[H.A.S.C. No. 115–37]

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

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS
AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

HEARING HELD
APRIL 26, 2017

U.S. GOVERNMENT PUBLISHING OFFICE
25–823 WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ELISE M. STEFANIK, New York, *Chairwoman*

BILL SHUSTER, Pennsylvania
BRAD R. WENSTRUP, Ohio
RALPH LEE ABRAHAM, Louisiana
LIZ CHENEY, Wyoming, *Vice Chair*
JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
TRENT FRANKS, Arizona
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia

JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
STEPHANIE N. MURPHY, Florida

Kevin Gates, *Professional Staff Member*
Lindsay Kavanaugh, *Professional Staff Member*
Neve Schadler, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

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

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, April 26, 2017.

The subcommittee met, pursuant to call, at 2:03 p.m., in room 2118, Rayburn House Office Building, Hon. Elise M. Stefanik (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, CHAIRWOMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. The subcommittee will come to order. I would like to welcome everyone to this hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee on the important topic of information technology [IT].

Several of us from the committee recently had a discussion with Eric Schmidt, who is the executive chairman of Alphabet, as well as the chairman of the Department of Defense [DOD] new Defense Innovation Board. That discussion was very helpful in provoking us to think about how the Department could do a better job incorporating best practices from industry. And while it is unrealistic to think that DOD will ever operate exactly like industry, it is nonetheless imperative that we achieve every ounce of efficiency out of our back office and IT operations in order to fully invest in combat capability. The challenge is finding that correct balance, and today's hearing brings us one step closer.

Information technology represents over $30 billion of the Department's total budget; however, too often it is treated as a support tool secondary to platforms, weapons, training, and the operations of the Department. But anyone who has seen U.S. forces operate over the past 25 years understands that our military advantage comes from those network systems providing the intelligence, precision strike, information fusion and warning capabilities our warfighters have come to rely on.

This committee has been focused on reforming the operations of the Department for the past 2 years, from streamlining acquisition regulations to streamlining an overly cumbersome bureaucracy. The end goal of these efforts has been to enable us to buy and develop systems with greater agility and flexibility so that state-of-the-art tools get into the hands of our warfighters faster.

I know our witnesses today will help provide us with a better framework for understanding how to think about defense management and acquisition practices for information technology as we explore the critical questions before us, such as: What are the characteristics of well-performing programs that we should focus on? What leading indicators should we be monitoring to determine if programs are going off the rails and before it is too late? And how can we better identify, encourage, and reward those program managers that are executing information technology programs well?

Let me now turn to the ranking member, Jim Langevin of Rhode Island, for any opening comments he would like to make.

Jim.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 25.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Chairwoman Stefanik, and thank you to our witnesses for being here today. I definitely look forward to hearing what you have to say, given your wealth of knowledge in this area.

So management and acquisition of information technology at the Department of Defense is one of the most challenging and pressing DOD organizational and administrative issues facing us today. For years, Congress, the executive branch, and industry have attempted to bring DOD's IT programs and processes into the 21st century. Despite attempts like the Joint Information Environment and streamlining acquisition processes, DOD's pace to improve its IT posture is not progressing with the desired speed to achieve serious efficiencies, increase security, and take advantage of enhanced capabilities that are readily available. For example, the intelligence community has developed and is using commercial cloud services, yet widespread use of cloud computing has not yet taken place at the Department.

All that said, I will be the first to acknowledge that the Department of Defense IT management, modernization, and cyber are extraordinarily complex. I will also acknowledge that Congress, in an attempt to be helpful, has taken action that has seemingly had the opposite effect.

That is why today's hearing is so important. IT management and modernization experts who served at the DOD sit before us. I look forward to their concrete recommendations for improving DOD's IT posture in an expeditious manner, and I hope they provide granularity on legislative, regulatory, and cultural barriers, like risk aversity, that are inhibiting the rapid change required. And I am certainly glad that they help us understand what is working as well as highlight the success that the Department has already had in this arena.

So with that, Madam Chair, I thank you for organizing this hearing. I thank our witnesses for being here today. And I yield back.

Ms. STEFANIK. Thank you, Jim.

Today, we welcome three distinguished witnesses, all of whom have served as senior officials within the Department of Defense, and so they not only understand the government challenges with information technology management and acquisition, but also how private sector practices can be applied or need to be avoided.

First, the Honorable Peter Levine, former Department of Defense Deputy Chief Management Officer [DCMO] and Under Secretary of Defense for Personnel and Readiness [P&R]. Next, the Honorable Terry Halvorsen, former Department of Defense Chief Information Officer [CIO] and Department of the Navy Chief Information Officer. And Mr. Ed Greer, former Deputy Assistant Secretary of Defense for Developmental Test and Evaluation [DT&E].

Welcome to all of our witnesses. I would like to remind you that your testimony will be included in the record, and we ask that you summarize key points from that testimony in 5 minutes or less for your opening statements.

And, Mr. Levine, I will start with you. The floor is yours.

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

Mr. LEVINE. Thank you. Chairwoman Stefanik, Ranking Member Langevin, and members of the subcommittee, I thank you for the opportunity to appear here this afternoon to discuss DOD's information technology management and acquisition processes. What I would like to focus on, with your permission, is DOD business systems acquisition.

For years, DOD has been trying to buy new business systems the same way that it buys weapon systems and other big ticket items, and the result has been a series of sometimes spectacular failures. The fact is that there is no such thing as a stand-alone business system and no such thing as a stand-alone business system acquisition. The DOD's business systems are interconnected not only with each other, but also with the business processes that they run.

When DOD wants to acquire a new financial management system or logistic system or HR [human resources] system, it inevitably finds links to dozens if not hundreds of other IT systems which either feed it data or rely on it for data. Each of these systems, no matter how outdated, redundant, or ineffective they may seem, has a core of devoted users who are likely to resist change.

DOD tries to ensure that change management and business process reengineering take place concurrently with new business systems acquisitions, but it has not been easy. Acquisition officials don't have the authority or expertise to require their customers to do business process reengineering when they buy new systems, and management officials responsible for those business processes have proven to be incapable of running large acquisitions.

In the last couple of years, Congress has helped this issue considerably by streamlining section 2222 of title 10, which provides the statutory requirements for DOD business systems acquisitions, and by repealing requirements for major automated information systems, or MAIS programs, that mimic the acquisition process for major weapon systems.

When I testified with Terry here last year, I promised that the Department would take advantage of the new flexibility granted by

Congress to better coordinate the roles of the DCMO, the CIO, and AT&L [Acquisition, Technology, and Logistics] in the acquisition of business systems.

Two weeks after that hearing, I left the position of DCMO to become Acting Under Secretary for P&R, but I am pleased to say that streamlining effort went on in my absence and that just a couple of months ago the Department issued a new DOD instruction addressing business systems acquisitions. This new instruction appropriately sequences for the first time decision points regarding business solutions, IT solutions, and acquisition solutions so that we don't have these redundant processes going on side by side without referencing each other, but we have a coordinated process.

This is also the first step toward building an IT-specific acquisition process as the Defense Science Board [DSB] recommended almost a decade ago. Consistent with the DSB's recommendations, the new instruction establishes a unique set of decision points for business systems acquisitions and requires prototyping and incremental delivery of capability.

I would have to say, though, that the DSB report, which is a 2009 report, recommended a unique acquisition system not just for the acquisition of business systems, but for the acquisition of all IT. It has been a disappointment for those who were here with the Congress—I was on the SASC [Senate Armed Services Committee] staff at the time that that report came out—that that still hasn't been fully implemented for IT.

Congress felt strongly enough about this that you enacted provisions on this twice, first in 2010 and then in 2015, telling the Department: Please go look at this DSB report and figure out a way to implement the kind of IT-unique acquisition system that the DSB is recommending, having looked at commercial practices, and figure out how it would best apply to the Department. I commend you to look at that report. It is still the right thing to do. It is still what the Department needs to do.

So while I think the Department has made good steps in the direction of change, there is still a long way to go. And one thing I would add before I wrap up and hand over to Terry is that the issuance of a new DOD instruction like this one I just mentioned is the beginning of a process of change, not the end of a process of change.

One thing that I have seen in the Department is it takes every bit as much effort to make sure that the instruction, the legislation, the regulation is really implemented, implemented in the spirit it was intended, as it does to enact it in the first place. So it will be up to the new team at DOD when it arrives to ensure that the new processes are appropriately implemented in practice, and in particular with regard to business systems, that the CMO [Chief Management Officer] will have to remain engaged throughout the acquisition life cycle to ensure that the Department adopts new and efficient business solutions rather than tailoring new business systems to old and inefficient processes.

With that, I thank you again for inviting me here today, and I look forward to your questions.

[The prepared statement of Mr. Levine can be found in the Appendix on page 27.]

Ms. STEFANIK. Thank you, Mr. Levine.

