulders” come in all sizes, shapes, and forms — active duty shoulders, Civil Service shoulders, Guard and Reserve shoulders, Academia shoulders, and Industry shoulders.

So, why Tap? When we as L-O-A grow, we prosper. When we prosper, we excite. When we excite, we explode. When we contagiously explode, there’s nothing to stop us….we grow….we mentor more, learn more, outreach more, problem-solve more, thought lead more, spark more, innovate more, think more, TESSERACT more….well, the list goes on. So let’s not cheat anybody out of the opportunity to say yes – to say yes to L-O-A, and when we convene in Salt Lake City this year, this phenomenal National LOA organization will be busting at the seams from continued, contagious explosive growth.

In closing, this retired Maintainer/Loggie remains in awe of what you do each and every day. Thank you. I hope your 2019 came to a meaningful close including relaxing, recharging, and enjoying the holiday season. May 2020 be a great year for all! Tap a Shoulder! Let’s Go — Let’s Grow — Let’s Get After It!

Thanks Log Nation!
Scott Fike
President
Logistics Officer Association
2018 - 2019 Year in Review

LOA SYMPOSIUM

Increasing Lethality Today, Readiness for Tomorrow’s Fight.

- 80+ Chapters
- 100+ OPD Events
- 1K+ Attendees
- $9K Scholarships
- 200+ New Members
- 20+ Articles
- 30+ University Sessions
- $8K Chapter Rewards
Persistent Logistics

Posture, Sense and Respond in a World of Great Power Competition

At this pivotal time in history, we are returning our focus to great power competition and are at the forefront of a technological revolution that will change the way we fight and win wars of the future. Last November, I met with senior leaders across the Air Force Logistics Enterprise, the Joint Staff, and key allies to discuss the critical operational problems listed in the National Defense Strategy (NDS) and how to adapt to deter aggression and prepare for future wars. Everything we do must contribute to our nation’s ability to deter a great power actor, and if necessary, inflict sufficient force to repel aggression. To stay relevant in this ruthless environment, we must consistently develop new and innovative ways to deliver our mission. As a result, we’re embarking on a concept of ‘Persistent Logistics’ to handle Logistics Under Attack, an homage to our steadfast commitment to warfighter support despite competition and attrition. This concept is in line with the development of the Joint Concept for Contested Logistics and will enable the force to ‘Move to Win.’ We will utilize Persistent Logistics to guide our approach to new and innovative ways to posture, sense, and respond.

To understand the three attributes of Persistent Logistics, we must first recognize who our competition is and why they are a threat. We are seeing ‘grey zone’ activities that challenge the rules-based international order and enable revisionist powers to operate from advantageous positions.

We are seeing ‘grey zone’ activities that challenge the rules-based international order and enable revisionist powers to operate from advantageous positions.

We are reassessing our posture to address the complexities of the changing global strategic environment and must review our approach to forces, footprint, and agreements. Similar to a commercial airline, we need to optimize our network of global operating locations that enables us to balance risk, investment, and mission generation. This network of operating locations will allow us to move and disperse the force, complicating the enemy’s targeting cycle. Our ability to forward position forces and operate from locations of advantage will be dependent on our relationship with partners and allies, and our operating locations may well still lie within contested areas. Therefore, we’ll need to ensure airbase defense and recovery capabilities are tailored to the operating location requirements. Furthermore, new operational concepts necessitate smaller, lighter footprints on the ground. As we introduce new capabilities, to include those that could be runway agnostic, we will need to examine the implications for logistics. AF/A3 and ACC have been experimenting with force presentation models, which will be refined over the coming year. Once we have determined where we will fight, and how, we can solidify requirements for prepositioned equipment tailored to support new operational concepts. Our new approach to prepositioning will necessitate a re-examination of policy and procurement practices to ensure they support contemporary warfighting requirements. New approaches for positioning, storage, and maintenance should be explored with partners and allies and industry. Greater emphasis needs to be placed on the utilization of operational contract support (OCS), which, when deconflicted with our joint and Allied partners, will support prepositioning and sustainment to reduce the burden on lift and enable a rapid transition to conflict operations. Additionally, we need to exploit technologies that reduce our need to stockpile class III, IV, and IX, reducing their vulnerability to attack and availability for “blue force” use. Finally, great power competition has highlighted a number of concerns across the defense industrial base. Initiatives such as the Sustainment Strategic Framework, Theory of Constraints, depot modernization programs, and SAF/AQ’s Supply Chain Risk Management are making positive progress to addressing these vulnerabilities.

This network of operating locations will allow us to move and disperse the force, complicating the enemy’s targeting cycle.

Sensing allows allied forces to observe the operational environment and orient the logistics enterprise in real-time and near real-time, providing actionable logistics intelligence. We are putting significant effort into digital modernization, leveraging commercial technologies such as secure cloud computing, artificial intelligence, and machine
ABOUT THE AUTHOR

Lt. Gen. Warren D. Berry is Deputy Chief of Staff for Logistics, Engineering and Force Protection, Headquarters U.S. Air Force, Arlington, Virginia. General Berry is responsible to the Chief of Staff for leadership, management and integration of Air Force logistics readiness, aircraft, munitions and missile maintenance, civil engineering and security forces, as well as setting policy and preparing budget estimates that reflect enhancements to productivity, combat readiness and quality of life for Air Force people.

学习。与联合全维域指挥与控制（JADC2）团队合作，我们旨在提供架构、网络和信息，这将使我们能够预测、预测并迅速响应操作要求。这将需要一个高度连接的组织网络，包括盟友和工业，利用自我愈合的网络。未来的冲突将更加依赖于信息，我们的能力以比敌人更快的速度处理和利用这些信息对于作战成功至关重要。我们的飞行员必须越来越熟练地使用、管理和保护我们企业依赖的信息技术。

响应不断变化的破坏性环境将依赖于在受到攻击时移动并生成作战能力的能力。这将需要能够快速灵活地将力量和物资部署到需要的地方。分配将是关键使能器，将依赖于对现有提升资产的最佳利用，以及新科技，如自主和垂直提升。此外，我们将需要新的方法来优化供应品的集装箱化，以增强移动性。

但请让我明确一点。我们正处于开发未来物流概念的早期阶段。还有大量工作要做。最近成立的贷款攻击跨职能团队（LUA CFT），由AF/A4和AF/A5A领导，将进行分析，以识别能力差距并开发解决方案。你们中的一些人将被要求加入CFT，但我鼓励所有人都继续创新并为物流界贡献你们的想法。你们的想法将帮助我们实现‘移动以赢得’。你们在持续发展世界上最强大的空天力量中扮演着极其重要的角色；感谢你们所做的！

Lt. Gen. Warren D. Berry

“响应不断变化的破坏性环境将依赖于在受到攻击时移动并生成作战能力的能力。”
Introduction

A future conflict between the US and our adversaries will be overt and violent. But perhaps more often, our interaction with competitors will include attempts to deter and deny us our strategic objectives by ambiguous and less attributable means while our adversaries aggressively maintain a coercive pursuit of strategic political goals.

No matter the environment, maintaining a responsive connection between the forward edge of the battle area with the supporting industrial base while under attack in a high-end fight will be the Air Force logistician’s greatest challenge. We must collectively begin to address sustainment operations while our advanced adversaries specifically target our logistics operations. However, before we can address it, we must first understand it. This article aims to share my personal journey, which began at I-WEPTAC (Installation-Weapons and Tactics Conference), that took me through the future operating environment, our strategy, and emerging warfighting domains. I hope you find some of our team’s lessons learned valuable in your own preparation.

Logistics Under Attack

By: Capt Alex Pagano

Introduction

A future conflict between the US and our adversaries will be overt and violent. But perhaps more often, our interaction with competitors will include attempts to deter and deny us our strategic objectives by ambiguous and less attributable means while our adversaries aggressively maintain a coercive pursuit of strategic political goals.

No matter the environment, maintaining a responsive connection between the forward edge of the battle area with the supporting industrial base while under attack in a high-end fight will be the Air Force logistician’s greatest challenge. We must collectively begin to address sustainment operations while our advanced adversaries specifically target our logistics operations. However, before we can address it, we must first understand it. This article aims to share my personal journey, which began at I-WEPTAC (Installation-Weapons and Tactics Conference), that took me through the future operating environment, our strategy, and emerging warfighting domains. I hope you find some of our team’s lessons learned valuable in your own preparation.
Understanding that we are under attack now and that this is the environment we must be prepared to operate in. We must ask ourselves if we are ready?

Unlike peacetime military operations and exercises, logistics is under attack now—competitors are attempting to shift the strategic advantage in their favor. Everything is being targeted from the engineering designs of weapons systems, our supply chain and sustainment activities, maintenance equipment, and networks and systems we rely on.

Victory, during armed conflict which may only be a few hours to a few days in duration, will be determined by our ability to move the right assets into the highest priority theatre of operation as rapidly as possible, while shifting our posture from various combatant commands, then moving those assets within the theatre—penetrating the same Anti-access Area Denial (AZAD) environment that our operators will—And we must prepare to do this in a world that is chaotic and unpredictable. In this fight, we will not have the benefit of knowing where significant events will occur, and when they do, we will have a short timeline to get there—and what I have come to realize is that this makes us unique. This is what sets our challenge apart from other private organizations and NGOs.

Logistics Under Attack

We can begin understanding the effects of these attacks by discussing the scenarios through each domain individually. By air, our adversaries will target airports and seaports within weapons engagement zones with an increasingly higher number of advanced ballistic missiles that can travel faster and farther. By land, they will attempt to interdict physical lines of communication to include rail, roads, and bridges using highly trained special operations forces. They will also interdict our sea-lanes of operation to prevent the ability to move the bulk of our assets by ship. In space, they will attempt to interrupt early warning, and position, navigation, and timing to limit our ability to survive and navigate. Finally, in the cyber domain, they will attempt to deny, degrade, and manipulate information to weaken situational awareness, which we rely on to move limited resources among and within theatres of operation.

Understanding that we are under attack now and that this is the environment we must be prepared to operate in. We must ask ourselves if we are ready?

How do we begin to prepare with the significant demands we have now taking up much of our attention and time?

1-WEPTAC hosted by Air Force Installation and Mission Support Center (AFIMSC) provided me an opportunity to be removed from the daily challenges and slow down, research, learn, integrate, and gain an understanding of what our senior leaders were seeing at the strategic level.

I-WEPTAC provides tactical level CGOs the opportunity to immerse themselves in an Air Force problem provided by senior leaders. The lead officer, or Chair, will develop a Mission Area Working Group (MAWG) of cross-functional experts from across the Air Force, Joint, Coalition, and industry partners with the time and funding to travel to conduct in-depth research and analysis. The MAWG Chair out-briefs the Chief of Staff of the Air Force (CSAF) directly to provide their view and recommendations as they see it from the tactical level in order to quickly change Air Force policy.

We spent months traveling to units and organizations across the Air Force and Joint Partners. We either went to your unit or had a chance to talk to your higher headquarters. We had conversations with the Joint and HAF Staff, COCOM and MAJCOM Staffs, and significant integration across warfighting domains with intelligence and cyber operators. At each organization across our mission sets, you told us that you:

• understood the strategic environment,
• articulated your unique challenges and,
• you each described solutions which you were working towards

It turned into a frustratingly repetitive cycle where we would return to our hotel rooms, discuss a new problem we thought existed, develop potential solutions, go to bed ready to discuss those ideas with the people in the unit we were visiting only to be told that “we tried that, we are doing that, or that won’t work because…”

With each organization and each person, it seemed the challenges were being addressed in some capacity. But, a problem still existed; we needed to take a step back and better define how we can contribute. Therefore, we decided to focus in on a mission set that is most common to the LRSs across the Air Force—the distribution process and more simply understand their vulnerabilities across the domains.

The MAWG broke down the distribution process into five key functions (Figure 1). First, the ability to communicate that a requirement for support exists. Then to have the physical inventory of that asset, ability to source the asset, transport it, and deliver it with the verification that it was the right part delivered to the right place. Throughout this process, what may be most important is that all these functions were predicated on having logistics situational awareness, which is currently accomplished through our logistics IT systems. In order words—although our Air Force logistics functions rely on capabilities within each domain, the one domain that has touchpoints across all our core competencies is the cyber domain.

ARMED with this new end-to-end framework, and the recognition that the cyber domain is our linchpin, we decided that we needed to begin to focus on the effects of how a cyber-attack would disrupt our operations and whether we were prepared for it.

We started to learn that not only will a cyber effect have a significant impact to logistics operations, but it is also becoming a preferred method for adversaries to utilize. It’s preferred because it can be:

• exploited prior to armed conflict,
• has a low political cost of employment,
• and creates effects on centers of gravity deep within the enemy’s territory.

We must also acknowledge that our dependence on networked systems and foreign suppliers will continue, and the volume of cyberspace vulnerabilities will only increase. China, Russia, and various other bad actors are taking advantage of that by targeting key terrain in cyberspace and seek to deny, disrupt, or manipulate Air Force core missions to break the seamless connection that I previously described.

We assessed an attack through the cyber domain is the most likely to occur, has a significant impact, and based on conversations we have had around the Air Force over the last year, it is least understood by our logistics community. Therefore, we sought to continue to focus on his domain.

There are already many examples of adversaries using the cyber-domain to deliver outcomes, and we can study the effects cyber-attacks have had in areas like Ukraine being targeted by Russian actors. One of the most notable case studies is a malware attack known as NotPetya.

Figure 1: Five key functions of the distribution process
It is possible a cyber disruption to our network will immediately be followed by a kinetic event. The success of our response will be determined by our ability to withstand the cyber event.

Effects to Logistics Operations

We will not have the convenience of time. It is possible a cyber disruption to our network will immediately be followed by a kinetic event. The success of our response will be determined by our ability to withstand the cyber event. To understand the potential impact, we must first understand what our reliance and vulnerabilities of our IT systems.

