DEPARTMENT OF DEFENSE AUTHORIZATION OF APPROPRIATIONS FOR FISCAL YEAR 2015 AND THE FUTURE YEARS DEFENSE PROGRAM

WEDNESDAY, FEBRUARY 26, 2014

U.S. SENATE,
SUBCOMMITTEE ON READINESS
AND MANAGEMENT SUPPORT,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY ACQUISITION PROCESSES, BUSINESS TRANSFORMATION, AND MANAGEMENT PRACTICES

The subcommittee met, pursuant to notice, at 2:34 p.m. in room SR–232A, Russell Senate Office Building, Senator Jeanne Shaheen (chairwoman of the subcommittee) presiding.

Committee members present: Senators Shaheen, McCaskill, Donnelly, and Ayotte.

OPENING STATEMENT OF SENATOR JEANNE SHAHEEN, CHAIRWOMAN

Senator SHAHEEN. Good afternoon. Sorry to keep you all waiting.

At this time, I would like to call the subcommittee hearing to order.

I want to begin by acknowledging my colleague from New Hampshire and ranking member, Senator Ayotte. It has been great to have a chance to work with her in this subcommittee, just as we do in New Hampshire. We are always pleased to be here representing New Hampshire on the subcommittee.

During the hearing today, we are going to be receiving testimony regarding information technology (IT) acquisition, business transformation, and management practices. This is the first hearing of the Readiness and Management Support Subcommittee. I think we are beginning with an issue that is critical as we look at the many other issues we will be addressing in the Department of Defense (DOD) this year.

The challenge of procuring IT systems in a timely and cost-effective manner is not something that is unique to DOD. Unfortunately, the stories of billions of dollars that are lost without any useful product as the result of that spending have appeared throughout the Federal Government, and while we recognize that this issue is not unique to DOD, it is clearly the biggest depart-

ment within the Federal Government, and we have seen these issues appear, unfortunately, over a period of years.

In fiscal year 2012, DOD IT acquisition investments totaled $32 billion, a sum which reflects DOD's growing need for sophisticated and reliable IT infrastructure. However, the $32 billion is expended across DOD under the supervision of multiple officials with what is often too little involvement of the operational users and those who must defend IT systems against cyber threats.

The Government Accountability Office (GAO) will soon release a report on acquisition of major IT systems in DOD, and though the report is still in draft form, the results that we have seen are disturbing. Of the 15 programs GAO reviewed, 7 experienced growth in their cost estimates, ranging as high as 2,233 percent, 12 programs experienced schedule slippage, ranging from a few months to 6 years, and only 3 programs met their system performance targets.

Among the programs assessed were some that could have an impact on DOD's ability to meet the statutory goal of achieving an auditable statement of budgetary resources by the end of fiscal year 2014 and an auditable financial statement by the end of fiscal year 2017 which, as I am sure you all know, is a major priority for this subcommittee and for the Senate Armed Services Committee (SASC) as a whole.

We must find ways to lower costs and improve inefficiency, while also improving our resiliency to cyber attack. A major piece of that challenge will be reforming our cumbersome acquisition process. Our current systems, which are better suited for weapons systems than IT, often produce systems already outdated once deployed. A new rapid approach with proper oversight which capitalizes on the knowledgeable IT workforce is necessary to correct these deficiencies.

As you all know, this is not the first time the SASC has tackled this issue. Section 804 of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 directed the Secretary of Defense to streamline and improve effectiveness of our current processes. The subcommittee remains interested in section 804 and we look forward to hearing from you all how DOD intends to move forward.

Another area of interest to the subcommittee is DOD's ongoing data center and server consolidation on cloud migration. This initiative, called the Joint Information Environment (JIE), is extremely ambitious and complex, and yet it seems to lack formal management structures and processes. We look forward to hearing more about how the JIE is expected to unfold.

With those opening remarks, and I have a longer statement that I will submit for the record. I would like to welcome our four witnesses this afternoon. Testifying today, we have the Assistant Secretary of Defense for Acquisition, Katrina G. McFarland; the Acting Deputy Chief Management Officer (DCMO), Kevin J. Scheid; the Chief Information Officer (CIO), Teresa M. Takai; and in addition to these representatives from DOD, we welcome the Director of Information Technology and Management Issues from GAO, David A. Powner. Thank you for being here.