Mr. Halvorsen, you are recognized for 5 minutes.

STATEMENT OF HON. TERRY HALVORSEN, FORMER DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER AND DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

Mr. HALVORSEN. Madam Chairman, Ranking Member, distinguished members, thank you for the opportunity to testify today before this committee. This is an important topic, and I would like to echo much of what Peter just said. Obviously, we did testify together on this topic last year, and I did testify the last 2 years on this topic.

DOD has made progress. They continue to face critical global challenges. I do think they will meet those 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 process today, because of the current thinking, delivers legacy solutions. We really do need to think about how we talk about capabilities and not dictating a series of technical requirements that will be out [of] date the day we publish them.

DOD needs a better understanding of the commercial environment to become more effective and efficient working with industry and determining how solutions should be implemented.

With respect to business systems, DOD really needs to ask itself: Should it implement whole commercial solutions or some degree of hybrid solutions retaining some government capability?

I will echo what Peter said, that this also needs to focus on the process, and I strongly recommend that the going-in position for business solutions until proven wrong through business case analysis is that the government and DOD should be adopting commercial solutions off the shelf. The real question really is what businesses should DOD be directly in and where should it offload those businesses to the commercial sector.

Regarding systems that are more aligned with the primary mission of DOD, such as national security systems, DOD must more carefully weigh the mission risk, the mission security requirements, and since these systems are more likely to be operated by military and civilian members, DOD must really look at the workforce implications of training and sustainment.

The new, changing environment also means DOD will be requiring 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 and expand those programs. The laws we have today have been written with great intention, but they are outdated. Many of them from a financial perspective still use numbers from the 1970s. They don't make any sense, and they limit the ability for DOD and other government agencies to function correctly.

We also need to look at the way we test commercial products for acceptance and security perspective today, and I elaborate this in my written testimony. The security accreditation process is costing both the government and industry lots of money and doing a disservice to, in the case of DOD, our service members for how long it takes to get those products certified.

We insist on testing stuff that has commercially been accepted and tested in industry. We need some legislation that says: Why can't I accept that testing as the official testing? Test can the government operate it correctly, 100 percent, that testing should be included, but we really need to look at how we do the testing. That has become one of the long poles in the tent.

You have to improve efficiency. I will talk a little bit about the McKinsey report, about the 125 million. DOD definitely took that report seriously, but some of those numbers in there were not well thought out in the end. But they should be continuing to refer to that report. It does give the right topic areas that DOD should be looking at to gain more efficiencies in.

As Peter, I am happy with the DOD CIO, and the DCMO relationship. I think it is strong today, and I think it will continue to get better. That is important, because it is a combination of the process and the technology.

In the end, this is a little bit about a cultural solution more than it is laws and anything else. We need to think differently. I think we have unintentionally been building for a long time a culture of distrust and one that was based on overregulation and a foundational belief that all the players, industry, government, and academia, all needed to be protected from itself, and we have done a good job at doing that.

Somewhere we have lost what was good in the systems we had prior. I was quoted at the DOD as saying that our secret weapon was our commercial capability and our relationships 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, and I look forward to your questions.

[The prepared statement of Mr. Halvorsen can be found in the Appendix on page 36.]

Ms. STEFANIK. Thank you.

Mr. Greer, you are recognized for 5 minutes.

STATEMENT OF EDWARD GREER, FORMER DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR DEVELOPMENTAL TEST AND EVALUATION

Mr. GREER. Chairwoman Stefanik, Ranking Member Langevin, and members of the subcommittee, thank you for the opportunity to express my views this afternoon.

In 2013, this same subcommittee hosted a roundtable discussion on IT acquisition reform, and it seems like the same challenges and the same issues were discussed 3 or 4 years ago. So we do need to be mindful of what kind of progress we have made.

Today, I am going to talk about MAIS [major automated information systems] challenges, best practices, the role of developmental test and evaluation, and business systems versus tactical weapon systems.

MAIS challenges. The challenging nature of MAIS acquisition can be attributed to many factors. I will briefly discuss three.

Program complexity. Typical MAIS programs have to be integrated into multiple existing and emerging enterprises that contain a large number of government and commercial entities.

Another challenge: unstable requirements. In many cases, the changes are driven by advancements in technology, vendors updating hardware, operating system upgrades, and so on, or by changing world events.

And the third challenge: build versus buy. While many IT companies regret building enterprise software solutions because it was much more expensive than expected, there are times when custom software solutions is the right answer. A rational build-versus-buy decision starts with well-defined requirements and a quantifiable outcome.

Second, the best practices. There are many best practices within the commercial sector and within DOD. I would like to highlight just a few.

Executive leadership participation. Robust and continued senior-level attention and participation contributed significantly to the success of agile MAIS acquisition programs as documented in the DOT&E [Director for Operational Test and Evaluation] 2016 annual report. When senior leaders are on-site, they can add resources as necessary and they can also shorten the decision cycle time.

Another best practice, continuous developmental test and evaluation. The program office should have a coherent DT&E strategy to find and fix problems as each software component is developed and delivered. Deficiencies are much easier to fix before integrating into modules and components.

And the best practice of evolutionary acquisition, which is a method intended to reduce cycle time and speed the delivery of capabilities to users. Often, in an evolutionary model, the development of increments must occur in parallel to deliver capability on time.

The third topic, the role of developmental test and evaluation. Conducting DT&E in an agile environment must be done early and often. During a major weapon system development cycle, 80 percent of the test and evaluation is developmental test and evaluation.

There are DT&E organizations within the services and at OSD [Office of the Secretary of Defense]. I have worked in both. They serve a different purpose. The DT&E professionals within the services are typically funded by the program managers [PMs], whether it is acquisition programs, MAIS, or whatnot, and they are potentially subject to biased reporting due to the pressure from the PMs. I have seen it firsthand. The OSD DT&E organization is not funded by the program managers. They are mission funded and therefore independent.

And the last area to talk about is business systems versus tactical weapons systems. It is important to make a distinction between cyber and IT/IA [information assurance] policies for warfighting systems and those pertaining to business systems or corporate enablers like email, common business systems, and cloud applications. Technical laboratories 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. There is not a cookie-cutter approach.

To ensure there is an appropriate focus on the cyber systems engineering, it is now time to pair a traditional CIO function with an RDT&E [research, development, test and evaluation] warfighting system cyber assessment function, which is focused on the tactical weapon systems and RDT&E infrastructure.

That concludes my remarks, and I look forward to answering your questions.

[The prepared statement of Mr. Greer can be found in the Appendix on page 46.]

Ms. STEFANIK. Thank you, Mr. Greer.

We now turn to members' questions. My question is for all three participants in the panel today.

Industry best practice calls for the use of leading indicators as a way to measure the health and performance of a sector; however, DOD, as you know, tends to focus more on lagging indicators because they are easier to measure, but they don't do a very good job of helping decision makers decide if a program is performing well or not, at least not until it is too late.

What kinds of leading indicators should we be using to measure IT programs as well as performance of our acquisition systems? And what are the obstacles to being able to collect that sort of information currently?

Mr. HALVORSEN. One of the first things we ought to do is concentrate on money. That is what industry does. We do look at how is the money being spent, and if you find that you are starting to have undocumented rising cost, that is generally a pretty good indicator that something is wrong.

Performance is the next best thing if you look at industry, they will look at performance. And it is not the performance of how the acquisition process worked. You ask what are one of the problems. We grade the acquisition process.

Now, I am going to say everybody in this room has fault in that. I did, and so does the legislation, because it requires that I had to report on how I was doing in the process. Most acquisitions, the day they were finally declared unfit, still had green in checking the acquisition process. That doesn't make a lot of sense to me.

So why aren't we looking at performance in the field? I mean, industry, if I am going to grade it, I grade it: Did it meet the customer requirements? That ought to be the number one, and track the money. If we did those two things, we would absolutely have a much better system today. And then get out of the rules and laws that require that we have to track and produce: Is the acquisition process itself being followed? The acquisition process is part of the problem.

So I really think if we followed—you could take these templates right off industry guidelines, we are not different in that respect, and track the actual outcome performance results, not the process.

Mr. LEVINE. I think that when we look at the DOD acquisition system not just for IT but for anything, we need to recognize that we rely on our contractors for almost all the data on their performance. So we need to be careful about what kind of data we prescribe, because if we say we want more data, then we are adding a contract requirement and a new regulation to a system where we don't need a whole lot of new regulation.

I would add to what Terry said about tracking dollars, though. It is important not just to be able to track dollars, but to be able to link dollars to performance. And certainly with the acquisition system in general, I have always felt that earned value management systems are one of the most important things that we have, because they don't just track how much money you are spending, but track it against measurable milestones so you can see whether you are progressing in the way you thought that you should be progressing.