To use an example—if I am an Aircraft Maintenance Unit’s OIC at Spangdahlem AB, and I need a DMT for one of my unit’s F-16s. In order to request it, assuming it’s not on base, I’m going to requisition the part. That demand signal is then sent to the 635th Supply Chain Operations Wing at Scott AFB, where they utilize ILB-5 to begin processing the MICAP request. After it is processed and pulled from the shelf of the sourced warehouse, it travels to the port of debarkation where the data is entered into CMOS, GATES, SMS, IGC, or potentially a commercial shipper’s systems, each providing in-transit visibility information. The part then makes it to the port of embarkation, and finally to the point of need. The physical movement of the part is happening while the IT systems are simultaneously being updated to track the asset. In order to move this single part, it took six primary systems to accomplish this request. Moreover, these primary systems are supported by 323 other wholesale and retail systems with hundreds of interfaces between them that drive the entire logistics enterprise—each one a vulnerability.

Our reliance on these systems is revealed through the changes in logistics response times when we begin to operate in a degraded environment. Continuing to use the European theater as an example—under normal day-to-day operations, it takes approximately twenty minutes to issue a part if it currently resides in one of the kits or in the warehouse on base. To transport that part, it takes, on average, 5.4 days to move it from the homeland into the European theater. Now consider data corruption in a supply system—corruption so severe that it shuts down the primary logistics IT systems we use. The issue, sourcing, and delivery time now more than triple when our Airmen begin to utilize degraded operations procedures to process transactions. With even further system degradation, they are relegated to using non-traditional communication means, and the sourcing time triples again.

This scenario begins to describe what is happening at a single location on just Day-One of the fight. Logistics response times in these conditions only compound and worsens as degraded operations continue, and assets are moved from various sources—any semblance of accurate and timely asset visibility is lost.

As we begin towards recovery and the network begins to come back online—we now must begin entering the manually tracked data back into the system. Not only does this take time, but also operations don’t slow down to focus on just this task. Once all previous entries are entered in, the unit begins to return to normal operations with all systems back up and running.

Security experts within the DoD consistently find mission-critical vulnerabilities in each of these systems and in nearly all weapon systems that have been developed or are under development. Do you think we are doing enough to address the cyber risk to the logistics mission properly?

Way Forward

From a strategic perspective, our senior logistics leaders are focusing on establishing a Combined Joint Logistics Enterprise (CJLE) that is better postured for a rapid transition to conflict operations, increasing the ability to sense significant events by creating actional logistics intelligence, and respond the threats below and above the threshold of armed conflict. But, how can leaders at the tactical levels begin to address the risk to logistics missions?

The first step is understanding that we own the risk that warfare across each of the domains has to provide a seamless connection between the forward edge of the battle area with the industrial supporting base. We can no longer view risk from the standpoint of Operational Risk Management (ORM), where risk is only viewed from a safety perspective. If a critical system that mission processes rely on goes down, we are still responsible for continuing to operate. If space assets critical to communication are jammed, the logisticians is still responsible for communicating. We must include resiliency into our processes the same way we have through more traditional warfighting domains, like attacks from the air.

If you suddenly heard an ALARM RED FP CONDELTA—would you instinctively know what to do? I bet most of us would.
ABOUT THE AUTHOR

Capt Alex Pagano is a US Air Force Aircraft Maintenance Officer currently assigned to Kadena AB, Japan, as the 44th AMU OIC. He is a graduate of Advanced Maintenance and Munitions Operations School (AMMOS) and former Logistics Career Broadening (LCBP) Officer. His previous maintenance experience includes providing executive airlift to the POTUS, VPOTUS, and senior government and military officials as well as experience as an F-16 AMU OIC at Shaw AFB, SC, Osan AB, ROK, and deployed to SW Asia.

Our Airmen at all levels know exactly how to react to an air attack and CBRNE scenario. Upon identification that a missile is inbound, our Airmen take protection by taking cover and donning MOPP gear, then detecting damage and additional hazards, restoring operations even through the attack, and recovering from damage after a strike. When a cyber incident propagates through your organization, will your Airmen be able to respond with the same instincts?

From a strategic perspective, our senior logistics leaders are focusing on establishing a Combined Joint Logistics Enterprise (CJLE) that is better postured for a rapid transition to conflict operations, increasing the ability to sense significant events by creating actionable logistics intelligence, and respond the threats below and above the threshold of armed conflict.
A New Data Acquisition Strategy and Operational Plan

By: Lt Col Christopher Monsey

The Air Force can benefit from adopting a data acquisition strategy (ends/means) and operational campaign plan (objectives, tactics, and lines of effort (LOE). Tactics include targeting threats/opportunities, prevention of avoidable sole-source contracts due to unjustifiable failure to order developmental task data outputs or use of performance-based contracting approaches, bypassing/flanking intellectual property (IP) obstacles, overcoming improper data rights assertions via improved inspection and challenge capabilities, and drafting contracts with “legal value.” Contracts with legal value provide a breach of contract remedies such as reimbursement of costs to reverse engineer parts or a technical data/software escrow release when a supplier breaches contract obligations. Contracts can be drafted with a cost, schedule, or performance obligation, specified risk or breach event, and breach remedy.

Often the primary problem the Air Force faces is not a lack of data rights but rather failures in data requirements/ordering, leverage, or pricing or a mismatch of negotiation approach (position based versus interest-based). Programs lack tactics on how to recognize, create, and use leverage to get good deals. A lack of leverage often leads to no-bid responses, and prices for data that are not fair and reasonable are far in excess of reverse engineering/qualification costs. Product support managers and program managers also lack an intellectual capital (IC), technical data, and data rights opportunity and threat precision targeting capability that aids in ensuring a return on investment (ROI) and drives life cycle decisions based on source of developmental funding (SDF) information at a part or subprocess level. Program life cycle sustainment plans (LSCP) that require high leverage to induce a contractor to deliver needed technical data or software in low leverage, post down select phase, or condition are doomed to failure and high conflict. IP strategies, product support plans, LSCPs, leverage/negotiation strategy, and acquisition plans must be synchronized to avoid a mismatch between leverage needed versus actual leverage available to obtain needed technical data or software development documentation.

A new data acquisition strategy and operational plan can significantly improve the Air Force’s institutional capacity to achieve affordable, sustainable, agile, effective, and legally enforceable outcomes.

The Air Force also needs improved data requirements capabilities. Data enables tasks and decisions. Thus, to understand data needs, programs and sustainment commands must understand the current and future tasks and decisions that require or produce useful data. Programs must operate with critical insights, such as how data is produced from developmental tasks. When the Air Force pays for development, it pays for some or all of the cost of producing the data and gets “unvested” data rights under standard data rights clauses. Ordering vests these rights. Thus, programs should align their data ordering, life cycle, competitive versus non-competitive, depot source of repair, repair, replace, and industrial source of repair decisions based on a SDF analysis. Policy can lead to timing problems with ordering and delivery. For example, policies that direct programs not to order delivery until reaching a stable baseline lead to failure to obtain data/software necessary to support depot and supply chain analysis/strategy and activation.

Data Ordering Strategy for Developmental Contracts vs. Non-Developmental Contracts

Where a contract funds developmental work, the Air Force should at least purchase a copy of Government-funded developmental task data outputs. The required deliverables should be in a format allowing reuse by organic depot or future secondary sources selected in full competitive contracts. Reuse and enabling of competitive follow-on secondary sources can be accomplished by adding task data outputs to program or system engineering documentation typically ordered in a development contract. For example, a contractor can be required to deliver a modified integrated master plan (IMP), system engineering plan (SEP), or work breakdown structure (WBS) with an added column of “data produced from task.” The contract can order such Government-funded task data outputs that can be ordered using a “not separately priced” (NSP) contract line item numbers (CLIN) (since the Government is paying for the developmental task) or creates the data output in a development CLIN. Where pre-existing data is used in the development task, costs of licensing such data can be added to the development task, which produces the NSP ordered data. The contract can include a contract data requirements list (CDRL) and a generic one-time data item description (DID) requiring delivery of the modified documentation. This CLIN/CDRL/DID combination can require periodic delivery of data listed in the data produced from the task column, e.g., not later than the end of the month following completion of the task that produced such data. When the Air Force pays for development, it should at least get what it paid for. Technical data and software funded at least partially at Government expense and aligned with the developmental tasks that produced it should not be left on the table due to a failure to include clear, binding delivery requirements.

Data Ordering Strategies for Non-Developmental Items

Programs should generally avoid ordering detailed manufacturing data for items developed exclusively at private expense. However, in such cases, the Government should order American Society for Mechanical Engineers (ASME) Standard Y14.24 “control drawings” as such documents are entirely or substantially form, fit, and function (FFFF) data. The Government receives unlimited rights to FFF data under the Federal Acquisition Regulation (FAR) 11.104. The Hirel Connectors case provides a detailed explanation of FFFF data in the context of electronics parts. By ordering application programming interfaces (APIs) and open system/modular system/object-oriented programming compliant deliverables, the Government can ensure Government-funded modules are separated and interfaced with modules developed exclusively at private expense. This ordering approach avoids delivery of technical data or source code that cannot be reused in any way due to portion markings of source code or technical data within a lowest portion or grouping of usable functionality. The Government’s use of technical data associated with these Government-funded deliverables would not be restricted as it
would be with functions or modules developed exclusively at contractor expense. Portion marking of technical data or software source code within vs. between the lowest unit of function can take the form of portion marking of a software subroutine. In this case, when the portion marked sections are removed from the subroutine, the resulting subroutine will not function for any purpose. This should be found to be an improper portion marking under the DFARS 227 rules that require a source of funding determination that drives Government data rights be done at the lowest practicable level given the portion marked subroutine cannot be re-used for any purpose thus that is not “practicable." Similarly, portion marking within a part versus between parts is not practicable given redacting portions of an indivisible part result in drawings that cannot be used for any significantly useful purpose. Contract interpretation rules or case law can be used to argue that contractor interpretation of the term “practicable” cannot be interpreted to thwart the commercial purpose behind ordering technical data in the first place: re-use.

Programs should generally avoid ordering detailed manufacturing data for items developed exclusively at private expense.

Reducing Rework in Follow-On Competitive Re-Procurement Contracts

Rework is a major barrier to full and open competition. Consequently, one primary objective of a data acquisition effort should be to reduce rework required by future secondary sources to recreate data. A flawed or non-existent data acquisition strategy, for example, one that does not order data that results from Government-funded developmental tasks or is not aligned with system engineering task frameworks, substantially increases the risk of follow on sole-source contracts. Major benefits flow from aligning data ordering with future secondary development and qualification tasks to reduce rework. One approach can include creating a current development task/data output list, then correlating that list with potential future secondary source development or reverse-engineering qualification re-work task/data output lists as an aid data requirements analysis for current contracts.

The Connection Between Government Funding of Developmental Tasks, Data Rights, and Ordering

When the Air Force pays for development (absent specifically negotiated rights or for commercial software), the Air Force gets automatic “unvested” data rights (unlimited, Government purpose (GPR), or limited/restricted) when the contract includes the mandatory DFARS 252.227 data rights clauses. However, the DFARS clauses do not include any ordering provisions. Instead, the Government must order data separately for a given part developed partially or exclusively at Government expense to “attach” or “vest” these “unvested” data rights to data that pertains to that part.

The Air Force Needs Improved Leverage Strategies

Buyers or investors only get good deals with leverage. Programs must develop an effective leverage strategy with data requests or ordering approaches that are compatible with current leverage conditions. Low leverage conditions exist AFTER down-select to one vendor from a competitive contract AND if an effective data ordering strategy was not used.

Data acquisition leverage strategies start with understanding when a program is in a high leverage condition versus a low leverage condition.

High leverage conditions are prior to down-select to a single vendor. Low leverage conditions are after a significant amount of sunk costs have been expended, and there would be substantial costs to terminating the current contractor and switching to a new vendor and paying for reverse engineering or re-development of the system with such sunk costs. Leverage in high leverage conditions takes the form of large amounts of development funding and the potentially much larger amount of sustainment dollars post-production plus upgrades and life cycle extension. Low leverage conditions are whatever point where the sunk costs are so great, and the time needed to switch vendors becomes significant to a buyer. How, when, and what data is ordered will increase the potential for no-bids or outrageous prices. When a program has high leverage, it can get more data and lower cost than the vendor would provide in a low leverage condition.
The Government can pursue alternatives to a no-bid or an outrageous price to a data request such as low leverage optimized supply chain, depot task, and data acquisition life cycle sustainment plan strategies.

Another useful leverage or influence strategy uses interest-based negotiation and conflict resolution principles. For example, programs should be alert to vendors demanding deals they would not agree to if they were in the Air Force’s position. In such cases, a negotiator can employ an appeal to shared values or interests, highlighting that what is bad for them is likewise bad for the Air Force (appeal to shared values and fair dealing norms). One example -- contractors frequently complain that Government deals deprive them of ROI. Negotiators likewise should identify and resist deals where a contractor is insisting on terms that deny the Government a fair return. When the contractor is an investor (e.g., paying all development costs for a part), then the Air Force should not demand a full manufacturing technical data package with unlimited rights. Likewise, when a part is developed exclusively at Government expense, then the contractor should not deprive the Air Force of its ROI by refusing manufacturing data orders with unlimited rights on such parts. Programs should call out companies who seek to deprive the DoD of its ROI while simultaneously complaining about DoD seeking their “crown jewels” IP funded exclusively at private expense. The Government should not allow these contractors to have their cake and eat it too.

A major reason for data acquisition failure is Air Force records retention rules that result in the destruction of contracts with critical information -- ordered developmental tasks, tech data, or software – a specified number of years after contract closeout.

Low Leverage Optimized Supply Chain, Depot Task, and Data Acquisition Life Cycle Sustainment Plan Strategies

The Government can pursue alternatives to a no-bid or an outrageous price to a data request such as low leverage optimized supply chain, depot task, and data acquisition life cycle sustainment plan strategies. For example, a program can analyze relevant parts, components, or depot tasks to identify those with affordability, sustainability, reliability, maintainability, or availability shortfalls. The program can then develop an interest-based proposal to a vendor designed to target “easier to get to yes” parts or data orders (ZOPA deals). Such part or task selection can be based on a ZOPA selection criteria. Programs should also avoid selecting parts, tasks, and data orders based on ZOPD avoidance criteria (e.g., a vendor has a bad relationship with their subcontractor, thus high friction conditions to getting the supplier to agree to anything).

