April 26, 2017

Creating a Flexible and Effective Information Technology Management and Acquisition System: Elements for Success in a Rapidly Changing Landscape

Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, United States House of Representatives, One Hundred Fifteenth Congress, First Session

Hearing Contents:

Witnesses

Ed Greer
President; Former Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
Greer Consulting, LLC
View Testimony

Terry Halvorsen
Former Chief Information Officer; Chief Information Officer
Department of Defense; Department of the Navy
View Testimony

Peter Levine
Former Deputy Chief Management Officer; Undersecretary of Defense for Personnel and Readiness
Department of Defense
View Testimony

Available Webcast(s)*:

Watch Full Hearing

Compiled From*:

https://armedservices.house.gov/legislation/hearings/creating-flexible-and-effective-information-technology-management-and

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

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.

STATEMENT BY

TERRY HALVORSEN

BEFORE THE

HOUSE ARMED SERVICES SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ON

CREATING A FLEXIBLE AND EFFECTIVE INFORMATION TECHNOLOGY MANAGEMENT AND ACQUISITION SYSTEM: ELEMENTS FOR SUCCESS IN A RAPIDLY CHANGING LANDSCAPE

APRIL 26, 2017

NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE
ARMED SERVICES COMMITTEE

Introduction

Good morning Mr. Chairman, Ranking Member, and Distinguished Members of the Committee. Thank you for this opportunity to testify before the Committee today on Creating a flexible and effective information technology management and acquisition system and elements for success in a rapidly changing landscape. I am Terry Halvorsen, currently an Executive Vice President for Samsung Electronics of America and Advisor to JK Shin the CEO of Samsung Electronics. I retired on February 28th 2017, after almost 37 years of military and civilian service to the Department of Defense. Until February 28th of this year I was the Department of Defense (DoD) Chief Information Officer (CIO). As the senior civilian advisor to the Secretary of Defense for IT, I was responsible for all matters relating to the DoD information enterprise, including cybersecurity and IT modernization for the Department.

DoD, today faces critical global challenges and budgetary issues similar to those it has had and met throughout history. I believe DoD will meet these challenges, but it is faced with an added and unprecedented dimension. This is arguably the period in history with the fastest developing and most complex technology. Unlike previous times, the vast majority of this technology growth is occurring in the private sector not originating with the government. This means in addition to identifying the right capabilities to meet DoD requirements, DoD must be able to acquire and integrate this technology with greater agility. Today's environment demands more broadly defining capability and not providing detailed requirements that dictate solutions. At times the government because of the current requirements thinking and process is procuring legacy.

DoD must also have a better understanding of the commercial environment and become more effective and efficient in working with industry and determining how solutions should be implemented. With respect to business systems DOD must ask, should it implement whole commercial solutions or some degree of hybrid solution retaining some government capability. I strongly recommend that the going in position for business solutions until proven wrong thru business case analysis is completely adopting commercial solutions. The real question is what businesses DoD should be directly in and where should it off-load to the commercial sector.

Regarding systems that are more aligned with the primary mission of the DoD, such as national security systems. DoD must more carefully weigh the mission risks, mission security requirements and since these systems are more likely to be operated by military or civilian members of DOD, the workforce implications of training and sustainment. This new changing environment also means DoD will be acquiring more services from industry as opposed to just buying products. To successfully buy services in this exploding technical environment will require DoD to form better partnerships with industry and for industry to be more open to sharing technical data with DoD. To facilitate the building of these critical partnerships, I believe this committee and others will need to look at the laws governing relationships and contact between DoD officials and industry members, expand programs that allow for exchange of employees, and most importantly encourage more interaction between DoD and industry through all means possible. I have personally benefited from mentorship and dialogue with leaders inside government and from inside industry. We must embrace this and proactively promote attendance at meetings between industry and government leaders, especially those that include wide segments of the IT sector. As an example and this is only one, each year CISCO holds a CIO conference that includes many of the leading CIO from industry attend. I have been fortunate to attend this, sometimes at significant out of pocket expense. I couldn't however reap the full benefits from these events or fully participate because of the current laws and interpretations of the laws about accepting gifts. While these laws were well intentioned they do not serve us well today and certainly need to be updated to include reasonable fiscal limits. Yes they are ways to get exceptions to most of these laws, but it is not encouraged and truthfully is discouraged. This is a cultural change more than a change in laws, it is a change in the way DoD, industry and the government currently thinks.