Now, some of our contractors have earned value management systems, some of them don't. It depends on whether—you know, if they are government contractors, if you are a Lockheed or a Boeing or somebody like that, you will have an earned value management system. If you are a commercial contractor, you may not have one that matches government standards. So we may need to figure out how we can work within data that is otherwise already provided and collected by commercial industry to determine these things without imposing new requirements.

Mr. GREER. Industry does a very good job at quantifying their requirements. They stay rigid with their requirements. They developed a product based on quantifiable outcomes. They also make it a priority to make sure their senior leaders are proactively engaged. They are on-site where the decision time is much shorter.

Proprietary data is an area that, as Peter mentioned, is a concern. In some instances, it is difficult to get our hands on the data, and when we do, it costs us dearly. So that is an issue.

The last one is a partnership, perhaps, an integrated product team with industry so we don't have to worry about lagging indicators. We will be right there working with the industry developing the leading indicators and monitoring the leading indicators.

Ms. STEFANIK. Thank you.

I now yield to Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair.

And I want to thank all of the witnesses for your testimony.

So to carry on on this point, in your opinion, what do you think is the single most important action both Congress and the new administration can take to enable a rapid modernization of IT? I know it is a broad question, but kind of following on with our discussion. Please give us your insights.

And then the other one, I will say, in your opinion, what cultural barriers, such as risk aversity or service preferences, exist within the Department and what recommendations do you have to overcome them?

Mr. HALVORSEN. So the first thing I would say is we need to push the authority to acquire down, and we can do that in small numbers. So, I mean, here is an interesting thing. In my previous job, I was the CIO. I had a $37 billion budget. Approved that. It is the only place in the DOD where as a single entity, I as CIO, I had to approve that budget, write that budget, yet I couldn't authorize directly a million dollars if I saw great technology to put right on the table. That doesn't seem to make a lot of sense to me. I think that is the first thing I would do.

Smaller numbers, control. Give it a limit of maybe $10 million total that the CIO could say, "Yes, that is great technology, I want it," and waive some of the requirements that an institution as big as DOD has to review every piece of that against some competition criteria. That does not make sense.

Part of the time, if I can see best practices in industry, and that is where industry is going, I ought to be able to say as the CIO, "Industry CIOs do that, they say this is where industry is going, I am making the decision," and we go. We could do that, try that, small amounts of money. I think that would really drive some rapid acquisition quickly.

The second thing, your question about what else do we need to do, I would really recommend that this committee establish a group, and I think in 90 days they could get some very good results. But stack it with both industry and military business systems owners, not just the technical guys, because in the end, back to our original question, I never had my customers, DOD, soldiers, sailors, marines, and civilians are not real shallow, and they are not real—they will tell you what the problems are really quickly in language you will get to understand quickly if you go ask them. We don't ask them enough.

And so I think that is the other problem. Let's go out and ask the customers. Bring some customers on this panel, bring some industry experts, bring some leadership, 90 days I think you could get a really good result on here are some of the specific things you could do to really get at the cultural issue, because this is cultural.

Even when it is fixed and even when we have the authority, the whole system, which includes the DOD, the way we inspect and review, and, frankly, includes the way GAO [Government Accountability Office] inspects and reviews, we are using the mindset that was 20 years old.

We have got to change that. That will take time. But I think this committee, because it has done it in the past, could establish that a committee take a review and put some things in legislation and then follow up on it with your personal attention, and that would get some good results.

Mr. LANGEVIN. Thank you.

Mr. Levine.

Mr. LEVINE. I agree with Terry, that I think that the real focus ought to be on planning and prioritization so that you are spending the money in the right place. We tend to focus in a hearing like this on what is wrong with DOD's policies and practices and how can we make things better through that and we can make things better.

But if you are really looking for how are you going to improve the IT environment at the Department of Defense, whether it is in business systems or weapon systems, the issue is, we have a lot of low-hanging fruit out there, things that need to be improved. We don't necessarily spend our money in the right places for the right priorities, and that prioritization, I think, is the number one task that we have.

Mr. GREER. In response to your first question, contracting is, in my mind, a major impediment, whether it is acquisition weapon systems or IT systems or whatnot. If you look at the entire food chain from A to Z in terms of delivering an IT agile system, it starts with the statement of work, then it goes into a do-loop in the contracting arena because of policies. It is not the executors, it is the policymakers, whether it is an OSD or the echelon command within the services on more pointed here at Congress, legislation that has been burdened on the contracting community. Conducting a zero-based review of all of the contracting policies certainly might be one approach.

I mentioned earlier about the CIO. My personal view is—and I am an engineer, I have the technical background more so than the IT side of the house—but certainly the CIO has such a broad responsibility. That is another long lead time approval cycle. It has been from my experience.

In terms of cultural barriers, a lot of the government organizations do have in-house software development teams. And sometimes they make less than informed decisions regarding whether or not they should develop in-house software solutions or go out to the commercial sector. And I believe that is a cultural issue that ought to be addressed.

Thank you.

Mr. LANGEVIN. Thank you.

I yield back. I will have additional questions if we go a second round.

Ms. STEFANIK. Mr. Scott.

Mr. SCOTT. Thank you, Madam Chair.

Gentlemen, thank you for your service.

And, Mr. Greer, you mentioned the proprietary data and how much—you said it costs us dearly, I believe is the term that you used. And regardless of what weapon system it is or IT system it is, I mean, we have seen examples in the past where we as the government, we paid for the research, we paid for the development, and then in an error in the contracting, even though we paid for all of it, some private company ends up owning that data.

I assume that we are not making that mistake anymore? Is that something that we have corrected in the contracting?

Mr. LEVINE. Congressman, I would be happy to respond to that.

Congress did change the rules on that several years ago, about 3 or 4 years ago. I was with the Senate Armed Services Committee then. But you changed the rules. In particular, there was a rule that said the way that rights and technical data work, if it is 100 percent developed through private expenditure, the private company owns it; if 100 percent developed at government expenditure, the government owns it; and if it is mixed expenditure, we get just government purpose rights.

But those rules also said you have to identify in the contract up front which data you are going to have ownership of as the government. So even if it was developed exclusively at government expense, if we failed to identify it up front, we didn't own it, and the contractor would come back and tell us, "Well, we own it now because you didn't say in the contract, so you are going to have to pay through the nose to use what you paid for in the future."

We changed the law so that it said, given that we were supposed to own it in the first place, if we failed to identify it in the contract, then the amount that we will owe you to provide us that data is the amount that it takes to produce the data. We are not going to have to pay you monopoly rights to buy it from you again. So we did make that change—or you did make that change—in the Congress a couple of years ago

Mr. SCOTT. Okay. I just know that as somebody who represents a depot, this is a problem for us in supply chain management in some of the older systems out there where we paid for the development of a product and we are having to then pay for the schematic to manufacture the part because they don't have it anymore.

Mr. LEVINE. It has been a huge problem. It should be better going forward, but of course that doesn't get us all the technical data from contracts in the past that we wrote under this old system.

Mr. SCOTT. Absolutely.

Mr. GREER. And I might add for just a couple of seconds here, even if it is just one piece of small source code within a weapon system, that will hold us hostage, and that is what is happening today. So you can have all of the lawyers get together and come up with compromises, generate legislation, but at the end of the day, the major prime contractors are still holding the government hostage.

Mr. LEVINE. The change that we made a few years ago, the change that Congress made a few years ago also attempted to address that by saying that you have to segregate the smallest piece of technical data that you actually spent your money on and isolate that and tell us how we can work around it so that you can't tell us that we have to pay for all of the technical data or rely on you for all the technical data. So there is an attempt to address that as well.

There is also currently, I believe, Congress——

Mr. SCOTT. Is that attempt effective, or do we need different language to make it more effective?

Mr. LEVINE. I believe it is effective, but it needs to be implemented and practiced over a period of time to see where the problems are. Congress has established a technical data panel to look at these issues. And I suspect that, with all due regard to my friends in the contractor community, they are going to try to reverse some of these changes. So I would urge you to be very alert to the recommendations of that panel and make sure that there isn't backsliding on those issues that you are concerned about.

Mr. SCOTT. If you would provide additional information to us on that, I would be very appreciative of it.

[The information referred to can be found in the Appendix on page 65.]

Mr. SCOTT. Gentlemen, it took the Army 10 years to decide on which new pistol they were going to use. I don't know if it was because of the law, the bureaucracy. But the iPhone came about about 10 years ago, the original iPhone. Flip phones were still popular back then. With technology there is certainly a timeline that we cannot operate in. Is it the law or is it the bureaucracy that needs to be changed?

Mr. HALVORSEN. Yes. Some of the laws still need to be restructured on that. There are some things that still treat off-the-shelf technology like a weapon system. We have got to stop doing it. We really do need to say off-the-shelf technology, commoditized technology, does not need to be treated like a weapon system, but then we have got to get through the bureaucracy.

Mr. SCOTT. Do you have any specific language that you could suggest, provide for our committee?

Mr. HALVORSEN. I will shoot you—yes, sir, I will do that.

