Creating a Flexible and Effective Information Technology Management and Acquisition System: Elements for Success in a Rapidly Changing Landscape Testimony before the Committee on Armed Services United States House of Representatives Subcommittee on Emerging Threats and Capabilities

Mr. Edward Greer

2:00 PM
Wednesday, April 26, 2017
Rayburn House Office Building, Room 2118

Chairwoman Stefanik, Ranking Member Langevin, and Members of the Subcommittee, thank you for the opportunity to appear before you this afternoon. I have over 22 years of executive experience (15 years at the Senior Executive Service level) including over 20 years of technical experience—the vast majority in Test & Evaluation. I served as the Deputy Assistant Secretary of Defense for Developmental Test & Evaluation -- DASD (DT&E) from 2010 to 2013. I was also the Chief Operating Officer for a large federal contractor (an IT-based company) with contracts inside and outside the Department of Defense. I was the Naval Air Systems Command's senior executive for test and evaluation and also served concurrently as the Executive Director for the Naval Air Warfare Center, Aircraft Division consisting of over 14,400 personnel overseeing all technical and business matters for the Command. I served as the Principal Deputy Program Manager for a major aviation weapon system.

Managing IT acquisition systems can be one of the most challenging aspects of program management. OSD has developed policy for acquiring IT systems and which is contained within DoD 5000.75. This policy differs from acquiring tactical weapon systems for many reasons from large production buys, advanced technological challenges, ever-changing threats—just to mention a few.

I would like to briefly discuss four significant topics this afternoon:

1. *Major Automated Information Systems (MAIS) Challenges*
2. *MAIS Best Practices*
3. *The role of DT&E within the Services and at OSD*
4. *Business Systems versus Tactical Weapon Systems Acquisition*

First, Major Automated Information Systems (MAIS) Challenges

The challenging nature of MAIS acquisition can be attributed to many factors, but software acquisition reference materials often cite complexity and unstable requirements as the most significant.

• **Program complexity:** DOD MAIS programs tend to be very complex. Typical MAIS programs have to be integrated into multiple existing enterprises that contain large numbers of interfaces with government and commercial entities, each with its own configuration, database structure, and security requirements. In addition, the program itself most often is an integration of large numbers of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) components with existing military and commercial networks. This complexity is often paired with an acquisition strategy that requires delivery of a full, mature product in a single development cycle, which often results in delays and performance shortfalls.

• **Unstable requirements:** DOD systems often have to deal with changing requirements. In many cases, the changes are driven by advancement in technology (e.g., vendors updating hardware, operating system, or database versions) and the program office must either pay sharply increased costs to continue the support or move to a newer version with associated changes. At other times, world events and doctrine changes drive the requirements to change (e.g., a system that was intended for use in conventional warfare may need new functions to be used in counterinsurgency warfare). In either case, changes in requirements necessitate changes in software, causing disruptions in the development cycle.

- **Build versus Buy:** While many IT companies regret building enterprise software because it is much more expensive than expected, there are times when custom software is best. When faced with a decision to build or buy, it is a difficult question to answer and it is too easy to make the wrong choice. Most decisions are a blend of two extremes A) make an emotional decision that "feels right" or B) make a rational decision driven by data. Many companies lean too far in the emotional direction, when hard data is available, making an emotional decision is not good business practice. A rational build vs. buy decision starts with well-defined requirements. If an organization has an in-house development team, there is always a push to build because they can supposedly satisfy all needs. However, from my experience, it is usually far cheaper and faster to buy than to build. While it takes significant work to execute properly, the cost of making the wrong decision will be felt for years. On the other hand, the consequences of the right decision can resonate with the bottom line for decades or more.

Second, MAIS Best Practices

There are many "best practices" within the commercial sector and within DOD. I would like to highlight a few that can yield significant efficiencies in the development of software intensive systems.

- **Executive Leadership Participation:** Robust and continued senior-level attention and participation contributed significantly to the success of agile acquisition MAIS programs like the Army's Logistics Modernization Program (LMP), Global Combat Support System – Army (GCSS-A), and GCSS – Joint (GCSS J). Senior leader support was key for securing necessary resources, enforcing updated business processes, and shortening decision cycles. Agile programs tend to have relatively short delivery cycles. This often means short development test- deployment cycles. Executing such agile cycles is resource-intensive for the entire acquisition team. A typical agile program deploys an approved release, develops the current release, and plans for the next release, all at the same time. To support such concurrent acquisition cycles, testers must simultaneously prepare evaluation reports from the last release, execute and witness test events for the current release, and conduct risk assessment and plan test events for the next release. One test team usually cannot adequately plan the testing, and report on other phases simultaneously.