Programs must also understand how to create leverage (BATNAs or alternatives to bad relative value deals) during typical sustainment low leverage level conditions. For example, a program can identify bad relative value parts or depot support using DoD Standardization Document (SD)-24, Value Management (value engineering). Next, a program can ask for better value, offer to help with fixing root causes of a value shortfall in exchange for consideration (e.g., data), offer to buy a data package for the cost of reverse-engineering the part, or executing a reverse engineering effort to create a substitute data package and then terminating the sole-source contract. Having an alternative to a bad deal creates leverage to get better deals not only on a current part but for all parts.

Decisions and Action that Increase or Reduce Data Acquisition Risks

How and when the Government orders data increases or decreases the probability of a no-bid or an outrageous price response to Government requests for data. Ordering strategies should take into account likely reasons a vendor would reasonably or even unreasonably refuse to agree to a data order versus the conditions where they would more likely agree. (ZOPA vs ZOPD data requests)

Data acquisition actions that reduce cost: Align life cycle/product support decisions with data available data.
A data escrow agent or breach of contract remedy that triggers the delivery of technical data or software can be based on a variety of delivery trigger events.

Self-Sabotage by Programs

A major reason for data acquisition failure is Air Force records retention rules that result in the destruction of contracts with critical information — ordered developmental tasks, tech data, or software — a specified number of years after contract closeout. Destroying these contracts, which contain active data rights licenses and provide support for the Government’s enforcement of its rights, deprives programs of needed evidence to show ordering and funding of development costs. This destruction undermines the program’s ability to fight unjustified restrictions on the Air Force’s use of technical data and computer software. It also destroys evidence required for successful breach of contract claims against a vendor that is improperly marking data on data uploaded to a data repository. This violation of DFARS data rights clauses that prescribe particular markings on technical data delivered to the Government. Such nonconforming markings are a major red flag, but the contractor’s mismarking of documents does not impact the Government’s rights.

An effective data acquisition framework should also use key questions to identify disconnects between LCSP, acquisition strategy, and IP strategy.

A program seeking to understand what is rights to a given item of technical data or software must locate a copy of the contract that ordered the data in question to determine whether or not the contractor improperly included a non-conforming marking on data uploaded to a data repository. Since data with nonconforming marking should not be delivered, it follows that data with non-conforming marking data should not be uploaded to data repositories.

Programs can also create leverage on other contracts by including past performance factors addressing sustainment as evaluation factors in source selections to impose consequences for abusive sustainment practices, e.g., placing the abusive contractor at a competitive disadvantage when seeking future contracts.

Per standard data rights clauses, a contractor has no obligation to mark unordered data since the contractor such data is not a contract deliverable. However, where data was ordered (and potentially other contracts that funded the development of the item, component, or process described in the ordered data) are unavailable, then the Government lacks an ability to know if a contractor improperly marked such data per the DFARS 252.227 data rights clauses. In this case, it is unclear whether the Government has unlimited rights, Government rights clauses. In this case, it is unclear whether the Government has unlimited rights, Government purpose rights data or software can be based on a

rights framework/source of developmental funding (particularly for detailed manufacturing and process data (DMPD). Ordering a COPY of data outputs of Government-funded developmental tasks (not separately priced) reduces cost given the cost of data is generally the cost of the development task that produced the data. Another cost reduction approach arises from accepting performance-based contracting (statement of sustainment objectives (SOSO) to data provisioning plan) and use of source selection factors in competitive contracts tied to refusal to agree to ZOPA or reasonable data orders. Data Acquisition actions that unjustifiably increase cost. Use of recurring use or “standard” DIDs that are not aligned with developmental task outputs, particularly for Government funded developmental tasks, can increase cost by ordering data that isn’t needed by a follow-on source or is not aligned with current engineering practices (these DIDs are very old). Many recurring use or standard DIDs read more like statements of objectives versus definite data orders aligned with current engineering development task outputs or design automation tools. Data orders that are ambiguous, vague, or contain omissions and/or errors (the mortal enemies of contract formation) also increase cost given such data orders are not legally enforceable (no contract formation). Defective specifications or data orders invite lawsuits, disputes, delay, and often lead to sole source awards. Timing of orders during high or low leverage periods will increase or decrease costs or odds of a no-bid response as well. A timing failure enables a contractor to demand high prices to LATER ORDERED data. Use of the deferred ordering or delivery clauses without specifying how to price the data in question (should at least specify pricing for unlimited or Government purpose rights data) increases cost given there is no agreement on pricing during a competitive or high leverage condition. Use of the data accessions list (DAL) without a pricing formula also increases cost and invites outrageous pricing (e.g., in excess of reverse engineering/qualification costs). Contracts, or legally enforceable obligations (cost, schedule, performance), were originally created to enable predictability and remedies. When contracts do not create predictable outcomes or enable judicial remedies (damages), they lack legal value. Thus, contracts should prevent a contractor from having the ability to charge for the tasks that produced the data plus a separate cost for such Government-funded task data outputs (“double plus charging”) to ensure predictable outcomes of return on investment and cost control.

A large amount of technical data or software development documentation has been uploaded to various data repositories. Data ordered on a FAR-based contract that describes a part developed exclusively at Government expense must be delivered without restrictive rights markings (other than an appropriate copyright marking) per standard DFARS 252.227 data rights clauses. However, a significant amount of data in these Government data repositories has restrictive rights markings. For example, such documents frequently include proprietary markings (e.g., “Company X Proprietary”). Proprietary simply means a legally enforceable right to stop others from unauthorized uses; consequently, even technical data subject to unlimited rights can qualify as “proprietary information.” Proprietary and other such markings are non-conforming markings per the DFARS 252.227 data rights clauses that prescribe particular markings on technical data delivered to the Government. Such nonconforming markings are a major red flag, but the contractor’s mismarking of documents does not impact the Government’s rights.

An uncertain rights data in possession of the Government

A major reason for data acquisition failure is Air Force records retention rules that result in the destruction of contracts with critical information — ordered developmental tasks, tech data, or software — a specified number of years after contract closeout. Destroying these contracts, which contain active data rights licenses and provide support for the Government’s enforcement of its rights, deprives programs of needed evidence to show ordering and funding of development costs. This destruction undermines the program’s ability to fight unjustified restrictions on the Air Force’s use of technical data and computer software. It also destroys evidence required for successful breach of contract claims against a vendor that is improperly marking data on data uploaded to a data repository. This violation of DFARS data rights clauses that prescribe particular markings on technical data delivered to the Government. Such nonconforming markings are a major red flag, but the contractor’s mismarking of documents does not impact the Government’s rights.

A data escrow agent or breach of contract remedy that triggers the delivery of technical data or software can be based on a variety of delivery trigger events.

Self-Sabotage by Programs

A major reason for data acquisition failure is Air Force records retention rules that result in the destruction of contracts with critical information — ordered developmental tasks, tech data, or software — a specified number of years after contract closeout. Destroying these contracts, which contain active data rights licenses and provide support for the Government’s enforcement of its rights, deprives programs of needed evidence to show ordering and funding of development costs. This destruction undermines the program’s ability to fight unjustified restrictions on the Air Force’s use of technical data and computer software. It also destroys evidence required for successful breach of contract claims against a vendor that is improperly marking data on data uploaded to a data repository. This violation of DFARS data rights clauses that prescribe particular markings on technical data delivered to the Government. Such nonconforming markings are a major red flag, but the contractor’s mismarking of documents does not impact the Government’s rights.
One solution can include a litigation risk driven approach where the Government reviews the documents with the non-conforming markings to determine if there are “indicia of ordering.” Where there are such indicia (e.g., a contact number is on the face of the document – normally only done per a CDRL requirement on a FAR-based contract), then the program can analyze the risk presented by assuming the data was ordered. The data rights clauses specifically dictate the language to be used to identify data delivered with less than unlimited rights – i.e., data subject to GPR, limited rights, or specifically negotiated rights. Non-conforming markings on such ordered data are a violation of the standard data rights clauses. If within a challenge period, the Government can bring a data rights challenge and force redelivery. Outside the challenge period, the Government cannot force redelivery but can find evidence that the contractor breached its contract and delivered mismarked data. Where there are indicia of ordering, and there are non-conforming markings, the Government can argue it has at least a good faith belief that the Government has enhanced rights. If the data turns out to be unordered, then the contractor can bring a claim under 28 U.S.C. 1498 for copyright infringement. The legal office can assist in computing potential damages for a compulsory license under 28 U.S.C. 1498 in order to evaluate whether the potential liability for copyright infringement is less than the cost of an exorbitant license cost, but it should not exceed the costs of calculating potential damages for a compulsory license under 28 U.S.C. 1498 in order to estimate based on the cost to recreate the data and qualify reverse engineering and qualifying the previously developed data. Contractors should not expect to get a return on someone else’s investment that is known by persons of average skill in the art of a given part or system.

### Improved Pricing Approaches for Technical Data and Software

**Data acquisition failure response should start with the creation of data acquisition strategies optimized for low leverage conditions.**

If the data with non-conforming markings was in fact not ordered, then assuming the data is not marked with a clear trade secret notice, the Government could argue it has a good faith basis to use the non-conforming marked data with indicia of ordering. If the Government’s good faith belief that it ordered the data turns out to be incorrect, then the Government is using data that may only have copyright protection (vs trade secret protection). In that case, the contractor’s sole remedy is a claim under 28 U.S.C. § 1498. This statute does not provide injunctive relief; therefore the Government will only have to pay a compulsory license fee. It should be noted that DoD policy is that the Government will respect private party intellectual property rights. Thus, such a decision to use uncertain rights data with indicia of ordering in ways that a contractor might object, even with a good faith belief that the Government has enhanced data rights to, is a policy significant decision that should be coordinated up through at least Air Force litigation support offices. Such use should be limited to cases where a contractor is objectively failing to provide needed support (e.g., has ended support, refusing to support, providing poor quality parts, or is very late in responding to requests for sustainment support and it is directly and seriously affecting combat readiness).

### Non-traditional acquisition approaches can provide additional leverage creating strategies.

On reasonable pricing approach for technical data or software is to value the data or software based on the cost to recreate the data and qualify a part produced with such data. For example, the Government can create a fair and reasonable price estimate based on the cost to create or recreate the technical data or software (e.g., reverse engineering costs). Where there are prior developmental costs, a contractor may legitimately add an additional license cost, but it should not exceed the costs of reverse engineering and qualifying the previously developed data. In addition, it may be appropriate to apply a discounting factor where the design in the previously developed item or design element is what is known as “prior art” or an obvious variation of prior art. Prior art is a term used in patent law to describe design information that has been published or is known by others. The Government automatically receives unlimited rights under data rights clauses to such data, if ordered, as it is publicly available; therefore the Government should not be forced to pay for prior art, i.e., “engineering cookbook” or public domain knowledge, for which the contractor has not paid developmental costs. Contractors should not expect to get a return on someone else’s investment that is known by persons of average skill in the art of a given part or system.

### Data Acquisition Operational Campaign Plan

Strategies provide ends and means. Plans are how the means will be achieved to the ends. A leadership vision provides a compelling future state that motivates people to achieve the vision’s future state. Generally, a new data acquisition strategy and plan should provide two basic capabilities: deliberate planning to prevent avoidable follow-on sole-source contracts, particularly on items developed exclusively or substantially at Government expense, and a data acquisition failure response capability. Prevention entails a strategy and plan for data acquisition that seeks to avoid errors that lead programs into unnecessary follow-on sole-source contracts. A response plan provides options to prevent or deter no-bid or the proposal of outrageous prices in response to data requests during a sustainment phase.

A data acquisition strategy’s ends should comprise affordable, sustainable/high readiness, agile, effective, legally enforceable outcomes. Each of these ends can be measured using measures of performance (MoPs) and measures of effectiveness (MOEs). MOPs track whether a plan was followed (a leader cannot judge a plan that was not followed) while MOEs evaluate the plan’s effectiveness.

A data acquisition strategy should include revised job descriptions, tasks, and technical knowledge requirements for key positions to enable the Air Force to meet evolving requirements and support current efforts such as the implementation of the Digital Enterprise. Data acquisition planning teams must understand current and future contractor system engineering/developmental tasks or workflows, electronic design automation (EDA) tools used for developmental and production work, and data outputs and inputs from such
Operational design’s initial focus is on helping a leader to visualize the operational or business/market environment, understand the problem that must be solved, and develop a broad operational approach that can create the desired end state.

Contracts can also include pre-paid delivery requirements that are triggered at any point after contract award or within a specified time period, such as up to ten years to ensure the Government has reasonably priced data transfer obligations inserted into contracts. A contract can also include pricing provisions for deferred delivery or ordering that are aligned to SDF categories and include pricing provisions for deferred delivery or ordering that are aligned to SDF categories. Such a map enables identification of items were developed exclusively or partially at Government expense. One major failure point in deferred ordering is a lack of agreement on pricing during a deferred ordering period.

A data escrow agent or breach of contract remedy that triggers the delivery of technical data or software can be based on a variety of delivery trigger events. Example triggers can include cases such as inability or refusal to sell parts to the Government that meet contract specifications or discontinuance of a sole source or limited source part particularly for a system with onerous qualification requirements and large impacts on warfighting capabilities. A release of data trigger can also be based on a value engineering analysis that shows a vendor is failing to deliver best relative value, fails to meet a specified demand satisfaction rate or responsiveness, declares bankruptcy, or delivers defective parts more than a specified number of times over a prescribed time period.

Contractors can refuse to agree to a contract obligation for delivery of technical data from escrow or as a breach either initially or during contract administration. These agreements can be difficult to negotiate and are difficult to enforce unless the trigger conditions are clear and unambiguous. Program offices can influence contractors to agree to such obligations with sufficient leverage or influence. Other ways to reduce the probability of a refusal or disputes in negotiating or enforcing such trigger event-based data transfers can include drafting delivery trigger conditions in line with commercial practices, agree to a reduced licensing fee, or make them more objectively reasonable. Negotiation strategies can also include incentive or carrot bargaining positions to induce or influence vendors to agree to a given delivery trigger condition. For example, a program can frame a data delivery trigger agreement as a mitigation measure that can be reflected as a positive mitigation measure comment in past performance reviews in case of a breach of contract such as for defective parts that do not meet specifications or reliability contract obligations.

An automatic deferred delivery order can be included to deliver technical data when a contractor ends support for a part or no later than a specified time period, e.g., ten years after delivery of a part.