[The information referred to can be found in the Appendix on page 65.]

Mr. SCOTT. I would appreciate that.

Madam Chair, I am down to about 20 seconds. I will yield the remainder of the time.

Ms. STEFANIK. Thank you.

Ms. Gabbard.

Ms. GABBARD. Thank you. Thank you, gentlemen.

I wonder if you can comment on what impact, if any, you think that Buy America provisions have on obtaining the best possible technology.

Mr. LEVINE. It has always been a concern in the acquisition community that if you have Buy American provisions that become too restrictive, it will limit our ability to get the best weapon systems for our warfighters.

The acquisition community always has a bias toward getting the best possible for the best possible price. As long as the Buy American provisions are in the area where they are now, the acquisition community has been able to work around them; but there is concern if you ramp it up too much, it might impede their ability to do what they need to do.

Mr. HALVORSEN. I will echo what Peter said. There are some cases where, unfortunately, you can't Buy American in much of the technical side.

I think the other thing we want to talk about here is that part of the Buy American also addresses some security concerns. What we really ought to be looking at, and this is maybe a bad way to say it is, where don't we want to buy? Very candidly, I don't want to buy stuff, I didn't want to in my last job, that was manufactured in certain nation-states. I think that needs to be more of the focus here.

And what I would say, the words here, we might in the technology area want to change that to Buy American and allied. The other problem we have in the technology communications business is we don't go to war alone, the DOD does not, and we need to be able to communicate effectively with allies. So that is something we have really got to make sure that agency by agency we don't put out Buy American rules that would preclude us from then communicating very well.

I also think there is great benefit if we focus this around Buy American and allied and how we could do some better arrangements for everybody in terms of cost, delivery times, and production.

Mr. GREER. Outsourcing integrated circuitry is a concern that I have had for quite a while from a cybersecurity and trusted systems point of view. We are second to none when it comes to manufacturing integrated circuitry and mass producing or producing small quantities. But the outsourcing of the large quantities is something that we all have to be concerned about only from malware perspective and other reasons.

Mr. LEVINE. I would echo what Terry said, though, that there is a difference between worrying about your supply chain vulnerability, where you are worried about countries of concern, and what you do with Buy American, which is to say that all countries are off the table.

Ms. GABBARD. Right. With regard to, you know, you mentioning Buy American and allied, what are some of the approaches that our allies are taking with regard to some of these challenges with workforce and improving their own speed of acquisition? Are there lessons we can learn?

Mr. HALVORSEN. There are. So an example, like the U.K. [United Kingdom] and Australia, their CIOs are permitted up to I think it is 10 million pounds to look at existing technology and say: Hey, this would fit. Let's buy a small amount of it. Let's test it. Let's put a performance objective around it and track the cost performance to Peter's.

They have to have those, but they can make the commitments right on spot to do that. That makes them a lot more attractive to new technology, because if you are a startup new technology, you are on a 6-month funding cycle. If you don't get that 6 months, you are walking away. You have to. So that is something we could do.

They also have changed their workforce construction. My counterpart in the CIO at the U.K. until just recently—he retired March 31—was what was they called a crown contractor. To get around the pay gap issues, they were able to negotiate not quite a civilian salary, but better than the government salary, and they were able to hire him, give him full civilian authority to make the decisions. But he came out of both industry and the military, he had been a retired two-star, he did 5 years with British Telecom. I think that is kind of what we want to be able to bring into the government, people who have both government and industry experience. You need both to succeed at the top level.

The Canadians are doing the same thing. And the way they are doing their supply chain also, those nations which are in Five Eye,† and there is only one nation that doesn't have this authority, and it is probably the leading nation in the Five Eye community, which would be us, they are allowed to look at a computer, say, check a supply chain.

So there are some U.S. companies that I wouldn't want to buy from because when you look at their components, they are all from countries I don't want. That is the most important thing. So they are allowed to say: Hey, if that is a U.K. company, but all of their parts are sourced out of a place we don't like, well, then we are going to go buy an allied company. We ought to have that kind of flexibility restriction to make those decisions when it is in the best interest of defense.

Ms. GABBARD. Thank you.

Mr. LEVINE. One thing that the last administration did, if we want to look to a domestic example rather than overseas, is to have teams of IT experts who came in from Silicon Valley to help DOD and other agencies look at specific problems and identify solutions. So they would identify commercial solutions. Sometimes they would write software themselves to address it.

I believe that the new administration is considering similar kinds of steps. But that gets you ahead of a cycle. You know, you don't have to take 5 years——

Ms. STEFANIK. We are running out of time, Mr. Levine.

Mr. LEVINE. Thank you.

Ms. STEFANIK. Dr. Abraham.

Dr. ABRAHAM. Thank you, Madam Chair.

Gentlemen, thank you for your direct testimony. It is appreciated. There was some great solutions or possible solutions mentioned in you-all's testimony. And as we know, industry has to make a profit. They have a board of directors that they report to. And, unfortunately, in the DOD or any bureaucracy, that word is not even in their dictionary. And, you know, that is a problem.

Again, it all comes down to accountability. And when you have a budget, Mr. Halvorsen, of $37 billion or whatever and you can't write a check for something that you see, it is just idiotcracy at its finest.

So it is a national security issue. And I understand we have to maintain qualitative and quantitative advantage over our enemies. But for these programs that we could just literally pick off the shelf and save literally hundreds of millions of dollars, it just—it bodes poorly for us in the government for us to allow this to happen.

Are there any examples, can you give me some examples of some successful industry partnerships?

Mr. HALVORSEN. Well, you know, I hesitate, because some of those I was directly involved in. But I will tell you, the Microsoft partnership with DOD, the ability that Microsoft let us, looking at the license agreement, let me at that point make the decision that the entire Department could go to Windows 10, get to a single oper-

† "Five Eyes" (or FVEY), refers to an intelligence alliance involving Australia, Canada, New Zealand, the United Kingdom, and the United States.

ating system, without having to renegotiate the current contract, that was a partnership with Microsoft.

That what they saw down the road, and I think this is going to happen if the government goes to Windows 10, to one of the Representative's comments earlier, it will actually facilitate then the follow-on move, which I know is being planned, into the 365 and public cloud domain.

So Microsoft saw that as investment. It was a good, open dialogue. That was very good.

Again, I hate to say it, I will go on the record, I am now working for Samsung, but one of the things that happened early, we put out a capability statement that said we needed a secure smartphone. That is all we put out. Samsung came in. We worked with them. We actually co-developed what today they feel is their KNOX security system. It kept everybody's prices low. We were able to field that at the secret and now top secret level in less than 24 months. The products, which are rare in my history, were delivered on time and at cost. And in the end, they actually cost less than we thought they would.

Dr. ABRAHAM. That leads somewhat to the second question I have. Mr. Scott referenced the iPhone 10 years or less. And, again, these products are being developed by a different generation of entrepreneurs, engineers, IT people. What are we doing to attract some millennials into the fold?

Mr. HALVORSEN. Not enough. We are going to have to address a couple things on that. One of them is the pay gap. I will tell you, I lost my director of security. You know, he went and he quadrupled his salary after spending, you know, 32 years serving the government. Good.

That is one thing we are going to have to address. But we are also going to have to address some of the other things that the millennials want, which is they want their technology.

One of the things that when I went in my old job and now in my new job, I talk to millennials, "Why don't you look at DOD?" "Well, because they will take my phones away. I won't be able to do the things I want."

Now, that is not true as much anymore. We are using multifactor phones, those type of things. But there is the perception that the government lags greatly in the ability to be flexible in the workplace.

We have got to get that message out. The rules are there. I mean, the laws are there. I mean, I could let my people telework. I could do those things. It just wasn't the way we thought. That is a cultural issue. The laws are there to make that happen.

That is something that maybe this committee and other committees ought to be asking some questions about what are we doing on the millennials, what are we doing to be more flexible in the workplace? There are some good answers to that, but that needs to be the holistic plan, not just individual efforts.

Dr. ABRAHAM. A minute left. Mr. Levine.

Mr. LEVINE. If I could just add one thing to that. We don't take advantage enough of the things that we do have to offer. I think that the most attractive thing for the Department of Defense for people who work there is the mission and the feeling of commitment to the mission and that they can make a difference. And I think that we don't take enough advantage of that. We don't sell that well enough. When we treat civil servants as bureaucrats who are just too much, there are too many of them, we need to get them out of the way, we need to fire them and cut their pay, it doesn't create the image that people want to see of themselves. And we need to do a better job of selling the mission to get the kind of people we want.

Dr. ABRAHAM. Very good.

Mr. Greer.

Mr. GREER. And just one or two points here. In the IT community, I believe that we have to raise the level of our professional series. We have a lot of nonprofessional IT specialists, and they serve a very good purpose, but where we are today, what the cyber vulnerabilities and resiliency challenges, I think making sure that we hire enough professional series in the IT community is important. And it is not necessarily the pay that is attracting, like Peter said, it is the quality of work for these millennials.