- **Iterative Developmental Tests that Start Early**: MAIS programs typically have one prime vendor that integrates hardware and software components from multiple vendors. The program office should have a coherent strategy to find and fix problems as each software component is developed and delivered, because software engineers are able to find and fix problems more quickly before a software module is integrated into a larger and more complex program. Isolating the root causes of a problem can be very difficult after the software has been nested with other vendors' products. In addition, the prime vendor may have to redo the integration work after receiving an updated software module.

- **Database Interfaces and Commonality:** MAIS programs typically ingest data from multiple sources to produce new database products. Each of these sources may be changing configurations for various reason while the program is in development and beyond. If data sources are not available or provide inaccurate data, the resulting product will be inaccurate. The program may not be able to ingest the data if a data source provides data in a different format. An early test of process and data in a controlled environment makes it much easier to identify and fix root causes of any discrepancies.

- **A Robust Developmental Test with Operationally Representative Interfaces and Networks:** Many complex MAIS programs perform well in DT and fail to perform in OT. Automated acceptance and regression tests provide an efficient and reliable option to verify that a code change works as intended without breaking anything. However, automated testing is not a replacement for a comprehensive DT. Automated testing is a prerequisite step to make sure coding is done correctly; it is not a validation of the software's ability to support the user's mission. Automated developmental testing is critical to gain efficiency and accuracy. Automated acceptance and regression tests provide an efficient and reliable option to verify that a code change works as intended without breaking anything else. However, program offices must avoid using automated testing as a replacement for a comprehensive DT. Automated testing is a prerequisite step to make sure coding is done correctly; it is not a validation of the software's ability to support the user's mission. Many complex MAIS programs perform well in DT and fail to perform in OT.

- **Persistent Maintenance of the Cybersecurity Plan of Actions and Milestones:** An enterprise network requires MAIS programs to interface with multiple outside programs, which often include commercial systems. Allowing such connections is inherently risky from a cybersecurity perspective, and often makes it impossible to eliminate all vulnerabilities. Thus, it is important to identify, document, and continue to monitor those risks. A Cybersecurity Plan of Actions and Milestones (POA&M) is the best tool to identify and document cybersecurity vulnerabilities and the mitigations for them. The POA&M should clearly identify all of the vulnerabilities by priority and urgency, the proposed corrective actions, responsible organization and person, and the milestone to achieve correction. It should include vulnerabilities associated with interfacing systems, and should not be a document that is approved once and put away; the threats are dynamic, as are the network environments.

- **Implementing Best Practices through Agile Acquisition:**

By “agile”, I mean the continuous collaborative efforts by the system integrator, software developer, the requirements developer, the tester, and the user to deliver regular software releases of incrementally increasing capabilities.

The intent is to avoid big bang integration and late defect discovery at the end of a prolonged development cycle, and instead validate requirements and deliver value sooner. This is done by delivering smaller but more frequent, higher-quality releases with end-to-end functionality. It is enabled by the developer’s transparency and regular access to users (or capable user proxies), and senior decision makers -- to resolve problems, issues, and make changes quickly. The goal of agile is to deliver a tested and error free capability to the field as soon as possible. Agile is not the Wild West with few rules to follow. Proper configuration management, documentation, and testing is still required to prove the value of the release and for the long term operation/training and maintenance support. Agile development demands great transparency, discipline and rigor to rapidly and reliably deliver working software capability on a frequent cadence.

The best practices identified above can help to improve the success of MAIS programs and should be applied broadly. In order to maximize the effectiveness of these practices, DOD should pursue the agile acquisition approach. Incremental software delivery is one aspect of agile acquisition and has already been implemented with some success. However, DOD can do more to accommodate agile software development. Using proven commercial agile frameworks is a good way to systematically integrate the best practices. To overcome challenges associated with program complexity and requirements instability, DODI 5000.02 includes an acquisition model suitable for incremental software delivery. Compared to a traditional “waterfall” model, where all of the functions are developed and delivered in one lengthy and monolithic acquisition cycle, incremental delivery allows each increment to focus on a selected set of functions, which reduces complexity. In addition, each increment takes a shorter time, and thus reduces the chance of requirement changes.

Third, the role of DT&E within the Services and at OSD

Conducting developmental test & evaluation in an agile environment should be done early and often. During a major weapon system development cycle, 80% of T&E is DT&E. It is the most valuable source of information to monitor and gauge the progress of our Nation's Major Defense Programs throughout design and development.