The ability to decide and adopt more quickly emerging technologies also requires some different approaches to acquisition and procurement. I believe that today we are doing much more procurement from industry of developed systems and services, then we are acquiring new systems and to a less extent new capabilities. The DoD needs to both succeed and fail faster in this dynamic ever changing environment. Many of our allies are embracing smaller procurements and giving authority to the CIO to make instant decisions on small new technology investments backed by quick business case analysis supported by industry trends. The efforts of DIUX and Digital services group help in this area, and should continue to be supported. However the CIO, with access to C suite personnel in both emerging and established companies and with the venture capitalist and key allied leaders will have key knowledge an insight on investment that could rapidly change the game. I would recommend this committee consider legislation that allows the CIO to make immediate small investments, up to a combined limit of 10M based on documented business trends and combined business/mission case analysis.

Testing of commercial products from an acceptance and security perspective today is often the long pole in the procurement/contracting process. These processes today are mostly based on processes established for weapons system or other large product procurements/acquisitions. These processes do not adapt well to the commercially procured IT world, this is especially true when applied to system and application software. Despite many diligent efforts by DoD, other government agencies and industry the security acceptance processes can take longer than a year and too often this is the case. I strongly recommend this committee consider establishing an industry and government group to work together on this problem and bring forth in 90 days a plan with recommended supporting legislation that leverages commercial testing provides government mission/security assurance at acceptable levels for secret and below systems. Today's processes in addition to being lengthy also cost the Government and Industry too much money. I am positive that the IT industry and IT security industry would embrace this effort. The output of this plan would also improve the threat information data flow between industry and the government. Again I believe that DOD, NSA and other agencies have been working within the existing limits of the law and current interpretations of the law, but that isn't enough. This is again a cultural change and in the beginning will require acceptance of at least the perception of more risk. I would however suggest the dangers in delaying the fielding and adopting of new technology and the upgrading and patching of software pose much greater risk.

Improved efficiency is one of the benefits that should be reaped from creating a flexible and effective information technology management and acquisition system. I believe that DoD is pursuing this and has identified millions in direct and indirect IT savings. I would like to say a word or two about what has been called by many the McKinsey report. This is the report that was supposedly buried by the DOD and ignored $125M in savings. I must say that is simply not true. The work done by the Defense Business Board (DBB) and augmented by separate work done by McKinsey was extensively used by DoD to develop savings plans, look at ways to reduce work and even today continues to be a resource. It was good work by the DBB and McKinsey, but was not at the detailed execution level and the savings were based on extreme numbers without consideration of many factors. This was widely recognized by members of the DBB and McKinsey in my personal discussions with them and I can positively attest that this work was used in aggressively pursuing IT savings within the DOD.

There is still much work to do and since I have left, the DoD CIO and the DoD DCMO have continued to aggressively seek savings and have identified more efficiencies in medical IT consolidation and revamping the DoD travel system. DoD continues to move forward with the windows 10 initiative, eliminating the Common access card and expanding the use of cloud computing or distributed compute. However, to reach the full potential of these efficiencies, DOD, Industry and the branches of Government are going to have to have a discussion on the civilian workforce and how to restructure and retrain significant numbers of that workforce. Work has and will continue to fundamentally change and evolve in the IT/cyber area. Today DOD and I would say government IT/Cyber workforce is not properly shaped with regards to required skills and numbers. Areas like cyber security are going to need to grow to accomplish the mission and areas like data center management and operations will need to reduce. Overall labor cost must reduce as a total % of the IT/Cyber budget. Industry had to do this and so will DoD and the Government as a whole. We need to think together with industry and all the branches of the government about retraining programs for those members with the aptitude to move into new work areas like cyber. This will not be free, but industry has found this to be cost effective and it is the right thing to do for all our people. We need to work to open the flow back and forth between the government and commercial workforce. Our allies are using interesting contracting and term employment options to attract critical skills and close the pay gaps. I do believe and think that employment trends support the conclusion that career employment in one area and with one organization will not be the norm. It needs to be much easier from a perspective of salary, retirement and medical benefits to change jobs and employers. We need to encourage the best and brightest from industry and government to move between the two workforces. This is how we will develop the best leaders for government and industry. I know from personal experience it is becoming increasingly hard to succeed in government technology areas like IT and Cyber without understanding the commercial sector and have also seen firsthand how hard it is to succeed in managing technical aspects of big government operations without having an understanding of how government works. Commercial and government workforce members who have participated in our exchange programs tell me they have benefited from working inside the government and industry. In my discussions with industry leaders they all agree making it easier to move between sectors is a winning idea. In my discussions with political leaders from both parties they all agree that this is a good idea. This is maybe an area where we could produce quick wins for everyone. I would again suggest that this committee consider establishing a group comprised of elected officials, government and industry leaders to report back in 90 days on specific recommendations that could be implemented to address these workforce issues.