A licensing fee can be included for a per part basis, but it should be in line with commercial profit margin standards (e.g., no more than ten percent of the part cost). A time period for a delivery trigger can be appropriate to meet the Government’s requirement while providing the contractor with a fair ROI or capital return and profit margin. Also, the DoD can highlight to vendors that it is better for the Government to retain data for rarely ordered parts or parts for major weapon systems which have unplanned extensions of service life. For example, the Minuteman III missile has been extended far beyond its expected service life, leading to unexpected data needs for parts that were never expected to require replacement. In such cases, a contractor expends funds to retain data that may or may not be needed in the future. The Government, with its superior knowledge on likely service life and possible extensions, should assume data retention responsibilities and help vendors save funds that could be better devoted to productive uses such as new product development.

This new strategy and plan will avoid ordering blunders and help programs develop effective leverage and negotiation strategies to deter no-bids and contractors proposing unreasonable prices in response to reasonable requests for technical data and software.

Means also can include training on the use of conflict resolution/interest-based negotiations (as contrasted to leverage hungry position based frameworks), negotiation concepts and skilllets needed to create a well-crafted offer. This means includes an ability to create business proposals that fall within a ZOPA, have effective BATNAs (alternatives to bad relative value deals which provide leverage), do not fall into ZOPDs, are based on an understanding what are deal or value killers for the Air Force (and industry), and an ability to create interest-based versus position-based relationships. Position based negotiation frameworks are ones where the party with the greater leverage (in government contracts, all too often the contractor) dictates terms (often bad ones) to the party with the weaker leverage (often the Government). The weaker party suffers as a result of this zero sum big winner and big loser bargaining relationship. Increased use of interest-based negotiation principles obviates a need for leverage and also increases the reducing leverage requirements.

Needed means also include creating improved knowledge or decision support tools. For example, creating a data rights and tech data/software opportunity and threat precision targeting map is critical for every program. Such a map identifies parts based on a SDF class tied to data rights categories. Such a map enables identification of items developed with Government funding vs. non-investment items.

This SDF map can facilitate identifying which items were developed exclusively or partially at Government expense. This targeting map should drive data ordering and decisions on major life cycle sustainment plan (LSCP), depot source of repair (DSOR), industrial source of repair (ISOR), competitive vs. non-competitive acquisition, repair versus replace, etc. A SDF coded threat and opportunity targeting map can help give needed insight to enable life cycle decisions through an art-of-the-possible (AOP) driven approach. Parts can be color-coded based on a SDF category aligned with categories of data rights. For example, green and yellow parts are associated with parts developed exclusively or partially at Government expense (which correlate to unlimited or Government purpose rights (GPR) for data describing such green or yellow parts). The program should select such green and yellow color-coded parts for DSOR, competitive follow-on buys, and maximum data.
orders given the Government’s higher level of rights in the underlying data. The program should likewise select red parts for ISOR, and sole source buys - unless a value engineering analysis shows they are a bad relative value. Where red parts are determined to be bad relative value, then they can be targeted for reverse engineering to create a replacement data package. Programs can order unlimited rights FFF data packages (e.g., ASME STD Y14.24 control drawings) for red color-coded parts to enable FAR 11.104 name brand or equal follow on buys as well. For software, a contract can prohibit customization of software (changing its function) and require new or significantly different functions be added as additional subroutines or modules with an application programming interface (API) or open system architecture interface at critical abstraction layers between restricted rights and modified or new software functions.

Additional means should include the development of improved tech data ordering doctrine and creation of standard operating procedures (SOP) that include ordering strategies that encourage ordering Government-funded developmental items vs. privately funded non-developmental items to align with the data rights framework. A data ordering strategy should also be aligning ordering with system engineering tasks that generate data and consume data with a goal to reduce a need for rework by follow on secondary sources to re-create OEM developmental task data developed at least partially at Government expense.

An effective data acquisition framework should also use key questions to identify disconnects between LCSP, acquisition strategy, and IP strategy. For example, a program LCSP that calls for all parts to be competitively re-procured and organically maintained by an Air Force depot where there is no IP strategy to order such data or without regard to SDF has a major disconnect between required tech data and data rights versus actual technical data and data rights. In another example, a LCSP that calls for a non-commercial sustainment strategy for a commercial item has an obvious disconnect between data acquisition strategy versus the LCSP. Another disconnect can be identified when a program buys commercial items without conducting the required market research to learn how the civil buyers sustain such parts or what technical data is normally acquired by non-Governmental customers.

Programs should also employ improved coordination or acquisition crew resource management (ACRM). A data acquisition planner should synchronize data calls between program managers and entities requiring technical data software to enable life cycle tasks. Air Force leaders also should institute procedures to oversee design agent decisions at the macro level to deter results that may be good for the contractor and in the short term for the individual program but devastating to Air Force and warfighter institutional needs such as long term affordability and sustainability. Such insight over program decisions that are detrimental at the Air Force or major command (MAJCOM) affordability and sustainability needs. New commander’s information requirements (CCIR) can be required to enable veto action or intervention by institutional leadership where it is necessary to avoid short term focused versus life cycle focused outcomes.

Needed new means also include ensuring contracts are drafted with “legal value.” A contract that does not provide a remedy for a given set of predictable cost, schedule, or performance failures isn’t a contract – it is a grant instrument. Contracts were created to create predictability and to allocate cost, schedule, or performance/value risks. Effective contracting enables breach remedies.

A legally enforceable contract is an enforceable agreement between the parties which is as definite as reasonably possible as to cost, schedule, and performance and, most importantly, enables a judge to compute monetary damages in the event of a party’s failure to meet its performance obligations or fail to effectively manage risks that the performing party should reasonably assume for various deal killer or failure scenarios.

Contracts with legal value provide cost control and provide disincentives for contractors overpromising and underperforming. Contractors must be held accountable for failures to deliver solutions or capabilities that are promised in legally enforceable agreements — all good things in the military start with accountability. A legally sufficient and unchallenged source selection that creates a legally unenforceable contract is not a success. Programs should avoid haphazard acquisition strategies primarily directed to bid protest avoidance or schedule risk at the cost of getting a good deal for the Government or meeting life cycle needs comprising a majority of total cost of ownership.

Programs that attempt to control costs on the front end via fixed price contracts or cost overrun cost shares without ensuring effective cost control during sustainment, particularly for items developed exclusively or substantially at Government expense, merely invite the contractor to shift procurement costs into the operations and maintenance (O&M) bill that should have been funded via procurement dollars.

A failure to create legally enforceable contracts risks creating a survival of the sickest or failure-prone industrial base without accountability for performance failure. The Government must realize that successful capitalism, in large part, is based on competitive pressure, sometimes leading to creative destruction (e.g., bankruptcy and transfer of assets from a zombie company to a phoenix company). Accountability ensures that mistakes or failure lead to companies changing directions efficiently versus replicating failure — doing it the same way and producing the same poor results.

Campaign Plan Overview

The proposed data acquisition campaign plan includes five objectives, four tactics, and nine lines of effort. Tactics generally fall into prevent, sustainment crisis response, blow-away, and enable breach of contract remedies. Prevention includes using the threat and opportunity map to align life cycle decisions with the SDF based data rights categories, which helps prevent avoidable bad deals (e.g., avoidable sole source follow on contracts).

Objectives

An overarching life cycle objective comprises enabling acquisition of affordable, sustainable, agile, and effective military systems with reasonable RoI for both Government and industry. This can be accomplished through legally enforceable acquisition outcomes that include both cost controls and executable remedies. Campaign Objective 1 includes Improving Air Force capabilities to enable acquisition of items developed partially or exclusively at Government through competitive to follow on parts buys from aftermarket part suppliers while also enabling organic depot maintenance on such items. Campaign Objective 2 includes maximizing Government developmental investment through reuse of resulting technical data and software task outputs. Campaign Objective 3 seeks to increase the enablement of life cycle tasks and reduce rework by future potential secondary sources. Campaign Objective 4 seeks to leverage aligned data acquisition strategies to get better deals through creating additional options. Campaign Objective 5 seeks to reduce technical data, software development, and logistics product data ordering failures or gaps.

Tactics

A first tactic focuses on the prevention of avoidable sole-source contracts. A first step in this tactic comprises the creation of the SDF coded part breakdown structure based map. The map is then used to facilitate improved ordering of technical data, software, and logistics product data. This improved ordering is comprised of at least four ordering approaches (two new and two traditional). A minimum order would be a copy of developmental task data outputs using, for example, a modified IMP with a NSP CLIN. A delivery requirement of not later than one month following completion of the related developmental task would ensure timely, useful deliverables. Ensuring inclusion of standard data rights clauses would provide appropriate rights to the Government (at a minimum Government purpose rights since the development task was completed using Government funding). This level of rights, with the deliverable in hand, would require competitive delivery requirements, would allow the Government to compete future acquisition of related parts or services — avoiding an unnecessary sole-source contract.

A second data ordering approach employs performance-based contracting — including use of statement of sustainment objectives (SOSOs) — to execute a data provisioning plan that enables
The contractor then leverages the DFARS data rights and objectives (adapting a MIL-HDBK-245D statement of objectives (SOW) to statement of work (SOW) approach). A modified data accessions list (DAL) DID can be included in the contract with a SOW or CDRL tailoring section listed generic task for design, development, testing, and manufacturing of items explicitly ordered. A generic order of all tasks required to design, develop, test, and produce all items called for in the contract, to include test and support equipment, to ensure the DAL lists data produced from implied tasks arising from product specifications and DIDs.

Programs should then use the SDF targeting map to order data and to drive life cycle decisions such as DSOR vs. ISOR, competitive vs. sole source, repair or replace, etc. Programs can also create leverage on other contracts by including past performance factors addressing sustainment as evaluation factors in source selections to impose consequences for abusive sustainment practices, e.g., placing the abusive contractor at a competitive disadvantage when seeking future contracts.

Contracts can also ban bad engineering design practices via negative specifications to prevent design practices that unjustifiably deprive the Government of usable technical data due to excessive portion marking of drawings with restrictive data rights and prevent any follow on the use of delivered tech data. Examples of bad engineering practices that can be avoided through negative specifications include spaghetti code, ravioli code, lasagna code, and non-open architecture or modular compliant designs.

Spaghetti code is a source code that is written by the developer to be unstructured and difficult to maintain. This code is developed to make it impossible to segregate portions subject to restricted rights from the developed systems or interface their system with reuse and integrate the previously delivered code.

Likewise, portion marking within a lowest unit of subroutine, function call, or an object (e.g., software designed using object-oriented programming or a mechanical part for non-software) that leaves portion marking incapable of being manufactured results in data deliveries that have no value or use whatever. Portion marking of co-mingled code within code objects or related blocks of code that are interdependent/interrelated is not “practicable” as required by the data rights clauses; thus should be prohibited or challenged.

Another bad software design practice produced “ravioli code” - a term specific to object-oriented programming. Ravioli code describes code that comprises well-structured classes that are easy to understand in isolation, but difficult to understand as a whole. Subsequent users of such code will have an extraordinarily difficult time attempting to reuse and integrate the previously delivered code into a new contractor or Government employee developed systems or interface their system with other replacement systems.

Lasagna code refers to badly designed software code whose layers are so complicated and intertwined that making a change in one layer would unknowingly necessitate changes in all other layers. Such code is not open system architecture, or modular system compliant given the user cannot reuse Government purpose rights or unlimited rights data easily interface such software with a new or replacement system. Such systems tend to be unreliable, hard to maintain, and poorly designed given changes tend to break other parts unexpectedly or parts not obviously related to each other.

Another useful data acquisition tactic comprises data acquisition failure response methods. Such methods enable programs to outmaneuver, flanking, or bypassing a lack of needed technical data, software, or data rights via the creation of new leverage (alternatives). Data acquisition failure response should start with the creation of data acquisition strategies optimized for low leverage conditions.

An example of low leverage condition approaches include the development of ZOPA strategies. ZOPA approaches can include creating data requests that are more objectively acceptable to a contractor first and decoupling these objectively more reasonable requests from more difficult requests. In particular, low leverage optimized approaches includes creating ZOPA driven data sustainment proposals/data orders (objectively reasonable business models/data orders). Such approaches also avoid ZOPD data orders (e.g., soliciting the delivery of data subject to unlimited rights, first and holding off on asks for deliverables containing detailed manufacturing or process data that were developed exclusively at the private expense).

One possible ZOPA focuses on bad value parts or tasks ZOPAs. Supply chain optimization focused value engineering analysis (see e.g., DoD Standardization Document (SD)-24, Value Management) can be used to determine whether the Government is receiving a bad relative value deal. Another ZOPA opportunity arises from common use parts. A prime may be acting as a pass-through vendor – obtaining parts from a supplier and then marking up the parts while adding no or only marginal value. Another ZOPA opportunity uses conflict resolution principles of appeal to shared values/interests in relation to unvested data rights where the Government can argue it has “inchoate rights” (unattached or yet to attach) to data that was not delivered. If the Government paid substantial or all costs for development, it is manifestly unfair for a vendor to refuse to deliver such data in which the Government has inchoate Government purpose rights or unlimited rights. The Government can adopt industry’s argument that is objectively unfair and wrongful for a vendor to deprive a party of the benefit of their bargain and investment. It should be no more acceptable when it is industry acting in this manner than industry argues it is when the Government does this. This ZOPA uses conflict resolution principles of appeal to shared values/interests.

Another ZOPA opportunity arises when a prime has a very good relationship with a supplier and thereby is able to influence the delivery of needed technical data or software. Similarly, a ZOPD can be characterized by a hostile relationship between a prime and a supplier that leads to a supplier refusing to agree to reasonable data acquisition requests. Another ZOPA opportunity arises from parts that impact readiness. Such parts drive degraded mission capable rates or benefit from depot assistance and potentially assume system integrator/design agent role) to improve outcomes. Another ZOPA opportunity arises where the Government uses its superior depot or supply chain expertise to help a vendor. Another ZOPA indicator arises from stable vs. unstable system configuration conditions. There may be less beneficial for the Government to assume supply chain or other responsibilities where a system configuration has not been stabilized or needs frequent redesign within a supply chain activation window (target is moving too fast). Likewise, a ZOPA opportunity arises where parts are subject to reverse engineering and relatively painless qualification since this gives the Government the ability to create a new tech data package at a reasonable cost. Under these circumstances, contractors have far less bargaining leverage.
One effective strategy for addressing low leverage circumstances is to give bad relative value vendors four options. This strategy involves pursuing various options. For example, options include asking a vendor to give better value; partnering with the Government to identify causes for value shortfalls and provide offsetting data and data rights deliverables to address those performance or contractual shortfalls (e.g., avoiding adverse past performance reviews or breach of contract claims); and paying the contractor a reasonable percentage of its development costs (when this cost would be less than the Government’s development costs) to deliver missing technical data or software for reverse engineering and qualification. If the contractor refuses these options, then the Air Force can eliminate the contractor from the transaction, reverse engineer the affected part, and conduct a competition for a replacement vendor(s) to supply the part.