Now I would like to turn to Ranking Member Senator Ayotte for her statement. Thank you.

[The prepared statement of Senator Shaheen follows:]

PREPARED STATEMENT BY SENATOR JEANNE SHAHEEN

Good afternoon. At this time, I would like to call the subcommittee hearing to order.

I would like to begin by acknowledging what a pleasure it has been to work with my colleague from New Hampshire, Senator Ayotte and her staff. We continue to work in a time-honored bipartisan fashion on this subcommittee and I sincerely appreciate that we have been able to reach agreement on so many issues.

I look forward to another productive year.

During our hearing today, we will receive testimony regarding information technology (IT) acquisition, business transformation, and management practices. This is the first hearing the Readiness and Management Support Subcommittee has convened in this session, and we are beginning with an issue of immediate importance, which is why I am pleased to begin the subcommittee's work on the National Defense Authorization Act (NDAA) for Fiscal Year 2015 before delivery of the President's budget. This is a complicated topic requiring creative, outside-the-box thinking, as well as the experience and knowledge of professionals throughout the Department of Defense (DOD) in order to find the most efficient, cost-effective way forward.

I would like to welcome our four witnesses this afternoon. Testifying, we have Assistant Secretary of Defense for Acquisition, Katrina McFarland; Acting Deputy Chief Management Officer, Kevin Scheid; and Chief Information Officer, Teresa Takai. In addition to these representatives from DOD, we welcome David Powner of the Government Accountability Office (GAO).

IT acquisition investments totaled $32 billion in fiscal year 2012, a sum which reflects DOD's reliance on sound IT infrastructure. However, this $32 billion is expended across DOD under the supervision of multiple officials, with too little involvement of the operational users and those who must defend information systems against cyber threats.

The Office of the Secretary of Defense organizational review conducted by former Secretary of the Air Force Mike Donley recommended major changes in the duties and responsibilities of the Deputy Chief Management Officer and the Chief Information Officer. The Senate Armed Services Committee also recommended major realignments affecting these officials in the Senate version of the NDAA. Neither set of recommendations were enacted into law. We hope to learn more about the rationale for the administration's proposals today.

The Bipartisan Budget Act provided some temporary relief to DOD, but sequestration is still very much a real threat. We must find ways to lower costs and improve inefficiencies, such as eliminating sub-optimal data centers and networks, which lead to unnecessarily high costs. Cybersecurity vulnerabilities must be addressed before a major cyber attack causes catastrophic damage. The IT infrastructure must increase interoperability to improve information sharing. The slow, cumbersome acquisition process, better suited for weapon systems than IT, results in systems already outdated once deployed. A new, rapid approach with proper oversight and which capitalizes on the knowledgeable IT workforce is necessary to correct these deficiencies.

This is not the first time the Senate Armed Services Committee has tackled this issue. Section 804 of the NDAA for Fiscal Year 2010 directed the Secretary of Defense to "develop and implement an alternative acquisition process for the rapid acquisition of IT systems." The legislation also required the new process to include "early and continual involvement of the user; multiple, rapidly executed increments or releases of capability; early, successive prototyping to support an evolutionary approach; and a modular, open-systems approach."

This subcommittee remains interested in the section 804 reforms. DOD delivered a report to Congress on December 9, 2010, outlining its plan for implementation; however, DOD has fallen short of full implementation. We are interested in hearing from our witnesses why and in what ways this reform mandate has so far failed, where we have successfully improved the process of acquiring IT, and how DOD intends to proceed in the future.

The committee has also passed legislation addressing the insider threat problem, supply chain risk management and software assurance against cyber threats, and the unique requirements for managing the rapid but disciplined acquisition of cyber tools and capabilities.

We expect that future reform efforts will capture and build upon the work done in the NDAAs since 2010. We have read Mr. Powner's recent report titled "Information Technology: Leveraging Best Practices to Help Ensure Successful Major Acqui-

sitions." It appears that many of the best practices he identifies track with the requirements of section 804.

Another GAO report also merits attention: "Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practices." This report is still in draft but its initial findings are significant. GAO's assessment of 15 programs found that 7 experienced growth in their cost estimates, ranging as high as 2,233 percent, 12 programs experienced schedule slippage, ranging from a few months to 6 years, and only 3 programs met their system performance targets.