Dr. ABRAHAM. Thank you, gentlemen.

I yield back.

Ms. STEFANIK. Mr. Larsen.

Mr. LARSEN. Thank you, Madam Chair.

Mr. Greer, can I talk a little bit about your build-versus-buy conundrum in your testimony, in your written testimony? I am sorry for being late, you may have addressed this. But I wanted to ask you in your experience on this build-versus-buy tension generally are there some criteria that we should be thinking about where there is a leverage point within the DOD where they ought to build versus they ought to buy in general?

Mr. GREER. That is a difficult question to answer in a short period of time, mainly because there is a hybrid solution. There are a lot of commercial software packages like SAP that we do purchase, but we use government people to program it and code the SAP system. And so that is always an issue.

Mr. LARSEN. Sorry. Mr. Halvorsen looks like he is excited to answer too. But go ahead.

Mr. GREER. Well, I am just expressing my views.

Mr. LARSEN. That is great.

Mr. GREER. Okay. And this is why——

Mr. LARSEN. So then continue.

Mr. GREER. But in terms of having firm requirements and quantifiable outcomes and making that make-buy decision, it gets difficult within the government, mainly because of cultural issues. There are a lot of software programmers in the government, and they inherently lean in the in-house solution side.

Mr. LARSEN. So let me ask you this then. Are there specific build-versus-buy decisions on cloud computing? Is that treated differently than, say, operational software like on the Microsoft decision?

Mr. HALVORSEN. It should be, but it is generally not the culture. But I want to be very clear on this: If you could buy it, buy it. I did not find that to be as difficult for anything that wasn't a weapon systems as [inaudible]. If you can buy it, we should buy that, and we should put—and we really did try to do this.

I mean, one of the plaques over at my desk was "customization bad." You should fight every attempt we take to customize that software off the shelf, because every time we do it, it is a lifelong contract for contractors without much gain. Our business processing systems, back to Peter's point, don't differ that much from the best in industry. They shouldn't, if they do.

So one of the first criteria is, if it is a business system, you should have to come in with a different business case that says why I am not buying that solution, why am I building any specific software.

It is getting that way for many communication systems, because we are using off-the-shelf communication. If it is off the shelf, really consider why you need to put something extra. And in the communications it might be for cybersecurity, but I have found if I go to industry, when I did that, if I told them I wanted that extra, most of the time they were happy to put it in, and most of the time they carried that in their commercial product because it was going to sell more as security becomes more important.

Mr. LEVINE. The track record of the Department is, if we are buying a commercial-type business system, if we start tailoring it, we end up spending more money on the tailoring than we spent on the system in the first place. It just doesn't make sense to do anything unique unless you absolutely have to.

Mr. LARSEN. I am sure if we went back to the first hearing that I attended on this issue when I was first elected in 2001 a lot of the answers would be the same.

On the build versus buy then does that principle, can that principle apply to the people? For instance, in Washington State, we have the example of the National Guard working with private sector and public sector folks on cybersecurity and doing red teaming and doing some mapping out of how to approach defense. And some of these folks are reservists and they are trying to attract folks in for 2 weeks a year, two weekends a month, in a sense buying people as opposed to building them internally. Does that model work in terms of the IT personnel acquisition side, if you are acquiring people?

Mr. HALVORSEN. It certainly needs to be part of your plan. It can't fill all the balance. And there are some security issues that you might not want to put everybody that way. But absolutely we need to be taking advantage of that.

If you look at our last sets of operations, you look at the Reserves we put on board, many of them were with those technical skill sets. As the CIO when I was there, I would reach out and bring Reserves on who were working for Google, working for whatever big company. And it is actually part of the deal, I will give DOD great credit, they actually have that in their plan.

Continuing that into other areas I think makes sense with caution. It is not as easy to do that with people as it is with software, but it is something that we certainly ought to be looking at.

Mr. GREER. Contractor support is an area that we need to leverage even more. There is always a need for inherently governmental personnel to be able to represent the government. But I think we can leverage more on the contractor support side, especially as your workload goes up and down. You are able to make adjustments much more quicker.

Mr. LARSEN. Yeah. Thank you.

Ms. STEFANIK. Thank you very much to each of our three panelists, Mr. Levine, Mr. Halvorsen, and Mr. Greer. And thank you to the members for their thoughtful questions. This is a critical issue that falls under this subcommittee's jurisdiction that we will continue to focus on as we prepare and draft this year's NDAA [National Defense Authorization Act], and we look forward to continuing to engage with you to get your suggestions.

Thank you very much. This hearing is adjourned.

[Whereupon, at 2:57 p.m., the subcommittee was adjourned.]

APPENDIX

April 26, 2017

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 26, 2017

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee
Creating a Flexible and Effective Information Technology Management and Acquisition System: Elements for Success in a Rapidly Changing Landscape

April 26, 2017

The subcommittee will come to order.

I'd like to welcome everyone to this hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee on the important topic of Information Technology.

Several of us from the committee recently had a discussion with Eric Schmidt, who is the Executive Chairman of Alphabet, as well as the chairman of the Department of Defense's new Defense Innovation Board. That discussion was very helpful in provoking me to think about how the Department could do a better job incorporating best practices from industry. While it is unrealistic to think the Defense Department will ever operate exactly like industry, it is nonetheless imperative that we achieve every ounce of efficiency out of our back office and IT operations in order to fully invest in combat capability. The challenge is finding that correct balance, and today's hearing brings us one step closer.

Information Technology represents over $30 billion of the Department's total budget; however, too often it is treated as a support tool, secondary to platforms, weapons, training, and operations of the Department. But anyone who has seen U.S. forces operate over the past 25 years understands that our military advantage comes from those networked systems providing the Intelligence, precision-strike, information fusion, and warning capabilities our warfighters have come to rely on.

This committee has been focused on reforming the operations of the Department for the past two years, from streamlining acquisition regulations to streamlining an overly cumbersome bureaucracy. The end goal of these efforts has been to enable us to buy and develop systems with greater agility and flexibility so that state of the art tools get into the hands of our warfighters faster.

I know our witnesses today will help provide us with a better framework for understanding how to think about defense management and acquisition practices for information technology as we explore the critical questions before us, such as:

> What are the characteristics of well performing programs that we should focus on?

What leading indicators should we be monitoring to determine if programs are going off the rails, and before it is too late?

How can we better identify, encourage, and reward those program managers that are executing information technology programs well?

Let me now turn to Ranking Member Jim Langevin of Rhode Island for any opening comments he'd like to make.

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.

PETER LEVINE

Work Experience:

March 2017 – Present: *Senior Fellow, Institute for Defense Analyses*

2016 – 2017: *Acting Under Secretary of Defense for Personnel and Readiness*

2015 – 2016: *Deputy Chief Management Officer, Department of Defense*

2013 – 2015: *Staff Director, Senate Armed Services Committee*

2001 – 2002, 2007 – 2012: *General Counsel, Senate Armed Services Committee*

1996 – 2001, 2003 – 2006: *Minority Counsel, Senate Armed Services Committee*

1995 – 1996: *Counsel, Office of Senator Carl Levin (D-MI)*

1987 – 1994: *Counsel, Subcommittee on Oversight of Government Management, Senate Committee on Governmental Affairs*

1983 – 1987: *Associate, Crowell and Moring*

Education:

J.D., *magna cum laude*, *Harvard Law School,* 1983

A.B., *summa cum laude*, *Harvard College,* 1979

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Peter Levine

Capacity in which appearing: (check one)

☒ Individual

□ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: None

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None			

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None			

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None			

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None			

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None			

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None			

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.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name:___Terry A. Halvorsen______
____

Capacity in which appearing: (check one)

__x_Individual

___Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: ____

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NONE			

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
none			

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
none			

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
none			

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
none			

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
none			

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.

Ed Greer

Mr. Greer is the President of Greer Consulting, LLC. Greer Consulting, LLC facilitates executive consulting services between Department of Defense organizations and Prime Contractors/Vendors. This includes providing executive consulting services in a variety of specialty areas. Greer Consulting provides program management, engineering, DoD acquisition consulting services to organizations within and outside of DoD.

Mr. Greer was the Chief Operating Officer for The MIL Corporation from February 2013 through October 2015 and reported directly to the CEO. In his capacity as COO, Mr. Greer was responsible for the company's day-to-day operating activities of six business sector consisting of 12 VP's, including in excess of $100M in revenue; expense, cost and margin control; and monthly, quarterly and annual financial goal management. He directed the company operations to meet budget and over 600 personnel. Mr. Greer was responsible for the short-term and long-range planning and budget development to support strategic business goals. He established the performance goals, allocate resources, and assess policies for senior management. He demonstrated successful execution of business strategies for company products and services.