Non-traditional acquisition approaches can provide additional leverage creating strategies. One such strategy is to create a consortium of buyers or developers for a part that is interchangeable or subject to mass production. One mechanism for such a consortium is a cooperative research and development agreement (CRADA) under 15 U.S.C. 3710a. A dual-use technology development strategy can also be used where a part development effort identifies civil and military functions, capabilities, and environments that overlap. Such overlapping needs can be the basis for a mutual need-driven development effort where multiple parties contribute to people, funding, technical data or software, facilities, etc. The resulting products can be sold to Government and non-Government buyers, which can vastly increase total quantities that can be sold to Government and non-Government software, facilities, etc. The resulting products contribute to people, funding, technical data or software, facilities, etc. The resulting products can be sold to Government and non-Government buyers, which can vastly increase total quantities that can be sold to Government and non-Government software, facilities, etc.

One tactic comprises training Government personnel to require contractors to produce records that are required to maintain to justify their marking, we can better identify technical data that is in the public domain or is prior art that is known by others or published by the vendor or others. This will provide ammunition to combat frivolous assertions and markings.

Another tactic includes enforcing breach of contract damages/remedies when a vendor fails to meet its contractual obligation to deliver technical data and computer software that meet Air Force needs. Such remedies include recovery of excess re-performance costs (e.g., costs to reverse engineer), automatic data escrow releases for breach of contract, withholding of payment or offsets, and adverse past performance reviews. For example, a contract can include specific and executable remedies if a part fails more than a specified number of times during an identified time period.

**Lines of Effort (LOE)**

LOEs fit into a background of operational design concepts. Operational design’s initial focus is on helping a leader to visualize the operational or business/market environment, understand the problem that must be solved, and develop a broad operational approach that can create the desired end state. Operational design comprises strategies, campaigns, and operations and organize and employ resources by integrating ends, ways, and means. In the context of joint operation planning, a LOE use the purpose (cause and effect) to focus efforts toward establishing operational and strategic conditions by linking multiple tasks and missions. The operational environment can be defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of a leader or decision-maker. To visualize an approach that can achieve objectives and accomplish the mission, the leader or program must be able to describe both the beginning state of the operational environment and the state of the environment desired when operations have achieved a desired end state. The operational approach is a visualization of broad, general actions—typically described using constructs such as center of gravity, lines of effort and lines of operations—to produce conditions that define the way a program or leader wants the operational environment to look when operations end.

**LOE 1** employs preventative approaches for avoiding unjustifiable and avoidable sole-source contracts. For example, an LOE 1 effort starts with an inventory of Air Force (as well as other services or allied military) data and data rights resources and identifies gaps. A program takes this inventory information and drafts a technical data, software, and data rights threat and opportunity targeting map. This effort identifies technical data and computer software that was ordered (and not ordered) that is required to enable full and open competition, 50/50 core depot compliance, 10 USC 2664 compliance, etc.

**LOE 2** uses the prevention of avoidable sole source tactics that include using effective ordering tactics to maximize delivery of Government purpose rights and unlimited rights technical data, software, logistics product data, etc. Such tactics include: ordering a copy of technical data or software using a modified IMP; use of performance-based contracting, ordering via a modified DAL; and ordering via current recurring use DIDs aligned with system engineering or development tasks.

**LOE 3** also uses prevention of avoidable sole source tactics, including aligning key life cycle tasks and decisions with the threat and opportunity targeting map. Under this LOE, the Government should align data ordering to ensure both the Government and contractors receive ROI.

**LOE 4** includes approaches used during sustainment to create leverage to get better deals and stop “no bids” or unreasonably high proposed prices to obtain technical data or software. Some methods to use to enable competition include bypass, flanking, or outmaneuvering tactics (e.g., using value engineering, reverse engineering, spare parts buyer consortiums).

**LOE 5** includes approaches that reduce/eliminate institutional barriers/data rights killers. Examples include fixing broken records, retention rules, and deploying improved MOPs and MOEs in inspections.

**LOE 6** includes creation of a risk register identifying risk events that create a significant risk to institutional needs (e.g., affordability/sustainability). This LOE can include issuing data acquisition CCRRs that require SAF/AQ and AFMC/CC notification in the event of a risk event trigger. For example, a risk event triggering notification might occur when a program declines to order at least one copy of developmental task data outputs generated during contract performance.

**LOE 7** includes creating teams that can be provided to program offices to perform data acquisition activities. For example, a coach could be activated to support program activities such as: creating a technical data or software precision opportunity or threat targeting map, performing a forensic audit to identify all contracts that ordered data or included Government-funded development tasks; inspecting data for surges in technical data deliveries; performing data rights challenges; or facilitating contract drafting or administration by providing additional engineering expertise or assistance with design tasks, EDA or PLM tools. This LOE can provide pre-packaged data acquisition capabilities to air logistics centers, acquisition and sustainment commands, supply chain product support managers, or other organizations at key life cycle points.

---

36 | EXCEPTIONAL RELEASE MILITARY JOURNAL | ATLOA.ORG | ISSUE 149

ISSUE 149 | ATLOA.ORG | EXCEPTIONAL RELEASE MILITARY JOURNAL | 37
LOE 8 includes drafting contract specifications or data orders with positive or negative specifications. For example, this LOE can deploy teams to help acquisition activities draft contracts that require modular system design, open system architecture, use of application programming interfaces (APIs), or otherwise avoid damaging engineering practices which unfairly deprive the Government of its RoI in the form of delivered, re-usable technical data or software.

LOE 9 includes tiger teams that specialize in drafting data orders for tools such as IDE, PLM, digital factory, digital thread, or other EDA tools. Such teams can ensure data orders are aligned with input interface requirements for EDA, IDE, PLM, or other tools and ensure data delivery requirements are included in contracts that mandate transfer of Government data from contractor hosted systems to Government systems at the appropriate point in the program’s life cycle. Such support also can facilitate the development of data interchange models required to enable cross-flow of data from different systems.

Conclusion

A new data acquisition strategy and operational campaign plan that includes objectives, tactics, and lines of effort (LOE) can provide tremendous benefits to the Air Force. Such benefits include targeting opportunities and threats, preventing avoidable sole-source contracts, ensuring appropriate RoI to both the Government and contractors, providing options to bypass or flank bad deal parts or cases where the Government failed to order needed technical data or software, challenging improper data rights assertions, and ensuring legal value in contracts (remedies). This new strategy and plan will avoid ordering blunders and help programs develop effective leverage and negotiation strategies to deter no-bids and contractors proposing unreasonable prices in response to reasonable requests for technical data and software.

References


ii A performance-based approach can include defining NEEDS or SUSTAINMENT OUTCOMES (which imply data rights) by:

1) Defining our sustainment concept (Di, I, O level maintenance, staticide vs. high intensity combat operations with highly contested supply lines, need for point of use manufacturing of repair parts at remote locations/during combat operations, etc.),

2) Listing the various sustainment phase TASKS that REQUIRE technical data. For example, tasks can include operations, maintenance, installation, and training (OMIT) tasks. Contracts should include specific definitions for maintenance, overhaul, repair, and other critical terms to avoid undesirable contractor strategizing to limit Government deliverables and rights and disputes with contractors on scope of terms such as maintenance (which should include all tasks needed to repair or maintain an item to ensure it reaches its maximum expected useful life). Definitions may also include the negative, e.g., maintenance does not include use to extend useful life or alter its basic function.

3) Competitively re-procuring parts developed at least partially at Government expense.

4) Identifying recipients of data who will perform these tasks (contractor vs. Government) if we may have misunderstood this #4).

5) Enabling meeting our requirements, including e.g., compliance with 10 USC 2664 WITHOUT using public-private party agreements.

6) Enabling programs to have effective insight into and control over design agent decisions which impact total cost of ownership, interoperability, sustainability, diminishing material sources, obsolescence management, use of effective design agent/system engineering approaches (e.g., open system architecture, modular system design, re-usability of existing defense system parts or systems where the DoD already has an effective defense supply chain depot capability, etc.). Next, create a statement of objectives (SOD) which includes:

1) Our desired initial operating capability and sustainment concept with respect to TASKS and who we want to perform those tasks (e.g. Government only, Government/OEM, Government/third party sources);

2) Need to enable compliance with 10 USC § 2464 50/50% Government organic depot maintenance that require technical data and software.

3) A requirement that the contractor deliver to the Government the most recent/updated copies of all technical data or software/software documentation describing items components or processes developed at least partially at Government expense;

4) A requirement that the contractor deliver to the Government form, fit and function (FFF) control drawings for all ICPS not developed at least partially at Government expense;

5) A requirement that the contractor deliver to the Government all technical data or other documentation required to create a secondary source for ICPS developed at least partially at Government expense using a FAR 11.104 Name Brand or Equal acquisition strategy.

6) A requirement on development contracts that the contractor develops a modular system design that enables the Government to use an open architecture based follow on acquisition strategy;

7) A requirement that the contractor deliver to the Government at a minimum: IEEE STD 12207 software requirements specification (SRS); interface control document (ICD); application programming interface (API), and software designed based on object-oriented design rules that is not spaghetti code or other non-open architecture compliant software.

ABOUT THE AUTHOR

Lt Col Christopher Monsey is the lead intellectual property (IP) and acquisition counsel at Air Force Sustainment Center (AFSC), Tinker AFB, Oklahoma.
8) Ensures the Government gets at least Government purpose rights (GPR) NO LOWER than subroutines or function calls to avoid “Swiss cheese” software or unusable source code/programs. Specifying a minimum level of rights is not needed but specifying minimum needs in terms of tasks, decisions, and sustainment concepts can and should be provided. Needs imply both data and data rights given data enables tasks and decisions. Where contractors assert restrictions to function calls, the contract should include delivery requirements for SRS and ICDs to the entire system with at least GPR. This can be supported by establishing that this is the lowest practicable level for segregating the deliverable as segregating at a lower level renders the deliverables unusable (see DFARS 252.227-7203-4(d)) (not practicable). All programs should have a good understanding of DESIGN AGENT DECISIONS that impact the total cost of ownership over a weapon system to include functional, allocated, and production baseline design agent choices. This will allow a program to exercise effective control to ensure such decisions do not create an adverse total cost of ownership, life cycle, or Air Force institutional risk impact – i.e., where a design agent decision is good for the design weapon system and bad for the overall Air Force or combined warfighting capabilities that DoD is required to present to the combatant commanders. The RFP should further require that all proposals provide a plan/data provisioning list that will deliver a technical data, software documentation, and software/software with appropriate data rights to support a “provisioning plan” that enables the Government to execute its sustainment concept, enable its objectives and perform the listed tasks by the specified entities. The source selection should evaluate whether each offeror’s data provisioning plan:

1) Shows a good understanding of the Government’s minimum technical data and computer software deliverable requirements and data rights needs required to enable the sustainment concept, tasks, users,

2) Shows an engineering approach with maximum use of modular system design and open system architecture that delivers critical abstraction layer (CAL) software/software documentation with at least GPR / application programming interface and software developer kits for interfacing restricted rights software and avoids use of customized software (vs. tailored software) absent a compelling total cost of ownership/life cycle value justification. A failure to provide at least GPR for the CAL destroys the utility of an open system solution. An alternate approach can entail requiring Government funding be used to design the CAL application programming interface (API);

3) Enables the Government to comply with 10 USC § 2664 / 10 USC § 2666 without the use of a public private partnership.

4) Requires delivery of at least one copy of technical data and software outputs of Government funded (on this contract or previous contracts) developmental tasks and all technical data, software and software documentation describing ICs/Software developed at least partially at Government expense.
Innovation in Sustainment
Business Processes Represent the Largest Opportunity for Innovation

By: Mr. Jeff Slayton

"Innovation is a way of thinking..."

When you hear the word “innovation,” what comes to mind? Additive manufacturing, machine learning, artificial intelligence, and robotic process automation are frequent mentions, and all represent excellent innovative technologies with significant potential. However, the idea of innovation isn’t limited to these technologies. Innovation is a way of thinking, and the real challenge and opportunity we face are innovating our business processes such that it is easier for process doers to access the right answer in sustainment. Decision cycle speed is the big deal.

Changing Paradigms
For years, we’ve focused on enabling and refining administrative methods almost exclusively in a business process sense, and more than two decades of low-end conflict have not yielded this focus invalid. Our bureaucratic bias defaults to sustaining the old because it is institutionally easier than developing a continual upgrade approach. Our new reality is characterized by smaller fleets and leaner, interlaced supply chains woven into a global economy populated with near-peer competitors where small perturbations can have disproportionate impacts. Assumptions of supply availability require adjustment around a new model in which the supply chain required to sustain our weapon systems must be viewed as a weapon system in and of itself, for without it, we cannot sustain the fight. This system – or machine – starts at the foundry and continues to the fight, and the health of a weapon system is only as healthy as our ability to sustain it.

An Example - New Expectations:

"Anyone planning to sustain an electronic subsystem or component in its base configuration for 30 years should be drawn and quartered publicly – figuratively."

− COL FICTITIOUS FAIRYTALE

The global supply chain and the pace of technological change, present the primary drivers for changing fundamental expectations in how we sustain systems – particularly those comprised of commercially developed technologies.

Everything starts with the demand signal and the business processes creating it. Industry responds to where we place the cash. If we keep asking to maintain the old, they will make old (or we’ll lament them publicly for not doing so, then spend exponentially higher sums to figure out how to redesign it). As the Diminishing Manufacturing Sources and Material Shortages (DMSMS) Resolution Average Cost chart (Figure 1) illustrates, the cost of mitigating DMSMS increases over time, further eroding our ability to recapitalize to meet emerging threats. Compounding this cost is the lost time component between upgrade decisions.