Conducting Developmental Test & Evaluation within the Services is a time and resource-consuming event. In aviation, it is potentially a life or death event. Safety is paramount along with robust test planning and review and approval of test plans. The vast majority of the cost of Service Test & Evaluation professionals is funded by the program managers responsible for fielding the weapon system, therefore they are subject to potentially biased reporting due to pressure from the program managers. It is almost impossible to obtain the raw data from a test until the program manager has approved the release.

During my three years as DASD(DT&E), I personally observed my action officers being unable to secure the data immediately after the test based on direction from the program managers that required the data to be reviewed by the program managers prior to release. The Services Test & Evaluation professionals followed the program managers' directions since the program manager funded their salary.

OSD DT&E is the only DT&E organization within DOD not funded by the program managers, therefore the action officers are independent evaluators. Developmental Test and Operational Test are two functions that are critical to maintain within OSD. As DASD(DT&E), my independent assessment of test schedule adequacy and maturity came from DT&E up until milestone C and from DOT&E from milestone C through the decision to go into production. The Services do a fairly good job of evaluating their weapon systems, but the "trust, but verify" approach has served DOD well over the years. In my opinion, the only issue with OSD DT&E is that it is organizationally misaligned to yield optimum results. It is buried too low within the organizational structure. The points listed below highlight a few reasons why OSD should maintain a robust DT&E organization:

- OSD/DT&E provides institutional funding to help programs across all of the DoD enterprise. If this office didn’t exist, these funding sources wouldn't exist. DASD(DT&E) initiated a joint requirements study, that delivered a consensus study on 5th generation aerial threat emulation needs, and is currently finishing a Joint Analysis of Alternatives (AoA). This resulted in major upgrades to QF-16 last year, and will inform a FY19 budget issue for long term material solutions.

- DASD(DT&E) facilitated enterprise-wide efficiencies by helping programs optimize test designs. In 2016, DT&E was able to help 40 programs quantify enterprise-wide efficiencies on 8 of programs to optimize test designs in various ways.

- DASD(DT&E) provided informed judgement on mitigation of design deficiencies and production/fielding decisions by providing independent assessments to the Defense Acquisition Executive (DAE) for Major Defense Programs across the Department.

- DASD(DT&E) is the T&E Career Field manager and that's not a task that can be stovepiped in one Service. The T&E workforce of 8,600 covers 4 Military Services and the Defense Agencies.

- Congress continues to want a report covering DT&E activity across the DoD enterprise. This can't be stovepiped in one Service.

- DT&E develops DT&E policy and guidance, and that must be developed from an informed position with experience across the entire DoD enterprise, not just a single Service view.

- There are significant DT&E activities that occur outside of the Services and within the Defense Agencies.

- The Fiscal Year 2017 Defense Authorization speaks to a stronger DT&E organization in OSD and a rebalancing of resources between DOT&E and DT&E. So Congress clearly wants to not only keep DT&E after the reorganization, but wants to fix the resource imbalance.

And fourth, Business Systems versus Tactical Weapon Systems

In the current complex Cyber threat environment, Defense Department needs have evolved far beyond traditional IT/IA and business systems best practices. Our ability to operate in the Cyber Warfare environment of the future hinges on agile changes to our policies, organizational structures, workforce, and infrastructure. How we respond today will affect how we own and control the battlespace of the future. The following comments will focus primarily on the technical aspects of Cyber in support of DoD Research, Development, Test and Evaluation (RDT&E) of warfighting systems and less on the business and corporate side of the IT/IA/Cyber equation.

What can be improved quickly to meet the challenge? It is important to make a distinction between Cyber and IT/IA policies for warfighting systems and those pertaining to business systems and "corporate enablers" like email, common business systems, and cloud applications. While there can be overlap in similar network vulnerabilities and workforce skills across the business and technical communities, we must be careful to ensure the right levels of engineering and RDT&E rigor are applied to defensive and offensive cyber of our aircraft, ship, subsurface, unmanned and space warfighting systems. Policies need to be developed with care and leadership must avoid applying blanket policies developed for business systems and networks to operational warfighting systems. Those making decisions must have the right background and skills and must avoid generating costly churn and bureaucratic approaches, which will slow rapid deployment of capability.