Mr. Greer is the former Deputy Assistant Secretary of Defense for Developmental Test and Evaluation. He served as the principal advisor on developmental test and evaluation (DT&E) to the Secretary of Defense (SECDEF) and the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)). Sworn in March 15, 2010, Mr. Greer initiated the rebuilding of DT&E as its first Deputy Assistant Secretary since its inception under the Weapon System Acquisition Reform Act of 2009. Mr. Greer was responsible for DT&E policy and guidance in support of the acquisition of major Department of Defense (DoD) weapon systems. Mr. Greer also served concurrently as Director, Test Resource Management Center (TRMC). In this role, he advised the USD (AT&L) on matters pertaining to strategic planning and oversight of the DOD's Major Range and Test Facility Base, the nation's critical range infrastructure for conducting effective test and evaluation (T&E) of major weapon systems. Other significant duties include reviewing and improving the organization and capabilities of the military departments with respect to DT&E and providing advocacy, oversight, and guidance to elements of the acquisition workforce responsible for DT&E. Mr. Greer served on the Defense Acquisition Board. Additionally, the Director, TRMC reviewed and certified proposed T&E budgets of Military Departments and Defense Agencies, administered the Central Test and Evaluation Investment Program (CTEIP), and had oversight responsibilities of the DoD program for T&E Science and Technology.

Prior to his political appointment and since 2002, Mr. Greer served as the Deputy Assistant Commander for Test and Evaluation, Naval Air Systems Command, and Executive Director, Naval Air Warfare Center Aircraft Division (NAWCAD) (SES Tier III), Patuxent River, MD. As the senior civilian for Naval Aviation Test and Evaluation, he was responsible for planning, executing, analyzing, and reporting of all Naval Aviation test and evaluation. As Executive Director, NAWCAD, he ensured that NAWCAD technical, business, and financial objectives were met across a workforce of 14,400 and a total operating budget of over $4 billion. As Executive Director for NAWCAD, Mr. Greer is responsible for ensuring that NAWCAD technical, business and financial objectives were met. In his role as Deputy Assistant Commander for Test and Evaluation, Mr. Greer was responsible for the appropriate implementation of policy and guidance on test and evaluation matters emanating from the Office of the NAVAIR Commander and Assistant Commanders.

In 1998, Mr. Greer joined the Senior Executive Service as Director of the Atlantic Ranges and Facilities, NAWCAD, responsible for all facets relating to the development, maintenance, and operation of the open-air range and installed systems test facility components of the Navy's principal Air Combat Systems test activity. ATR controls fully-instrumented and integrated test ranges that provide full-service support for cradle-to-grave testing. Airspace and surface target areas are used for test and evaluation of aircraft and for warfighter training missions. In addition to radar and optical tracking systems, fixed and mobile assets provide the necessary capabilities for diverse testing and training scenarios.

Mr. Greer represented the Navy on the 2007 Defense Science Board Task Force on Developmental Test and Evaluation. Mr. Greer is the current and past President of the Southern Maryland Chapter of the International Test and Evaluation Association (ITEA). He also serves on the National Board Of Directors for ITEA. He earned his Bachelor of Science Degree in Electrical Engineering from the University of Maryland, College Park, and received a Master of Science Degree in Management from the Florida Institute of Technology. He is a graduate of the Defense Systems Management College and of the Senior Executive Management Development Program. Mr. Greer is the NDIA 2013 recipient of the Walter W. Hollis Award for Lifetime Achievement in Defense Test and Evaluation. Mr. Greer is married to Ms. Phyllis Greer. Ed and Phyllis have two children and four grandchildren.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Edward Greer

Capacity in which appearing: (check one)

☒ Individual

□ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: ______________________

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None	NA	NA	None

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None	NA	NA	None

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
None	NA	NA	None

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None	None	N/A	N/A

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None	None	N/A	N/A

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
None	None	N/A	N/A

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

April 26, 2017

RESPONSES TO QUESTIONS SUBMITTED BY MR. SCOTT

Mr. LEVINE. The statutory provision to which I referred in my testimony is section 815 of the National Defense Authorization Act for Fiscal Year 2012. As I indicated, this provision:

- Ensures that DOD may require the delivery of data generated in the performance of a contract that is necessary for the purpose of reprocurement, sustainment, modification or upgrade, even if such delivery was not required by the original contract. In exchange for the delivery of the data (which was generated at government expense) the government is required to compensate the contractor only for reasonable costs incurred to covert and deliver the data in the appropriate form.
- Requires the contractor to provide technical data "is necessary for the segregation of an item or process from, or the reintegration of that item" with the rest of the system. In other words, if a contractor wants to withhold data on a widget that was developed at contractor expense, it has to tell DOD how to work around the widget, so that the rest of the technical data, which DOD owns, won't be useless. Since I am no longer with the Department, I am unable to give a report on the extent to which this provision has been successfully implemented. However, section 813(b) of the National Defense Authorization Act for Fiscal Year 2016 establishes a Government-Industry Advisory Panel to review statutory requirements regarding technical data rights. Some may seek to use this panel to unwind the 2012 reforms. [See page 13.]

Mr. HALVORSEN. Language that stresses DOD should use commercial business case analysis to include review of DOD business process when procuring what is clearly a commercial solution to include hardware, software and IT service contracts. Something like the following:

"DOD will apply commercial best practices when conducting business process and detailed market analysis when procuring readily available IT hardware software and services in support of or in replacing business systems. If DOD can demonstrate through business intelligence and analysis a clear product/service leader(s) in a specific area DOD can pursue sole source or limited partnership procurements. These facts can include the ability to support a large enterprise like DOD, similar to how other large commercial companies develop procurement partnerships.

An example of this would be using the MICROSOFT based Services Cloud supported by MICROSOFT 365 and Azure. This is the leading cloud solution for the fortune 500 and clearly dominates the market and would be considered a best of breed solution. If DOD can make this case it should be allowed to by-pass current acquisition rules and go direct to procuring a best of breed solution, negotiating and spending time on obtaining the best value (pricing and performance) instead of defending and deliberating on multiple of solutions. This doesn't mean the MICRSOFT would be the guaranteed provider, it does mean that MICROSOFT products/services would be the used to form the service cloud architecture and operating system.

I want to make it clear I am not a MICROSOFT employee and receive no compensation from MICROSOFT for these recommendations. My current employer Samsung receives no direct benefit as a result of these recommendations. These recommendations are aligned with statements and testimony I made as the DOD CIO. I use MICROSOFT as it is the most compelling example and in my opinion moving to the cloud is a necessary and critical step to improving DOD security, greatly improving productivity and saving dollars.

With respect to all of the responses I have provided to the Questions for the record, they represent my personal opinions and beliefs and are in my own words. I am currently an employee of Samsung Electronics of America. The responses I have provided have not been endorsed, constrained of approved by Samsung Electronics of America or any other entity. [See page 13.]

Mr. GREER. There are a few acquisition programs that have had difficulty obtaining data/software/interface rights by prime contractors. Despite language that stipulates the Government has purpose rights if Government funds are spent to develop a deliverable, industry still presses back when the Government attempts to exert its rights. Industry is interpreting that if a deliverable contains their proprietary information or reveals the workings of what they claim as their intellectual property (IP), they may limit access to it. Additionally, for software intensive deliverables, industry has started 'bundling' IP with the deliverable to the government, and claiming the government has less than purpose rights to the overall product. This is leading to complex licensing issues for deliverables the Government should have purpose rights to. This has happened on F–35 as well as many other programs. Language should be clarified to state the Government has no less than purpose rights to the code segments (source and executable) and interfaces used in an overarching deliverable funded in any part by the Government.

From an acquisition oversight perspective, with the KC–46A program, Boeing made it clear during contract negotiations that they would not use Boeing 767 reliability data to meet the government requirement. That sounded like the right approach at the time given the KC–46A differences in configuration, but in practice it meant that Boeing will not share any reliability test data from their Boeing 767–2C (the provisioned freighter) either from Boeing DT&E or FAA Amended Type Certificate (ATC) certification testing. Although we do get some anecdotal failure data from these flights in which the government participates, it is purely word of mouth from those attending the briefings or flying the tests. We do have reliability data from flights, which are used to meet contract specifications. The net result is that we have very incomplete reliability data. The DASD (DT&E)'s official MS C assessment concluded, "As a result, the Lead Developmental Test Organization (LDTO) used data only from flights in which the Air Force participated to estimate the system's progress against the reliability growth curve, which presents an incomplete picture of the system's reliability."

Also, the tension over Boeing 767 proprietary data makes it difficult and time-consuming to obtain test data that the government feels is necessary to evaluate the system under test when that data comes from Boeing DT&E or ATC testing. When it was in Boeing's interest to share more quickly and "freely" during the boom issues prior to MS C, the data flowed more freely. Most of the time, it can take weeks or longer to get the data the government believes that it needs.