Alternative sustainment models have been studied, and at least one found “a strategy designed to upgrade and replace electronic avionic components (versus sustaining the original design) can improve lifecycle reliability and can result in significant annual and total lifecycle sustainment cost saving.”

Sources and Material Shortages (DMSMS) Resolution Average Cost chart (Figure 1) illustrates, the cost of mitigating DMSMS increases over time, further eroding our ability to recapitalize to meet emerging threats. Compounding this cost is the lost time component between upgrade decisions.

Alternative sustainment models have been studied, and at least one found “a strategy designed to upgrade and replace electronic avionic components (versus sustaining the original design) can improve lifecycle reliability and can result in significant annual and total lifecycle sustainment cost saving.”

Assumptions of supply availability require adjustment around a new model...

So, why don’t we continually upgrade as part of normal sustainment? There are, after all, existing authorities within the planning, programming, budgeting and execution process for this type of life cycle sustainment planning. Aside from situations where the laws of physics limit alternatives, I offer the issue has less to do with the absence of authorities and more to do with how said authorities are utilized. More simply, today’s business process to get to the right answer is administratively challenging and slower than the pace of change. Let’s walk the process and find out.

First, the environment is characterized by different organizations involved in sustainment, which presents ambient challenges (and no, I’m not suggesting a reorg). Then, assuming leaders have driven organizational alignment, discussion on planned upgrades invites immediate – and sometimes ill-informed – debates about whether the adjustment makes changes to the subsystem or component’s Form Fit or Function (aka, “F3” or “F-cubed”).
The real innovation challenge: making the right (strategically relevant) answer the path of least tactical, administrative resistance by innovating business processes.

This decision point is critical (some may characterize it as a significant emotional event) because the decision informs two paths with diverse administrative and fiscal implications. If no change to F3, nothing changes in terms of administrative steps, and life goes on in the same sustainment funding (e.g., Working Capital Fund) stream while only slowly appreciating the costs of managing DMSMS. If it is determined the change affects F3, an investment funding path must be utilized to affect the change. This involves considerably different planning and programming processes, different input and decision cycles, different acquisition panels, and multiple reviews up different chains of command (cue the Benny Hill music). Beyond the administrative challenge, modifications to sustainment then have to compete with administrative and fiscal ramifications, represent or perceived, the F3 decision, and its associated ruleset was established by good people who were strike the right (strategically relevant) answer the path of least tactical, administrative resistance by innovating business processes.

In 2019, AFMC adjusted the scope of IIRP to include improvements of items in the face of obsolescence and safety of flight challenges. More importantly, this reduces the nature of the constraint around the F3 decision and leverages sustainment funds to field improved items as part of the overarching sustainment strategy. The process is by no means perfect, but it’s a significant policy step towards recognizing the need to introduce improved items within sustainment planning and funding streams.

A Starting Point

Change the demand signal. (for the Air Force)

The 448 Supply Chain Management Wing, within the Air Force Sustainment Center, Air Force Materiel Command.

Mr. Jeff Slayton is the Director of Special Programs, Strategy, and Policy for the 448th Supply Chain Management Wing, within the Air Force Sustainment Center, Air Force Materiel Command.
Maximize human potential with Infor Coleman AI

Leverage concentrated artificial intelligence solutions that deliver:

- Access to MICAP status, briefing updates, and mission-critical data in real time
- Improved efficiency with a voice-powered user experience
- Increased smart automation and predictive logistics

Copyright © 2019 Infor. www.infor.com. All rights reserved.

A forward-looking, learning, and fair-minded aviation culture is an ideal. You could also say that in a country that is first in flight, first to fly around the globe, first to fly to the moon, and still pioneering in altitude, duration, and effectiveness, it is an American ideal. And yet, some ideologies contend against progress -- punitive management and the prosecutorial imperative in the face of accidents, mishaps, and error, and that of fear. In a broad sense, we all recognize it when we see it. We empathize with scenes from films such as First Man, where Neil Armstrong, played by Ryan Gosling, declares after a near-fatal accident, “We need to fail! We need to fail down here, so we don’t fail up there!” We relate with these monumental learning moments because they are ingrained in our cultural psyche, and we know that their resulting successes transformed our world. Yet, we struggle to see the same prospect and importance of failures at the tactical level, on the flight line, where our Airmen regularly pioneer into the unknown. To maintain a balanced compliance culture at our tactical level, do we treat failure and error with consistency and fairness, pursuing the root cause instead of attributing blame? Do we promote accountability and communication with a learning system approach in keeping with a values-based compliance culture and a forward-looking vision? Or, do we offer imposing, constricting, subjective policies and even reflexively punitive managerial behaviors; barriers? Do we? What effect does this have on performance, innovation? I believe we do a bit of both, and that is a big part of the problem. We are consistently inconsistent, and effectively, it breaks the circuit of integrity within our US Air Force Maintenance organizations leaving us operationally fragmented. Additionally, although we are still our nation’s engine of air superiority, I believe we are not firing on all cylinders. By taking an honest look at our organization, and engaging in “critical self-examination and innovative thinking to identify solutions to organize, train, equip, and ultimately enable tomorrow’s Joint Force,”1 by asking whether a “…culture of compliance and innovation (are) mutually exclusive?”2 by communicating and cooperating, we can build a culture where they genuinely coexist. By using values-based frameworks, such as Just Culture, we can increase our strength and thaw the “frozen middle”3

Overcoming the mindsets, practices, and policies that act as barriers to our growth. Troubleshooting a culture is like troubleshooting an aircraft,

Leveraging Integrity and Trust:
A Call for Values-Based Compliance in U.S. Air Force Aircraft Maintenance

By: Capt Dave Loska

Unless the progressive elements that enter into our makeup are availed of, we will fall behind in the world’s development.

– Brigadier General William “Billy” L. Mitchell,
Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military, 1925

Copyright ©2019 Infor. www.infor.com. All rights reserved.
both require abstract diagnostics and resolute fault isolation. The ultimate reward comes from discovering the break in the circuit and restoring the livewire.

The intent of this paper is to start a conversation, or rather provoke the resurgence of a forum in which a much older conversation can come to the forefront -- offering honesty and transparency to generate ideas and reveal solutions, for us. From the scrape of the wire brush against the seized component, to the scratch of the policy pen; to those Airmen, NCOs, SNCOs, and Officers that support our policies and accomplish our mission. AF MX compliance policy, practice, and culture intertwined to present an opinion, mainly from a practitioner’s perspective. It concludes with three recommendations to the USAF on doctrine, policy, and practice. I believe we must discuss these matters, and reconcile these disagreements, if USAF MX desires to consider itself transformational.

Motivation

You might think that a focus on compliance culture reform as the single most significant opportunity for improvement in AF MX might seem a bit narrow. There are so many areas in which to progress. You might not even see a problem yet. My motivation for this view is probably in my upbringing. As a kid from Chicago land without much prior knowledge of tools-and-their-uses, joining the Navy to fix attack aircraft on the flight deck of an aircraft carrier was an uphill learning experience; you could even say a listing deck. I made a lot of mistakes, nearly all that could be made. For example, there was an ill-fated day when, as a “seasoned” Plane Captain, I suspended flight deck ops, causing an uphill learning experience; you could even say a listing deck. I made a lot of mistakes, nearly all that could be made. For example, there was an ill-fated day when, as a “seasoned” Plane Captain, I suspended flight deck ops, causing the convenient workaround of “deep-sixing” unaccountable shop rags off the side of the ship, in a task-centric effort to save time from hand carrying them below decks to later be tossed from the ship’s stern. The pile of rags caught a very unfortunate gust of wind, and the rest is a two-beer story as they say, but it ended with my first (and only) unpleasant encounter with the flight deck “Dog” whom I met with my tail between my legs. After learning through many failures, and taking flying lessons and working as an A&P after my enlistment. I also learned the power of the trust of a few good mentors, some of whom were my Quality Assurance Representative (QARs), who saw potential in me even in my worst moments. This trust instilled in me a sense of purpose, which over time cultivated an understanding and ownership of broader organizational objectives, leading to greater adaptability as a technician and leader. As an Aircraft Maintenance Officer in the USAF, I have worked alongside excellent and inspirational leaders at every grade. I have found a culture that sacrifices everything of itself for service. Over time, however, I have become sensitive to some very unfathomable elements in the USAF MX culture, aspects that seem contradictory to a maintenance culture of paramount integrity.

Troubleshooting a culture is like troubleshooting an aircraft, both require abstract diagnostics and resolute fault isolation.

Collaboration

Collaboration in an aviation culture is a Holy Grail-type objective. The USAF has the potential to outperform over every other facet of global aviation because of our shared competitive incentive to Fly, Fight, and Win, an advantage we do not fully apprehend. We often relate to our organizational structure as a network of networks, and refer to barriers to communication as silos and stovepipes. Collaboration, i.e., the breaking of barriers, and the interconnection of silos is good; in contrast, rewarding group-think and building barriers is bad. This Macro/Micro organizational model frames our mind to the importance of information-sharing and divergent thinking. Aviation regulators such as the FAA, also promote information sharing and collaboration in building and sustaining a strong safety and compliance culture -- an informed, flexible, reporting, learning, and fair-minded or just culture. However, aviation regulators have historically met opposition toward information sharing from air carriers. Air carriers who felt that regulators might use the information to punitively beat them over the head, or incidentally share some of their trade secrets with their competitors.

Since the early 2000’s the FAA has made improvements to the US safety regulatory environment in enlightened and trust-building approaches to collaboration such as the Aviation Safety Information Analysis and Sharing (ASIAS) System, and the enactment of Public Law 111–216 requiring each air carrier operating under 14 CFR part 121 of the Federal Aviation Regulations (FARs) to develop and implement a Safety Management System (SMS) to improve the safety of its aviation-related activities, relying on the safety management of the airline. This act may, however, reinforce an incongruity between the incentives of the airline and its mechanics; incentives to maintain profits, vs. integrity. Putting regulators in an awkward push-pull position, responsible for both promoting and regulating the same airline. Airlines questioning mechanisms over finding any maintenance discrepancy outside of their specific maintenance tasks -- reinforcing the temptation to cut corners, relax standards or look the other way... leading to the fear of retribution. Would an airline even be willing to share safety data on its production processes for fear of losing trade secrets to its competitors, or increasing liability for just being honest? In July 2019, during a hearing focused on aviation safety, inspired by the trend of Boeing 737 Max accidents, Congressman John Katko of New York questioned representatives from the NTSB and aviation trade unions on what it would mean to “… change the aviation regulatory culture from punitive to collaborative?”

The slow pace of adaptation of safety tenets and mindsets into aviation maintenance, is perplexing. The available literature on human factors shows a complexity of factors, both profit and production, regulators might use the information to punitively beat them over the head, or incidentally share some of their trade secrets with their competitors.

Over time, however, I have become sensitive to some very confusing elements in the USAF MX culture, aspects that seem contradictory to a maintenance culture of paramount integrity.

Culture

The USAF aircraft maintenance compliance culture belongs to the AF’s more than 70K enlisted and 1.5K officer maintenance personnel responsible for more than 5K military aircraft. It is established by the AF’s history, training, programs, policies, and, most importantly, people. At the unit level, it is primarily defined by policies found in Air Force Instruction (AFI) 21-101, Aircraft and Equipment Maintenance Management, specifically Chapter 6 which delegates technical compliance responsibilities from the Maintenance Group Commander, establishing the Quality Assurance function to the Maintenance Group Commander, establishing the Quality Assurance function to the Group’s staff as the “primary technical advisory agency in the maintenance organization.”

“...
Aside from the flight line, the QA office is an excellent place to pick up the pulse of the MX compliance culture as they are primarily responsible for running the Maintenance Standardization and Evaluation Program (MSEP). According to the AFI 21-101, “The purpose of the MSEP is designed to provide unit’s [sic] with a method of evaluating technical compliance and measure how well they comply with established standards.” The MSEP tends to be the thread of the conversation on unit compliance from day-to-day. It manages all program inspections and provides a routine inspection plan called the Routine Inspection List (RIL), which is the product of a coordinated effort between maintenance leaders for checks, both over-the-shoulder management technical processes and after-action inspections. The resulting inspection findings are categorized by type, and assigned a heuristic score based on either type or severity, especially those findings related to safety violations, deviations from technical data or found otherwise unsatisfactory. The factors of this sample are then compiled, and the average score becomes the squadron’s compliance grade, intended to represent the quality of maintenance.

According to survey data from the AF Safety Center compiled from maintenance units across the AF over the past ten years, 46% of the 87,6K Airmen surveyed would not say that “QA/QAE is well respected in their Squadron” and were either neutral or disagreed with that statement.18 18% disagreed or strongly disagreed. Even more interesting, 24% of the 89.5K surveyed would not say that “Individuals in my squadron are willing to report safety violations, unsafe behaviors, or hazardous conditions.” On this matter, 7% disagreed or strongly disagreed.

Initially, this may not be overly concerning to you. But consider…isn’t it odd that nearly half the Air Force’s maintainers will not say that they respect the one organization especially chartered to maintain quality, compliance, and integrity? That organization is, after all, just a representation of our leadership. Or that roughly 1 out of 5, or truly, thousands of Airmen out there are reluctant to self-report? What are they seeing go unaddressed? Contrary to the survey results, there can be no neutrality when it comes to integrity and trust. Why then the lack of trust? It starts in the heart, but I also think it may begin in part in our compliance model and the implementation of our processes -- our leadership.

“...

I would offer then, that the USAF as an enterprise is better postured than industry to lead in compliance culture, safety thought and ideas, because of our shared competitive incentive to Fly, Fight, and Win.

Quality History

Historically, quality management was between artisans and apprentices. Practices were entrusted individually, and products were sold within communities where the artisan and apprentice held a shared incentive to maintain quality and their own reputation. This was often represented by the maker’s mark of the practice. Very early evidence for this can be seen on bronze weapons developed in China during the Zhou Dynasty in the third century B.C. (Figure 1). Weapons were inscribed with the names of craftsmen and the managers responsible for their quality.19 A powerful aid in quality and accountability from the longest-ruling Chinese dynasty in history. The dawn of the industrial revolution, 20th-century production, and post-WWII globalization brought on advances in quality science, enabling vast improvements in product output, but further distancing quality management from the craft.