Currently the Department is spending large amounts of money "rationalizing" data centers and applications with an eye toward reductions and mandating edicts about "moving to the cloud". This might make sense in many cases and be a valid goal but when trying to apply to research labs, warfighting systems and highly classified programs, it can involve spending unnecessary time and money justifying why policies don't make sense and takes our collective eye off the ball of hardening our technical systems against vulnerabilities and developing offensive techniques. As an example, when looking for “data center reductions” in some Services, every server has been viewed as a candidate for consolidation, even if being used to drive a warfighting lab which requires computational support locally. There should always be an eye toward continued efficiencies and saving in IT but not at the expense of common sense. Technical labs and communities should be held accountable for making recommendations for IT consolidation and savings but should control their own destiny in determining the best solutions. This could involve improved use of existing High Performance Computing assets or virtualization of assets but these are very different that the choices you might make for a common email or business system.

In the past, IT/IA compliance has been more about policing functions and paperwork vice risk assessment and a focus on hardening technical systems early in development. Those in the field have often had a compliance or business system background vice a systems engineering, network engineering or “hacker” based set of expertise. This must change. Each Service should review their IT/IA compliance organizations, processes and tracking system and shift from “checking the checkers” to staffing with a new RDT&E and Cyber engineering and testing skill set. To ensure that there is an appropriate focus on the “Cyber systems engineering”, it is now time to pair a “traditional” CIO function for business systems, email, common databases and promulgation of policy with an “RDT&E Warfighting System Cyber Assessment” function which is focused on the tactical weapons systems impacts of Cyber. The recent movement to the Risk Management Framework is a good step in the right direction but this process needs to be managed by Executive Leadership and a supporting workforce with the right technical skills and risk assessment experience to make the best technical tradeoffs as we deploy complex systems in this new Cyber threat environment. Warfighting acquisition programs and Cyber technical work must be staffed by the appropriate mix of Government experts from the Systems Engineering and RDT&E community vice the traditional CIO community or corporate operations workforce. The Engineering and Test Cyber workforce must have relevant training, skills and certifications aligned to meet these new requirements and should not be part of a cookie cutter approach applied to a professional job series.

The Department of Defense has made an ambitious start to ensure the right Cyber infrastructure is developed. The Test Resource Management Center within OSD is leading the way as the Cyber Executive Agent for enabling test infrastructure with the development of robust National Cyber Range nodes and connectivity. However, there must also be appropriate resourcing for Service Cyber laboratories and the development of robust hardware-in-the-loop laboratories to experiment and ensure our systems are agile in their defenses and hardened against emerging cyber threats. Each Service should provide a development plan for specialized cyber capabilities and be resourced to develop key avionics, ship, submarine, space and operational network laboratories as required. TRMC should be the Executive champion and investment arm for common tools and ensure linkage and integration of Service capabilities so DoD can "Develop, Experiment, Test and Train Like It Fights" in the Cyber realm.

To understand our readiness to face the new Cyber environment, Test and Evaluation is critically important. Operational Testing is key before deployment of capabilities and must include cyber measures of performance and vulnerability assessments. However, early and comprehensive Developmental Testing is even more critical, as early vulnerability findings can be addressed with design changes. Finding Cyber issues in Operational Testing is too late to be cost effective. This is why a strong Developmental Test Organization at the OSD level is needed. A focus on Cyber T&E policy, consistent execution and connectivity across individual Service and program efforts will ensure that the entire process will work as needed when called upon. Cyber is just one area where this is needed but must be a key focus as we prepare to operate in the highly competitive battlespace of the future.

Conclusion: The challenging nature of MAIS acquisition can be attributed to many factors, but software acquisition reference materials often cite complexity and unstable requirements as the most significant. Continuous developmental test & evaluation is mandatory if agile software development principles are followed. DT&E answers the question "Did you build the "thing" correctly." OT&E answers the question "Did you build the right thing." Independent DT&E helps the Military Decision Authority, by providing data that enables him or her to decide to commit resources appropriate to the phase of the acquisition process. There are many “best practices” within the commercial sector and within DOD. I highlighted just a few that can yield significant efficiencies in the development of software intensive systems. In the current complex Cyber threat environment, Defense Department needs have evolved far beyond traditional IT/IA and business systems best practices. Our ability to operate in the Cyber Warfare environment of the future hinges on agile changes to our policies, organizational structures, workforce, and infrastructure. How we respond today will affect how we own and control the battlespace of the future. To ensure that there is an appropriate focus on the “Cyber systems engineering”, it is now time to pair a “traditional” CIO function for business systems, email, common databases and promulgation of policy with an “RDT&E Warfighting System Cyber Assessment” function which is focused on the tactical weapons systems impacts of Cyber.