To the best of my knowledge, Boeing has provided (or will provide) the data required for gov't spec verification, though it has been a painful process that runs through Boeing Commercial Aircraft (BCA) because they technically own the aircraft during EMD. As best as I can tell, we will never get the B–757–2C reliability data from Boeing internal and ATC testing. I sat in on a meeting between BCA, Boeing Defense, and the program office and can relate that BCA was surprised that we wanted the requested data. In the commercial world, BCA simply delivers aircraft that meet the customers' specifications. The commercial customers don't care how the aircraft was built and tested. Maybe part of this equation involves the gov't rethinking what data we really need, which drives back to the acquisition process and how the gov't buys stuff.

The Department of Defense has tremendous capabilities to modify legacy weapon systems if full data rights were available. Government personnel could perform the Non Recurring Engineering development for small to medium upgrades in-house saving millions of taxpayer's dollars. For example, The NAVAIRSYSCOM's Naval Air Warfare Center, Aircraft Center has an Aircraft Prototyping Facility for modifying DOD weapon systems. The DOD should be taking advantage of facilities like this as opposed to sole sourcing modifications to the prime contractors. The Army has similar modification facilities.

The lack of government access to design data related to items (platforms, systems, components, hardware, software, etc.) already purchased by the government has been and continues to be a major cost driver for any subsequent upgrade done to these items during their service lifetime. Although IT systems are certainly a critical element of this problem, the problem is pervasive. Asserted data rights involving organic government prototype development programs costs time and money at a minimum and, in the extreme, can simply stop an effort.

This problem is further compounded on a broad scale by government laboratories and field activities that are reticent to reverse-engineer the data out of the government-owned items due to ultra-conservative legal advice predicting litigation as well as fear of Congressional inquiries. This is in stark contrast to the private sector where backing data out of owned items through reverse engineering is commonplace, protected by legal precedent and an essential element of one company modifying or upgrading another's product. Reverse engineering is not always practical but it is often an effective work-around particularly in situations where the prime contractor no longer produces the item.

The complexity in system acquisitions and understanding intellectual property rights in Modeling & Simulation (M&S) acquisitions, requires a clear understanding from Program Managers, System Engineers, and Procuring Contracting Officers to

M&S Integrated Product Teams of the Government's license rights in intellectual property comprised of technical data (e.g. technical packages and other information relating to the developed product's design, configuration, or to operation, maintenance, installation, or training data) and computer software (e.g. executable code, source code, code listings, algorithms, formulae, design details). The lack of clear understanding among various Program Offices highlights the need for specific guidelines for contracting for open M&S systems and the data rights required. Open System Architecture is a key pillar of the Department of Defense's Better Buying Power (BBP) initiative to implement best practices to strengthen the Defense Department's buying power, improve industry productivity, and provide an affordable, value-added military capability to the Warfighter. [See page 13.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

April 26, 2017

QUESTIONS SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. In addition to investments in IT to improve its use of data to inform decision-making, DOD also needs to address the cultural barriers that hinder effective information sharing throughout the Department. For example, RAND found in 2015 that "institutional structure and bureaucratic incentives to restrict data access are exacerbated by policy and guidance to protect information. The result is a strong conservative bias in labeling and a reluctance to share." In your opinion, what are the initial steps that the Department needs to take to address these cultural barriers, and who should be responsible for leading this effort?

Mr. LEVINE. There are both good and bad reasons for restricting data. Some restrictions on access to data are appropriate to safeguard classified and sensitive unclassified data from unauthorized disclosure. Widespread dissemination of such data to those without a need to know, even within the Department, could lead to compromise.

Other restrictions appear to be imposed for more parochial reasons: program managers, PEOs, and component acquisition executives may seek to retain control over their programs by controlling the flow of data to Comptrollers, to CAPE, and even to others in their chain of command.

Before I left the Department, DOD was seeking to address this issue through a coordinated "big data" project. The objective of the project was to identify data elements are needed by users at all levels of the acquisition system, as well as by outside stakeholders in the Department, and standardize that data to increase transparency. If successful, this project should help address the problem identified by the RAND review.

Ms. STEFANIK. In addition to investments in IT to improve its use of data to inform decision-making, DOD also needs to address the cultural barriers that hinder effective information sharing throughout the Department. For example, RAND found in 2015 that "institutional structure and bureaucratic incentives to restrict data access are exacerbated by policy and guidance to protect information. The result is a strong conservative bias in labeling and a reluctance to share." In your opinion, what are the initial steps that the Department needs to take to address these cultural barriers, and who should be responsible for leading this effort?

Mr. HALVORSEN. Representative, when I was the DOD CIO and I believe it is still true, that DOD is making good strides in this area and this is currently being led by the Deputy Chief Management Officer and fully supported by the SD and DSD. I would encourage Congress and DOD to work with industry to look at the current laws and rules that restrict government employee direct interaction with industry and restrict the sharing of information with industry. Industry should also be challenged to share data more openly with DOD and the government in general. One specific recommendation I would make is for DOD supported by legislation to include industry more directly in developing policy/instructions with respect to business systems. While DOD CIO I explicitly involved industry in developing the cloud policy and security guidelines. This was challenged by many groups inside and out of DOD but the resultant document was well received and is allowing in this area much better communications between industry and government.

Ms. STEFANIK. What is the DOD role as it relates to developmental test and evaluation for IT systems that are predominantly commercially based and where DOD is integrating, but not actually developing new capability? Is there a particular balance in developmental testing between what DOD is responsible for and what industry should be responsible for that can reduce duplication in effort, cost and schedule performance?

Mr. GREER. Yes, there is a balance between what testing DOD is responsible for and what performance certifications can be provided by industry and accepted by the test community. DOD tests are conducted in mission relevant environments to ensure overall capability is effective and suitable and to assess resilience to CYBER threats. Component level testing of individual COTS hardware components may often be conducted at the supplier level and accepted by the Government.

DOD is in the process of acquiring multiple defense business systems (DBS) based upon commercial enterprise resource planning (ERP) systems. The first priority is to conduct business process re-engineering to try to change DOD processes to fit the commercially offered systems and minimize customization of the ERP. In most cases, the unique nature of the DOD identifies gaps between the DOD process and the ERP capabilities. In this case development of special report, interface, conversion, extension, form, and workflow (RICE–FW) software objects are required.

In these cases, developmental testing of the DBS focuses on the RICE–FW and integration into the DOD facilities and networks rather than the basic capabilities that are proven by use in industry. Mission-oriented developmental testing using actual users performing mission tasks in a test environment allows integrated testing with the operational testers, early identification of human factors integration problems, and identification of software defects in the RICE–FW objects with sufficient time for correction prior to operational testing.

Additionally, DOD's roles in developmental test and evaluation of IT systems integration are in the realm of cybersecurity. DOD must ensure that the new IT system does not introduce a vulnerability to the DOD network and that the combined cyber defenses are integrated. Just because a commercially based IT capability meets industry, it does not mean that it is secure. The IT capability may meet standards of performance (certification) but it must be tested for effectiveness (penetration).

DOD should be responsible for cybersecurity testing and the vendor must correct those deficiencies. This should be in a developmental test environment that allows time for the vendor to make corrections. After corrections are made, the IT capability is ready for operational cybersecurity testing. Cybersecurity is an area where the test-fix-test methodology is still relevant.

Ms. STEFANIK. In addition to investments in IT to improve its use of data to inform decision-making, DOD also needs to address the cultural barriers that hinder effective information sharing throughout the Department. For example, RAND found in 2015 that "institutional structure and bureaucratic incentives to restrict data access are exacerbated by policy and guidance to protect information. The result is a strong conservative bias in labeling and a reluctance to share." In your opinion, what are the initial steps that the Department needs to take to address these cultural barriers, and who should be responsible for leading this effort?

Mr. GREER. Cultural barriers are often difficult to overcome. A good method of breaking down barriers is to encourage more transparency with regard to ongoing developmental efforts. Sharing visibility into IT related projects, investments, and infrastructure may help increase re-use of development that would otherwise be unknown across organizational boundaries, reducing duplication of effort. Establishing a community of interest (COI) for IT related investments may be beneficial in fostering this kind of exchange of ideas and information. This is a leadership challenge, as is all cultural change. At a minimum, the Director, Developmental Test and Evaluation should get back statutory authority for oversight of ACAT ID and MAIS programs and to ensure access to all data in DOD and have direct access to the Defense Acquisition Executive with regard to his independent assessments of system performance and issues regarding his ability to make those assessments in time to effectively inform decisions.

I believe that an organization such as the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD (DT&E)) helps break down these barriers, where they exist. For example, the staff specialists in the DASD (DT&E) engage in multiple programs across all the Services. Similarities exist in some programs and the staff specialists, by their close association with the program office testers, identify lessons learned and share this information among other staff specialists and other programs. Where appropriate, the staff specialists have encouraged and facilitated direct contact between programs to delve into the details of the lessons learned.