In the late 1950s, the USAF faced a management dilemma – a veritable crisis. The confluence of the aggressive advancement in aviation technology following WWII - supersonic aircraft, digital electronic computers, over-the-horizon radar - and the rapidly draining pool of specialized technicians -- 54% to 76% first term airman departing between 1959 and 1961 -- creating an exodus of 18,000 “highly technical” mechanics and gutting the force and secondarily creating a flood of quality escapes.10 The increasing maintenance per flight hour rate led to a steadily rising operational cost. Resulting in a scenario where “…about three-fourths of its equipment required some kind of repair, and 13% had broken down entirely.”11 Not to mention the threat of nuclear war! In 1965 the AF looked to the Strategic Air Command’s (SAC) promising Standardization and Evaluation program (Stan Eval) previously called the Standardization Board (Stanboard)12 which was showing some success in reducing the rate of error of flight crew through administering check rides and tests.13 The comical logo for this program was a vulture with the slogan “Harsh, but Unfair!”14 The maintenance program offshoot, the maintenance standardization evaluation program, was designed to “improve maintenance quality through standardization.”15 You are not alone if you are glad they did not call it the M-Stan-Board! Around the same time, management theorists were designing methodologies, such as multicriteria decision analysis, used to evaluate multiple factors for decision-makers in environments of uncertainty, within the newly designated discipline of decision analysis.16 SAC was the first to adopt this MSEP process in 1965, after which an unpublished Air War College study, only a year later, recommended its adoption to the Air Staff.17 Its subjective Sat/Unsat pass-fail scoring had its origins in the IG inspection teams from days of yore and was later adopted by HQ Maintenance Standardization Evaluation Teams (MSEt’s).18 In 1970 the MSEP was first enacted into the language of the AFM 66-1 (predecessor to the AFI 21-101), and by the following revision in 1972 the AF’s quality inspection policy had grown from 3 bullet points in 1965, to 68 pages when the MSEP program was formerly instituted AF-wide (though not uniformly implemented and therefore ironically not standardized)19 This signified the growing focus...
Confidential Reporting, author David Marx discusses proactive and reactive systems. Dissimilar to today’s program, however, was that using a similar scoring distribution as that of today. The technical inspections of the former program that are proactively pursuing trends acts as a hindrance to that pursuit. Moreover, organizations that are proactively pursuing trends and design intervention could be doing so despite the limitations of the MSEP – the program itself is then left generating reactive heat, and not proactive and predictive light.

Safety Management Systems

Quality and compliance management are both elements of a Safety Management System. The International Civil Aviation Organization (ICAO) categorizes safety management methods into those that are reactive and event-based, proactive and process-oriented, and predictive and analysis-driven (Figure 2). A mature safety management system is proactive and predictive. Immature systems are reactive and event-based, locked into fly-crash-fix-fly daily operations. Hazards within the system are then avoided through the use of controls, of which there are two types: closed-loop systems (those with a feedback mechanism) and open-loop (those that operate without feedback). In his book titled, Whack-a-Mole: The Price We Pay for Expecting Perfection, author David Marx discusses one type of cultural closed-loop system, what he calls a “Learning system” (Figure 2). In which, a group of people familiar with an operating environment convenes to understand errors and work together to design interventions that reduce the likelihood of future mistakes. Designing interventions requires a complete understanding of the system and full cooperation, from the handle of the bullwhip to its cracking end. This requires accurate root cause analysis of error.

There is nothing inherently wrong at face value with our MSEP design. It sits on the shoulders of the giants who created it, the “past generations who made harsher sacrifices so that we might enjoy our way of life today.” But I wonder if we measure the right things? Also, if our scoring of inspections, which dates back to the pass-fail days of yore, is holding short of the bigger picture and impeding our performance.

Auditing consultant and author Dennis Arter addresses the shortcomings of compliance audits in favor of performance audits by stating, “A different perspective on audits is needed. Instead of examining past conformance to requirements in minute detail, you can use current performance to project future actions. It is better to avoid dwelling on mistakes of the past. They can never be changed. A backward-looking view cannot achieve the goal of improved performance within the organization being examined. It will only lead to antagonism and fighting. This is because people are powerless to change the past. They become frustrated and strike back, usually at you. Instead use past practices to predict future performance, which can be changed.”

Figure 2: “Safety Management Continuum” adapted from Stolzer, Halford, & Goglia, 2008
Watershed research supports that process implementation, not just barriers, can prohibit innovations. Moreover, that the inspection of a process rather than a product is known to reduce defects. And yet, how much of our RIL and time is dedicated to the late? How many process-based Management Inspections (MIs) do we conduct in comparison to equipment-based inspections? And does the assignment of subjective grading to event-based audit results and lumping them all together into a super metric introduce competing incentives within our organization to maintain a grade rather than compliance and performance? Does it cause us to run at full speed with our hands over our eyes, and preclude root cause realization? That is a question only those of us that are practitioners under the MSEP can honestly answer. Instead of grading inspection findings in similar categories, could we use them to highlight focus areas in which they spend the majority of our effort in root cause process analysis? If not, is it because we are untrained to determine the root cause adequately? There is a way to fix that. Is it because our QA doesn’t have the time because they are saddled with production-related administrative tasks and programs that could otherwise be delegated to “revitalize the squadron?” There is a way to address that, as well.

Objectivity

To accurately determine the root cause of error, the priorities of the entire maintenance organization must be aligned, and inspections must be objective. Objectivity is a hard thing to maintain, as is trust. Drury & Dempsey capture this difficulty by stating: “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed ‘customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed “Customers rely on the judgment of professional inspectors, checkers, and auditors to make informed

Problem-Solving

An oft-cited example of problem-solving and out-of-the-box thinking is that of the Hungarian born Jewish statistician, Abraham Wald. During WWII, in an effort to increase the survivability of its combat aircraft from sustained battle damage, officers from the U.S. Navy enlisted the support of the Statistical Research Group located at Columbia University, whose aim was dealing with problems of military importance. To those military officers, the solution was clear; increase aircraft armor while limiting deterioration to maneuverability and fuel efficiency from the increased weight. The officers supplied the bullet hole data of returning combat aircraft to Wald. The Officers requested that Wald help determine the location of the greatest need for armor based on where the planes were getting hit the most. Wald’s observations were quite different, however. Wald questioned if the bullet holes were distributed across the aircraft, why were there fewer bullet holes in the aircraft engines? Where were the missing bullet holes? Wald concluded that the missing bullet holes were on the downed aircraft and that the aircraft being shot in the engines were not returning home. His recommendation was, therefore, to increase the armor around the engines, and his methodology would benefit US aircraft survivability in combat for decades to come. Wald’s problem was one of missing data, requiring contrapositive reasoning and the contradiction of convention. Reinforcing those airframe areas that were initially proposed would have done nothing to increase the integrity of the aircraft. By acknowledging the missing information and applying a different perspective, Wald’s recommendations saved lives and vital resources. I believe a comparison could be made, and a similar approach could be taken to correct our course and increase the integrity of our organization, eliminating competing incentives and recovering the missing data.

Competing Incentives

The competing incentives of the MSEP, simplified, and ceteris paribus are as follows:

Figure 3: Abraham Wald and the Missing Bullet Holes

The Quality Inspector, an NCO who always puts integrity first, sets out to conduct an inspection, and later observes a finding. The Quality Inspector must then record and categorize that finding into the generalized buckets of the MSEP. Each is graded, with those regarding safety, technical manual deviation, or those that are generally unsatisfactory assigned a weightier score deduction from the final average. By immediately assigning a scored category, a general root cause may then be obliquely attributed, and root cause realization suspended. In some cases, attributing a scored and graded premature root cause to a squadron, unit, section or individual, and inadvertently attributing blame.

The Maintenance Manager, who eats work and spits excellence, is now incentivized not only to produce safety and reliability but also to maintain an excellent score on behalf of his unit. Understanding that the immediate assignment of a grade is a misrepresentation of his unit’s compliance, he knows that achieving a grade is more the result of the inspector’s findings than it is the representation of his operational environment. He may have, on some occasions, even considered highlighting areas of personal concern for inspection, and would have found the results helpful. But, understanding that more inspections will likely result in a lower grade, he is disincentivized to share. Also, if the findings are in some way unsatisfactory to the manager, he will challenge the inspector. The Manager, often well senior in rank to the Quality Inspector, will challenge the inspector to have those findings discarded. He will challenge when the inspection was conducted, and whether the inspector followed procedural rules of informing the technician before, or debriefing his supervisor after the inspection. He will challenge the inspector’s intent and if the finding was associated with the type of inspection initially intended or if the finding was discovered obliquely. He will challenge the categorization of the finding and whether it was poorly articulated or referenced during documentation. He will test the accuracy of the procedural reference. These will be contended and relitigated until an agreement is made, or not.
The Quality Inspector is now incentivized not only to ensure safety, reliability, and compliance but also to maintain the integrity of MSEP and its weighted average score, this amongst the many other production programs which policy dictates he must keep; he is a busy man. He knows that the Maintenance Colonel does not tolerate the reiterations as they do not represent safety or reliability, and she will either impose time restraints on them, delegating ultimate decision authority to her staff or squash them entirely. However, this reiteration process has by then driven a very surprising informal dynamic. This bullying to justify applies a further burden on QA inspectors to prove intent and thereby creates an informal warranting procedure. QA inspectors are now bound and restricted on what they can report and therefore inspect, and inspections are then reduced from being conducted during a constant presence at the point of execution to golf cart drive-bys of mostly after-the-fact items. Furthermore, the data which was possibly imperfect but nonetheless useful for intervention design never made the cut. This results in the incomplete narrative of the unit’s compliance and whitewashed reporting. Missing data; Missing bullet holes. This shapes our compliance culture even further. This reiteration and warranting distort the self-perception of the QA inspectors, now seeing themselves as a type of police and no longer the brother-at-arms in quality they once were. This policing style of quality management can be identified in some of the widely accepted inherently punitive symbols representing our compliance culture today — a policeman’s badge with its implications of criminality, and the QA crest.

Symbols, Language & Culture

The QA crest is an interesting symbol, as it is truly only an apt representation of a punitive compliance culture. A vulture, dating back to the days of the SAC Stanboard, perch and its peers on a tree trunk — their quarterly meal or “picking up their toolboxes and shutting down productivity when QA arrives. This reactive and event-based compliance process results in an incomplete compliance narrative that drives a whitewashed operational scope. Its weighted average score then becomes only useful as artificial means to enhance an end-of-year individual personal performance report as it most likely shakes out to a >90% annual average, encouraging only mediocrity in the end. This decreases the quality and design of interventions. It breaks the feedback loop. It fractures teamwork; it is a waste. It is in the grain of our organizations, where the stress begins to splitter. And it may also start to explain why some say that “maintenance eats their own.”

There is an inherent friction between compliance and performance that can sometimes lead to adversarial relationships. However, embracing and fortifying the cultural adversarial roles of that natural push-pull relationship, instead of addressing and correcting them, pull an organization in a third direction, ultimately suspending momentum.

If left unchecked, our litigative approach to compliance can translate into an unbalanced black-and-white leadership approach, and a policy paralyzed culture through a lack of teamwork and a culture of fear. For there to be compliance, there must first be a requirement. However, an over-reliance on bureaucratic controls can dangerously impede development, production, and innovation.

Technical Orders

Technical Orders (TOs) provide guidance on the maintenance of weapon systems. Additionally, TOs implement the policy of AFIs such as the 21-101. These sources are authoritatively written by order of the Secretary of the Air Force, an oath-taking officer with powers delegated by the Executive Branch, established by the Constitution of the United States, the highest law of the land. TO deviation is also a leading contributor to maintenance mishaps annually. And yet, we as leaders often stop our root cause analysis at whether a TO was violated from or not, instead of taking a broader system-focused view. Thought leaders within industry conclude that managers often do not pursue root cause of TO deviation, stating, “For many incident/accident reports, Failure to Follow Procedures (FFP) is listed as a causal factor and not analyzed further to determine why the procedure user took the unusual and unauthorized step of failing to follow the given procedure. There is a need to understand the reasoning for not following procedures if we are to help reduce FFP incidents.”

TO adherence, while predominant to maintenance and safety, is only one factor in weapon system diagnostics. Therefore, a policy fixed leadership vision is myopic. For instance, in addition to serving as policy, TOs have unignorable economic and systematic aspects.

Economically speaking, TOs or technical data is Intellectual Property (IP). From a program management perspective, IP is much like a trade secret that translates into the maintainability and sustainability of a weapon system that transacts into dollars. Program managers purchase IP and maintainability from the manufacturer during the procurement of a weapon system. This costly and complicated bargaining chip dictates future maintainability and operations & sustainment costs of an aircraft. These bargaining chips or “trade-offs” come under pressure from factors within the Defense Acquisition System, i.e., cost, schedule, and performance. This largely accounts for why some TOs are “better” than others and why some aircraft are better sustained. Technicians that have worked multiple aircraft can tell the difference between the quality of TOs and maintainability intuitively but are seldom aware of the underlying cause.

Further, maintenance leaders will likely not be aware of these upstream decisions making it challenging to recognize their downstream consequences.
Technicians and maintenance leaders alike, exposed to the backpressure of operational demands, might be unconsciously tempted to overextend their assumption of risk through the bottleneck of poor maintainability and supportability. When confronted with defect, maintenance leaders with a limited scope of the black-and-white of a TO in order to troubleshoot, so to maintenance leaders must consider the entire operating environment when designing interventions or administering discipline. This is where we sometimes go wrong, and when halting our root cause analysis at adherence to instructions means holding short of an understanding of a more actual operating picture. This myopia is what drives failures of creativity and short-sighted, inherently blame attributing behavior. Such as reading technicians Miranda Rights before discussing error, channeling operational feedback via AF Form 1168 “Statement of Suspect/Witness/Complainant,” or a hyper-reliance on ever-accumulating military progressive administrative discipline, tools that are wholly inadequate for the task. While these methods are possibly helpful in preparation for a future court-martial scenario, they take a significant withdrawal from the unit’s piggy bank of trust and likely create a deficit in open communications. In order to determine a real operating picture, we need to begin with our people and how they (we) think.