I would like to address an efficiency area that I failed to produce the right results in, while I was both the DoD and Navy CIO. This is the area of data center closure, I badly underestimated the complexity of this issue, the resistance internally and externally and I addressed the problem incorrectly. This is not about consolidating data centers and reaping savings, it is about developing a more holistic data strategy that focuses on providing the right data to the mission owner in the time dictated by the mission. It must be about the data content, data delivery and data security from a mission/business perspective. I have been quoted as saying data is like milk. It is true most data has a shelf life and is time dependent. This also means most of the time data security levels are time dependent, this is true of business and warfare data. If DoD and industry work together on this, I believe that it will result in tremendous savings, but also in great mission improvement. We should consider just how much data needs to be stored? How and to whom should the data be distributed? What timeline does it need to be distributed on? For what length of time does data require high security protection? How do we change the level up or down more rapidly? Where can pure commercial services be used? What about data as a service? If DoD works on a total plan with industry at the start to answer these questions it can be successful. It will however require consistent decision making and enterprise commitment. For this reason, I do believe authority needs to be consolidated at the DoD level. I was not a believer that all planning and execution of IT needed to be at the DoD level and I still believe that to be the case. However in this matter I do think to gain the most mission and cost advantage, the approval of all data management plans and subsequent consolidation plans needs to be at the DoD level. The execution of the plans should remain with the service components and agency heads.

Lastly as this committee and others look at reorganizing and restructuring acquisition, and the roles of the DCMO etc. I strongly recommend you keep an independent CIO. I do not think this position needs to be confirmed to be successful. Success is really about the relationships with the secretary, the deputy, the DCMO and the military leadership. I would look to give mission and business owners to include the CIO more decision authority with respect to final acquisition and procurements. The CIO should be constantly reaching out to industry for their thoughts and asking for industry participation in developing policy and business process. The CIO should aggressively use organizations like AFCEA to reach out to industry and should encourage military and civilian membership in these activities. This committee should actively support this behavior and continue to ask questions to insure it is happening.

Conclusion

I believe DoD recognizes the importance of creating a flexible and effective information technology management and acquisition system. I believe Industry does too and wants to be part of the solution. I also believe that the legislative branch as represented by this committee wants the same thing and the same results. This is however more about culture change than it is about just changing practices and laws. I think we have unintentionally been building for a long time a culture of distrust and one that was based on over regulation and a foundational belief that all the players needed to be protected from each other. During the second world war and the years immediately following we had a culture where people moved more freely between government and civilian work, where industry and the government cooperated better on projects and both the civilian workforce and the commercial workforce were highly valued for their expertise and dedication to mission. This period was not a panacea and there were abuses. Somewhere however the cultural cure became worse than the problem we were solving. We lost too much of the good and today too much time is spent by many groups on criticizing the civilian workforce, attacking its credibility and expertise and making the contract workforce feel less and less like full members of the team. I was quoted as the DoD CIO saying that our secret weapon was our commercial capability and our relationship with industry. I would amend that to read our secret weapon is our commercial capability, our relationship with industry and the combined efforts of the military, civilian, contractor and commercial workforce to make it all work and deliver the results. Thank you for the opportunity to testify today and I look forward to your questions.