Ms. STEFANIK. The 2016 Annual Report on Developmental Test & Evaluation stated that the Department's current knowledge management capabilities and processes used to gain, collect, and analyze the information necessary to conduct acquisition assessments and evaluations are deficient and ineffective for today's world. In your opinion, what investments in analytical tools and technologies should the Department prioritize in order to begin to remedy this situation?

Mr. GREER. There is a need to transition to an Enterprise environment for Weapons Systems RDT&E and Cyber engineering to store, access, and share program RDT&E data. Establishment of a classified environment with the right controls in place as well as mechanisms to increase cross-program security collaboration is needed. With this, comes the need to pair an "RDT&E Warfighting System Cyber Assessment" CIO function that is focused on the tactical weapons systems impacts of Cyber to work alongside the "traditional" CIO function for business systems, email, common databases and promulgation of policy. 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. 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. Another Enterprise Solution that would benefit acquisition programs is a Shared Data Warehouse and Repository. Currently, data is stored and process on separate servers in a single program office. This data is isolated from many groups that can use it. A DOD Enterprise Solution to data storage and data warehouse tools would provide the necessary access for DOD acquisition programs to use and share data across various platforms. As mentioned in another question is an urgent need to gain access to industry acquisition data, which in most cases today is industry owned. The right Contract and Legal clauses to obtain access to this data freely and use it in government owned facilities and programs would provide the capabilities necessary to perform data analytics to conduct acquisition assessments and evaluations for all programs.

QUESTIONS SUBMITTED BY MR. SHUSTER

Mr. SHUSTER. Can you tell us how many DIUx projects have transitioned to programs of record or other major programs within the Department of Defense? What is the process for transitioning prototypes or pilots to the services or other agencies of the Department? Is the contractor required to lead these efforts? What outreach does DIUx do within the Department of Defense to alert them to the potential innovations available from commercial providers?

Mr. HALVORSEN. Sir I cannot with any specifics and would recommend that this question be referred to DOD. I can say that I am a believer in the concept and programs that expand DOD presence in technology hubs like Silicon Valley are worth pursuing. I would also suggest that measuring the effectiveness is a little premature. DOD has not had this type of program in place much longer then a year and both DOD and the technology hubs are learning how to make this work. In addition to this program DOD has been pursuing employee exchange programs with industry. These programs though limited to date have been well received by DOD and participating companies.

QUESTIONS SUBMITTED BY MR. FRANKS

Mr. FRANKS. Can you give a specific example of a good, well-performing, or successful IT acquisition? What were the characteristics that made it successful? How long did it take?

Mr. HALVORSEN. Sir, the Next Generation Department of Navy IT services contract is a good example of a successful IT procurement. This was the follow on to the Navy Marine Corps Internet (NMCI) contract. The contract yielded about $2B dollars in savings to the DON and as importantly continued commercial like services for the DON. Planning for this took over a year but was shorter then contracts of like size and scope. It involved close coordination with industry providers, a very detailed understanding of the capabilities desired, and a willingness to understand trade space as related to price and performance. I no longer have access to the details on this contract, but I am sure DOD could provide. There are still some issues with this contract but overall I give it very high marks. The negotiation of the Windows 10 upgrade license agreement is another good example of the DOD applying good practices and working well with an industry partner, in this case MICROSOFT. This negotiation was truly an enterprise effort in the department with DOD and the services working closely with MICROSOFT to interpret the action as an upgrade covered by existing agreements and not a major systems change. This enabled DOD to not have any bill for the actual license, while the business case for MICROSOFT was having DOD be better positioned to transfer to the cloud and elimination of costs in supporting older systems. When completed the transition to windows 10 will improve security, position DOD for cloud transition and result in cost savings. The biggest cost associated with the transition to Windows 10 is equipment modernization, which had fallen behind in DOD, but would have to be done at some point. Doing the modernization in conjunction with the windows 10 upgrade, allows for some modernization delay while gaining 80% or more of the new windows 10 capability. This is the type of DOD-industry partnership that is needed.

Mr. FRANKS. When you consider the critical need of modernizing the network, particularly to harden against enemy attacks and infiltration, shouldn't an immediate and complete overhaul of the IT procurement process be a priority?

Mr. HALVORSEN. Yes and this review needs to focus on both the requirements/capability process as well as the acquisition process. The current requirements process often results in very detailed and technically restrictive solutions being acquired that don't get DOD the latest solutions or the best value. Many times because of the length of the process and over specification, DOD is buying legacy the day the contract awards. The review needs to look at successful commercial process and encourage partnership with industry. This will present some problems, especially with small business, but I believe creative solutions can be applied to offer small business an opportunity to partipate in major enterprise acquisitions. DOD also needs to increase the dialog between the mission/business owners, the acquisition workforce and the industry providers. We need to look at the current rules restraining DOD employees from direct discussions with industry, many of these rules have not been updated in 30 years.

Mr. FRANKS. Can you give a specific example of a good, well-performing, or successful IT acquisition? What were the characteristics that made it successful? How long did it take?

Mr. GREER. I can think of several IT acquisitions that were executed efficiently—the examples are described in more detail below:

1) The Army Logistics Modernization Program (LMP) Increment 2 was a highly successful Defense Business System program that came to the Limited Deployment Decision milestone in 2015 with a 98% test case success rate during developmental testing. All failed test cases had work-arounds and corrective action plans acceptable to the user, and zero open severity 1 or 2 software problem reports. LMP success may be attributable to:

The LMP program management office (PMO) was highly experienced, knowledgeable of the system, and effectively planned and executed the complex program consisting of three waves of deployment with multiple functional areas. The PMO also established a close working relationship with the functional user to perform business process re-engineering, clarify requirements, and resolve issues quickly and effectively.

Increment 2 was a continuation of Increment 1; with the same system integrator using the well established and understood change management processes. Developmental testing (DT) included various events to specifically address performance, interoperability, and cybersecurity. Most importantly, the test strategy included mission-oriented developmental testing (known in the PMO as Business Operations Test (BOT)) that used actual users from the depots performing operational mission threads for their test cases. This identified human factors improvements that led to better user performance. The DT actual users became operational test (OT) trainers that resulted in a very high success rate for all the tasks and transactions that were tested during Initial Operational Test and Evaluation. The overall schedule from milestone B to milestone C was approximately 22 months.

2) The Marine Corps' ACAT IAC Common Aviation Command and Control System (CAC2S) Phase 2 was a very successful integrated acquisition. The operational test community worked well with the developmental test (DT) community, and accepted much of the DT data that satisfied OT requirements, reducing the overall acquisition time by 6-months. USD/AT&L nominated the CAC2S acquisition effort as a Defense Acquisition University integrated acquisition case study. Time between MS B and MS C was 34-months.

3) Defense Agencies Initiative (DAI) has been a successful Defense Business System Program. It enables compliance with Congressional direction for all DOD organizations to be auditable. The Defense Agencies Initiative (DAI) transforms the budget, finance, and accounting operations of most DOD Defense Agencies in order to achieve accurate and reliable financial information in support of financial accountability and effective and efficient decision-making throughout the Defense Agencies in support of the missions of the warfighter. Defense Agencies Initiative (DAI) is a critical DOD effort to modernize the Defense Agencies' financial management capabilities.

Mr. FRANKS. We've all heard of Moore's Law and know how rapidly technology advances and evolves. Do you know if there are any requirements for new systems we are building or purchasing to be capable of growing and evolving alongside technology—perhaps "upgradeable" systems which won't be obsolete the moment they become operational or shortly thereafter?

Mr. GREER. The rapid development pace of IT does mean that the Government will need to start driving requirements into new systems for Non-Proprietary deliverables, interfaces, and use of open systems architectures. Additionally, use of system virtualization and cloud technologies may mitigate IT obsolescence issues. Ensuring system designs, interfaces, and computing hardware are non-proprietary and open to the Government mitigates the possibility of "vendor lock in" and provides multiple flexible upgrade paths. The DISA Defense Enterprise Office Solution (DEOS) is a program that provides e-mail, voice and data conferencing, office products (e.g., word processing, etc.) and other capabilities with a cloud-based solution, potentially across the entire DOD enterprise. The acquisition strategy for DEOS contains a provision, which DISA calls "Evergreen", that will require the system integrator to provide upgrades, at no charge, whenever DEOS capability upgrades are offered commercially.

DODI 5000.02 supports growing and evolving alongside technology through the use of a modular open systems approach (MOSA). It requires programs to identify how a MOSA will or will not be used in their acquisition strategy. (Sec 801 PL 113–291). This approach integrates technical requirements with contracting mechanisms and legal considerations to support a more rapid evolution of capabilities and technologies throughout the product life cycle through the use of architecture modularity, open systems standards, and appropriate business practices. A modular design coupled with an appropriately open business model provides a valuable mechanism for continuing competition and incremental upgrades, and to facilitate reuse across the joint force.

○