The Mind of The Maintainer

When Orville and Wilbur Wright required an engine for the first powered flight, the brothers knew they needed one that produced eight to nine brake horsepower, weighed no more than 180 pounds, and was free from vibration. With crude drawings, and nothing but a drill press, shop lathe, and hand tools, Charles Taylor built the first aviation engine. It produced 12 horsepower at full RPM, allowing 150 additional pounds of strengthening on the airframe. Rooted in the same vein, as Charles Taylor, our technicians use limited resources with black-and-white, binary, and basic requirements to accomplish the infinite. Often pioneering into the unknown, they must both firmly hold that which is “concrete,” and reach out to obtain the “abstract.” As leaders, our job is to help them hold-fast to both, and we fail if we pry their grip from either. One fundamental question seems to strain this endeavor.

Upon deviation and error, we repeatedly ask ourselves, “why don’t people just do what they are supposed to?” This, in essence, is the human factor of our business.

For example, sometimes mistaken as a policy to which we strictly adhere, the use of fault isolation and decision making “trouble trees” are a beneficial aid in narrowing the possibilities of fault diagnosis and increasing the probability of accurate troubleshooting which leads to increased weapons system availability and reduced costs. But these tools will only put technicians out on a limb without abstraction. This is why technicians will sometimes anthropomorphize an aircraft during troubleshooting, attributing animate characteristics to the inanimate, and asking questions such as “what is the aircraft thinking during this phase of flight?” They are processing in abstraction -- thinking beyond the concrete. Nevertheless, the repair of complex systems in complex environments introduces the increased potential for error, and when presented with error and deviation, even well-meaning maintenance managers can be tempted to invent simplistic and binary doctrine in an effort to distill the operational scope into a more handy paradigm. An error then exists as either this or that, a “misdemeanor” or “felony” for example, or as the result of either training or attitude, ignorance or ineptitude or committed by the “unfortunate or the incompetent” etc. Root cause analysis of error then instead of becoming distilled, becomes diluted. And the technician can quite possibly be browbeaten back into concrete thinking. That is why simplistic and experiential approaches just won’t do.

Compliance Doctrine

Currently, there is a need for a common doctrine and lexicon in our maintenance compliance culture. Aviation safety research widely concludes that 80% of aviation maintenance accidents are influenced by human factors.36 It is, therefore, critical that leaders have a firm grasp on recognizing the signs and types of human error. This is foundational to maintenance management and should be incorporated in every technical training for technicians and leaders alike. The Dirty Dozen of Aircraft Maintenance lists twelve common human factors to maintenance technicians and is widely adopted as an industry standard for a straightforward discussion on human factors in maintenance. Additionally, our culture needs to be one in which error, and our people are treated fairly with consistency and transparency.

Values-Based Compliance

In a progressive effort to improve its safety culture, in 2015, the FAA published its compliance philosophy to establish a “just safety culture.” To the FAA, this meant fostering “an open and transparent exchange of safety information,” and obtaining “a higher level of safety and compliance with regulatory standards.”

The International Civil Aviation Organization (ICAO) defines a Just Culture as:

“One in which all employees are encouraged to provide, and feel comfortable providing, safety-related information. It is an environment in which employees understand they will be treated justly and fairly on the basis of their actions rather than the outcome of those actions, in the case of positive, as well as negative safety events. A Just Culture recognizes that systemic factors (not just individual actions) must be considered in the evaluation of safety performance and interpretation of human behavior. A strong Just Culture in each aviation organization is perceived as the basis for a successful safety culture.”

Eurocontrol and the European Civil Aviation Conference define Just Culture as:

“A culture in which front line operators or others are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but where gross negligence, willful violations and destructive acts are not tolerated”

In a 2015 memorandum titled “Proactive Aviation Safety Programs and Just Culture” General Carlton D. Everhart II, the Commander of Air Mobility Command stated that “In a Just Culture, airmen are encouraged to report safety-related information, knowing their leadership recognizes the difference between acceptable mistakes and unacceptable behavior.”
Outcome Bias

In the 1951 film titled Flying Leathernecks, John Wayne stars as Maj. Daniel Xavier Kirby in an allegorical clash between the military mission and its people. Kirby’s F-4F Wildcat fighter unit performs relentless missions over Guadalcanal with an undisciplined crew and significant resource constraints. Kirby takes a hard-line disciplinary leadership approach. Kirby’s protagonist in the film is not the enemy but his second-in-command, executive officer Capt Carl “Griff” Griffin. Repeatedly passed over for command for lack of endorsement, Capt Griffin disapproves of Kirby’s hard-line approach. Sympathetic to the needs of the squadron pilots, Griffin often removes men from combat missions. Kirby considers Griffin soft, “you just can’t bring yourself to point your finger at a guy and say, go get killed!” Eventually, Kirby wins him over, and Griffin makes the hard call, earning respect from Kirby and his endorsement for Griffin’s eventual command. In this story, however, there is another character, inconsequential to the plot, but performing a role that is meaningful to maintenance in its own right, the unit’s Line Chief, MSgt Clancy. With no given first name, Clancy is responsible for the readiness of the squadron’s aircraft and just about everything else. He weaves in and out of scenes, often illiciting commandeering needed equipment, everything from reengineering a mess hall washing machine motor into a fuel pump, to stealing a rocking chair for the base’s Colonel. All with the adoring approval of Kirby. With resources stretched thin, the officers admire Clancy’s improvisation. However, towards the end of the story, Clancy is busted in rank to Private First Class when the outcome of that same resourcefulness finally catches up with him. This is oddly laughable to both Kirby and Clancy in a way only appropriate for Hollywood. The relationship culminates with Kirby’s sentiment, “If I have to go where there’s another war, I hope Clancy will be there.” This is a very cliché and admittedly cheesy example, but its subtle implications are considerable. Are we, like the silver screen portrayal of the Flying Leathernecks Kirby and Griffin, at war with ourselves? Do we ever extend our people into double standards in complex operational environments, only to “grab ‘em by the balls” when the outcome is inopportune or even...embarrassing?

Outcome Engenuity defines Severity or Outcome Bias as: “Punishing or disciplining a person who made a human error or engaged in an at-risk behavioral choice, simply because there was a severe outcome.” Conversely, “Not addressing the behavior at all when no adverse outcome results, even though harm could have occurred in a similar circumstance.” A failure to provide a consistent discipline framework causes a break in the feedback loop, preventing open communication about risk and system issues. As Outcome Engenuity states, “The severity bias causes us to “label” people, events, into categories that don’t help us define performance issues.”

Take the cost of an aircraft part, for example. Determining a more severe intervention based on the price to the government of damage to a $100K part as compared to a $100 part might seem entirely rational, the severity or outcome of the former obviously more significant than the latter and therefore the greater severity of the intervention in good keeping with government stewardship. But challenge yourself, does the technician really have any visibility at all into the procurement cost of supply? Or the ergonomics of stewardship. But challenge yourself, does the technician really have any visibility at all into the procurement cost of supply? Or the ergonomics of...
clearly be ridiculous. An error occurring on more expensive aircraft being treated with more severity than a less expensive weapon system. The severity of the discipline of the unit eclipsing that of the other. And yet ask yourself, how many times have you seen, or maybe even written, the price tag of a part damaged in error on the punitive paperwork of a technician? Why was that important to mention? Did it alone influence that intervention decision? If not, how much so? Moreover, the management by exception of audit and inspection outcomes by full reliance on progressive discipline is akin to jumping between gears while pedaling uphill and snapping the chain of communication and trust. Nevertheless, how many times have you seen levels of progressive discipline or hierarchy of management confrontation assigned to categories of inspection findings? TDVs, DSVs and UCRs go straight to the top? In these cases, does education and learning happen at the point of execution or at the point of punishment? I would offer, that sort of learning is as stiff as a stanch uniform at the position of attention on a Saturday morning. All of this begging the question, "might we be our own worst enemy?"

I firmly believe that our AF is entrusted with good leaders of high standing in the ranks of which I often feel unworthy, but I am grateful to be counted. Bad ideologies creep in, taking many forms, and we need to train our minds and fortify ourselves to keep them out. I think it is in this area that we are weakest, most often and often reverses values-based compliance leaders as "Mr. Nice Guys" and unaccountable leaders. Truly, laissez faire leaders based compliance leaders as "Mr. Nice Guys" and weakest, we cave, and often will dismiss values-based compliance culture, what would it look like? Would you ask, "Experiences with Inspector-Generals had convinced me the established concept of the office was wrong... aimed at finding fault. I decided to turn the whole system upside down and view it from the bottom, rather than from the top. My objective would be to give local commanders the tools with which to ensure their efficiency."10

Revitalizing the Squadron, before it was cool! If we play the part of the Air Force anthropologist, for a moment, we can ask what effect does this duplicity have on the trust of our technicians, and what behavior does it promote? What if the “hats” were taken off and just... simply... disappeared? Would our approach to compliance be more consistent, less polarized? What would we do if there were absolutely, no hats on the flight line? One notion that is errantly perpetuated within our ranks is that of obtaining organizational balance in this compliance model. Pulling tools and tricks from the white-hat or the black-hat depending on the timing. There is a reason why attempting to fix your unit through this approach is confusing and unsatisfying. Balance in a black-and-white model is a myth. As the decks of time are continually rocking and its sands ever-shifting, finding balance is only as momentary as the instance in which it was struck. Therefore, its pursuit is fleeting and, in many ways, blinding. Managers pursuing balance through this paradigm often guise their decisions like that of a swinging pendulum, borrowing methodology from each end of a black-and-white spectrum as if each approach pick up the tempo of this metronome. But a mixture of flawed methods does not a pure method make, and more “black-hat” will not fix your problems. What truly exists in this fundamentally flawed compliance model is a path of multiple personality-driven discordant pendulums belonging to its many maintenance managers upon which our technicians must perfectly time their steps in order to avoid the trap. It is imperative that our compliance systems are consistent and not contingent on the personality or impulse of our diverse team of AF leaders.

Imagine that you could reshape our compliance culture, what would it look like? Would you ask, does our culture and subjective processes promote competing incentives? Is a good grade more critical than quality data? Do competing incentives begin the loose chain of distrust and fractured teamwork? Does that lead to the missing bullet holes of missing data, and myopic, policy fixated vision? Does the way in which we treat information from our Airmen catarize the source and restrict its flow? Does it demoralize our people? What behavior does it promote? Would a proactive change lead to better information upon which to design intervention, improving safety, and quality? Are we using all the tools we have available to complete the circuit, create a learning system to educate minds with meaning and purpose at the point of execution? What would you change in the AF, or more importantly, in your unit? Do our symbols of compliance evoke pride and a sense of deepened empowerment? Is there a foreign debris in the throttle quadrant of progress, preventing the advancement required to retake our lead in the formation? As Brig Gen William “Billy” L. Mitchell wrote, “Transportation is the essence of civilization” and humbly submit that it is vital that we have this conversation now, as AF MX leaders.

Recommendations and Final Thoughts

This paper makes three recommendations to the USAF and strives to emphasize their need by offering a wholistic discussion on culture and relevance, mainly from a practitioner’s perspective.

1. Develop and publish compliance doctrine in keeping with industry, regulatory, and academic best practices and research. This must be a collective effort. As far as I have read, the best content is being developed by Outcome Engenuity. In 2015 the FAA published its Compliance Philosophy and Airman Rights, a 6-page, forward-looking, document establishing compliance doctrine and vision, but limited in its practicality. An approach could begin with a combination of the two. Developing a framework consistent with our organizational values and building a common lexicon is key to ensuring our performance and combating negative ideologies.
2. Overhaul the outmoded MSEP, beginning with abandoning the complicated and unnecessary scoring criteria in our multi-criteria analysis MSEP methodology. Decoupling the inspections and results from the short-sighted grade, will allow for more adaptability within inspection areas, better precision in personnel evaluations and ultimately better data. This should also encourage a more process-oriented, performance-based approach/model from which to launch into root cause analysis and increase future performance. Further research should be conducted into the appropriateness of this methodology, considering the sensitivity to and the mutual independence of the input factors and the output, as described in the competing incentives example. There is a great degree of flexibility in audit design. There are many available ways to analyze and display audit data, i.e., balanced scorecard, dashboard, heatmap, control chart, attribute chart, pareto etc. Many ways to design audit systems. The key is in simplicity and the ability to lead to what is most important, achieving organizational goals and promoting change.10

Personnel evaluations should, at the very least, be disaggregated from this metric. Our policy should reflect our organizational identity and within that reality strive to develop a “learning culture” in a “learning system.” Considering the average age of an industry Aircraft Maintenance Technician is 51 years old and with an average age of workforce entry of 25 years old after a minimum of a 24-month trade school. Awarding A&P, a certification that by industry is considered a “license to learn.” And compare after a minimum of a 24-month trade school. The weapon of the maintainer artisan is our integrity behind the panel. It is the trust of a warrior with our maker’s mark of integrity and trust, a symphony of Technical Sergeant Joseph Gardner III that can’t be rewound. It is the icy klaxon call on a frigid coastal morning. It is the breathless silence on the cockpit voice recording of Technical Sergeant Thomas Mueller, trapped in his prison cell of guilt. It is the virulent vulture, sorts, and then get out of their way. For now, at least, our symbols of compliance are what we’ve made them. The virulent culture, punitive police badge, and duplicitous black and white hats adorn our units and remind us of the correlating current state which they promote. A better symbol could be employed. An empowering symbol, intelligent and bold. An example could be taken from the ancient Zhou Dynasty weaponry craftsman. The weapon of the maintainer artisan warrior with our maker’s mark of integrity and trust, set in the black heart of a common enemy.

A better symbol could be employed, an empowering symbol, intelligent and bold.

References
8. Ibid

Captain Dave Loska

ABOUT THE AUTHOR
Captain Loska is a U.S. Air Force Aircraft Maintenance Officer, currently serving as a Logistics Career Broadening Officer assigned to the Oklahoma City Air Logistics Complex, Tinker AFB, Oklahoma.

12. Ibid


23. Ibid


25. Ibid


33. Ibid


58. FAA. Flight Standards Information Management System Retrieved from FAA. http://fsims.faa.gov/PICResults