Mr. Terry Halvorsen

Executive Vice President and Advisor Samsung Electronics of America

Currently Mr. Halvorsen is an Executive Vice President and Advisor to the CEO of Samsung Electronics Mr. JK Shin. Mr. Halvorsen retired February 28 2017 from federal service after serving almost 37 years with the DoD in uniform and as a civilian. His most recent assignment was as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen was the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provided strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions. Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

STATEMENT OF PETER LEVINE
FORMER DEPUTY CHIEF MANAGEMENT OFFICER AND
ACTING UNDER SECRETARY FOR PERSONNEL AND READINESS
DEPARTMENT OF DEFENSE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES
HEARING ON CREATING A FLEXIBLE AND EFFECTIVE INFORMATION TECHNOLOGY MANAGEMENT AND ACQUISITION SYSTEM

April 26, 2017

Chairman Stefanik, Ranking Member Langevin, and Members of the Subcommittee, thank you for this opportunity to appear before you this afternoon.

My name is Peter Levine, and in 2015 and 2016, I served in the Department of Defense, first as Deputy Chief Management Officer (DCMO) and then as Acting Under Secretary for Personnel and Readiness. Before that, I spent 28 years working for Senator Carl Levin of Michigan, the last two as Staff Director of the Senate Armed Services Committee.

The views I express are entirely my own, and should not be interpreted as reflecting any position of my new employer, the Institute for Defense Analyses (IDA). IDA is a government contractor. However, I am testifying in my individual capacity, and as such, I do not have any federal contracts or grants, or any contracts or payments from a foreign government, to report.

I understand that you have invited the three of us here in our capacity as former DoD officials to discuss the manner in which the Department organizes and manages its information technology (IT) and cyber programs and workforces. It's a big subject. Information Technology is everywhere in the Department. It's not just in our core C3I systems – our communications systems, our command and control systems, and our intelligence systems. It runs our logistics systems, our acquisition systems, our financial systems, and our HR systems. And of course it central to the operation of every one of our weapon systems.

This makes for an exceptionally complex governance problem. With regard to the acquisition of new or upgraded business systems, for example, the Chief Information Officer (CIO) has a vital role in ensuring compliance with IT architecture and cyber requirements, but others have equally important roles. The Chief Management Officer is responsible for ensuring that business case analyses have been conducted and appropriate business process reengineering will take place, while the Chief Acquisition Officer (AT&L) is responsible for ensuring the use of appropriate procurement mechanisms and providing effective oversight of contractor cost, schedule, and performance.

It would be nice to think that we could make the Department more efficient by giving all of these authorities to a single official or office, but experience shows that it is just too big of a job. When AT&L tried to run business system acquisition by itself, it lacked both expertise in business process reengineering and the authority to insist that requiring the components – their customers – get it done. When the DCMO tried to take charge, it became bogged down in technical minutiae and lost track of the big picture. I do not believe that the CIO has the expertise and authority needed to do the job by itself either.

For this reason, all three offices need to play a continuing role. The key to making this work is ensuring that each office stays in its appropriate role of providing policy guidance and oversight, rather than trying to run the programs directly out of the Office of the Secretary of Defense (OSD). Policy and oversight reviews are a lot easier to coordinate than day-to-day management decisions. If business system programs are run by program offices in the components as they should be, the CIO, the DCMO, and AT&L can all provide oversight in their appropriate lanes.

Of course, there will always be substantial overlap: a business case is likely to address many of the same issues as an acquisition plan, and an acquisition plan won't be complete unless it addresses cyber and architecture requirements. If the Department isn't careful, program offices could be whipsawed back and forth, as they have to comply with different review processes, at different times, for the same issues.

When Terry and I were the CIO and the DCMO, we had a smooth coordination process: major decisions on business systems were approved by both of our offices, as well as AT&L. However, that the process can and should be made more efficient by better sequencing the acquisition review process, the architecture review process, and the business case review process.

When I testified before this Subcommittee a year ago, I promised to take on this project. Although I left to take a new job as Acting Under Secretary for

Personnel and Readiness two weeks later, I understand that the effort culminated with the issuance of a new DoD Instruction 5000.75, which was jointly approved by the AT&L, CIO, and DCMO on February 2, 2017. I urge you and your staff to have the Department brief you on this new policy.

