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NOT FOR PUBLICATION UNTIL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.