The effort to coordinate the positions and activities of the DCMO, the CIO, and AT&L also dovetails with the requirement that Congress established, under sections 901 and 902 of the FY 2017 NDAA, for the Department to reexamine the roles of the DCMO and the CIO.

With regard to those provisions, the Committee made the right decision in keeping the DCMO and the CIO as separate offices. When we looked at planning a merger between the two offices a year ago, we found very few areas of overlap. We were basically pasting together two organizational charts without change. The DCMO plays no role at all in IT other than business systems, and even with regard to business systems, the DCMO and the CIO have completely different areas of expertise.

The new Chief Management Officer (CMO) should maintain the role that the DCMO currently plays in reviewing investments in IT business systems. When I was DCMO I tried to focus these reviews on Return on Investment. When we make a major new business system investment, we should have a plan for turning off legacy systems and for reducing manpower requirements based on new, less manpower-intensive business processes. The new CMO will be a success if he or she can ensure not only that these plans are developed, but that they are carried out and the savings actually achieved.

Beyond that, the Department would do well to consider an additional role for the new CMO as a resource that other elements of the Department could turn to for assistance in organizational streamlining and process improvement. The DCMO engages in some of these activities now, but their effectiveness is limited by the fact that the requirements tend to be imposed from the outside. The office would get more cooperation and achieve better results if instead of seeking to impose savings initiatives on the components, its role were to assist the components in their own efficiencies efforts.

When I was serving as Acting Under Secretary for Personnel and Readiness, I asked the DCMO for assistance on process improvements and organizational streamlining on several occasions. Of course, since I was still the Senate-confirmed DCMO, they were pretty good about giving me the help that I needed.

It would require some new resources and capabilities, but the Department could really use an internal management consultant, and the new office of the CMO would be the ideal place to put it.

At the same time, it would be a mistake to give the CMO responsibility for overseeing the management of Defense Agencies like DLA, DFAS, and the Defense Health Agency, as some have suggested. If management oversight is divorced from policy responsibility, both functions are likely to be less effective. Moreover, these added responsibilities would overwhelm the resources and capabilities of the DCMO, making it unlikely that the new office would be able to serve the more important function of driving organizational improvement throughout the Department.

I urge you to consult with some of the capable career officials in the Department about these issues before you proceed. When was I was DCMO, Dave Tillotson served as my deputy; he is now acting DCMO and will undoubtedly play a key role in getting the CMO legislation off the ground. Nobody is more familiar with the office and what it is (and is not) capable of.

You have asked what the Department could do to improve its IT acquisition processes and better leverage commercial industry best practices. This issue was thoroughly explored in a March 2009 report by the Defense Science Board, which recommended the development of a separate acquisition process for IT systems. The DSB recommended a process that incorporated early and continual user involvement; multiple, rapidly executed increments or releases of capability; early, successive prototyping to support evolutionary acquisition; and a modular, open-systems approach.

Section 804 of the FY 2010 NDAA directed the Department to develop an IT acquisition policy along these lines, but I do not believe that the Department met the intention of the provision. For this reason, Section 804 of the FY 2015 NDAA directed the Department to revisit the requirement. I still believe that the DSB recommendations were sound. Sometime in the near future, the Department should have a new acquisition policy team in place; I would encourage you to take up the DSB recommendations with them and see if more progress can be made.

Finally, I would like to turn to the IT and cyber workforces. When Terry and I were in the Department, we greatly appreciated the new authority that the Department gave us for the cyber workforce in section 1107 of the FY 2016 NDAA. The Under Secretary for Personnel and Readiness teamed with the CIO and the Principal Cyber Advisor to implement this legislation. Before we left, we had an approved plan in place to establish a new personnel system that should make it easier to recruit and retain the talented personnel the Department needs to protect our information systems.

However, the new personnel system is just step one of a broader plan. It isn't enough to have the authority to hire capable people – the Department needs to know where the gaps are in its workforce and what kind of people it should hire to fill those gaps. In other words, the Department needs a strategic workforce plan for its cyber workforce. We initiated this effort last year, but we didn't get very far before the end of the Administration. I think it would be helpful for the Subcommittee to call this issue to the attention of the new team as well.

Thank you again for inviting me to testify today. I look forward to your questions.