Among the programs assessed were some that could have an impact on DOD's ability to meet the statutory goal of achieving an auditable Statement of Budgetary Resources (SBR) by the end of fiscal year 2014, and an auditable financial statement by the end of fiscal year 2017. On the positive side, we note that the Marine Corps achieved an important initial milestone, an unqualified opinion on the current year of their budget statement. However, clearly so much more remains to be done.

The most recent Financial Improvement and Audit Readiness Plan Status Report states that most but not all of DOD will meet the 2014 goal. We would appreciate an update on which areas are most in danger of failing to achieve an auditable SBR and what has been done to ensure that as much of DOD succeeds as possible.

Section 2866 of the NDAA for Fiscal Year 2012 imposed a moratorium within DOD on the acquisition or upgrade of data servers, server farms, and data centers. It required the implementation of a plan developed by the DOD Chief Information Officer to achieve reductions in the size of data centers and in the energy consumed to power and cool data centers along with increases in server virtualization and utilization rates. That plan also called for migrating from 700 data centers to fewer than 100, while reducing the number of network operations centers from 65 to 25. The NDAA for Fiscal Year 2013 required DOD to inventory all the applications it is running, eliminate redundancies, and rationalize its licenses. Progress here is critical to cost reduction.

Section 2866 also directed DOD to transition to commercial cloud services wherever possible to take advantage of cost and efficiency advantages of commercial cloud providers, consistent with security constraints. The committee will closely monitor the progress of DOD's pilots and associated policy development regarding the use of commercial cloud capabilities.

The ongoing data center and server consolidation, and cloud migration, are only elements of a far larger effort to transform DOD's entire telecommunications network. This initiative, called the Joint Information Environment (JIE) is an extremely ambitious and complex undertaking, and yet DOD has chosen to not make it a program with a program manager, requirements, milestones, schedules, and the like. It affects every command, every Service and DOD agency.

The Defense Information Systems Agency advertises the JIE programs as delivering:

> " . . . the largest restructuring of IT management in the history of the DOD. The end state is a secure, joint information environment comprised of shared IT infrastructure, enterprise services, and a single security architecture. JIE will enable DOD to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies."

The apparent lack of formal management structures and processes for this enterprise-wide initiative is striking and demands attention. We look forward to our witnesses' explanations.

Thank you to our witnesses, I look forward to hearing your testimony. I now invite the ranking member, Senator Ayotte, to make her statement.

STATEMENT OF SENATOR KELLY AYOTTE

Senator AYOTTE. Thank you, and I want to thank Chairwoman Shaheen. It is an honor to serve with you on the Readiness and Management Support Subcommittee and also to serve New Hampshire in the U.S. Senate with you. We have been able to work in a bipartisan fashion on issues that not only impact our State, but also issues that impact the country in this important subcommittee, and certainly today's topic is no exception to that.

Within the existing problems associated with acquisition reform, one area of growing concern is how DOD acquires IT. I will also say that this is not a unique problem across the Government. I also

serve on the Senate Homeland Security and Governmental Affairs Committee, and this is an issue that has been replete within that agency as well.

But getting this right is not just important from an acquisition process point of view, but it is also critical because IT can be used as a vital tool to help DOD become more efficient to serve as a better steward of taxpayers' dollars overall.

One of the most glaring examples of problems with IT acquisition was the termination of the Air Force's Expeditionary Combat Support System (ECSS). After 7 years and over $1 billion, this program was terminated in 2012 after it was determined that it would require another billion dollars to salvage, and even then, only a fraction of the program's requirements could be met.

This is an example. We need to understand what went wrong and how we are going to prevent these types of situations going forward, particularly with the challenges we face with limited defense dollars.

Equally disturbing as the cancellation of the ECSS, it places in doubt the Air Force's ability to conduct the Statement of Budgetary Resources by the end of this fiscal year which has been a concern with the SASC as a whole. This is an incredibly important issue that we do not plan to let go, and I hope that you do not either.

However, I do appreciate that addressing problems related to IT acquisition appear to be on the minds of the authors of the recently reissued DOD Instruction (DODI) 5000.02, which articulates the defense acquisition process. It appears that many of the guiding principles set forth in the report mandated by section 804 of the NDAA for Fiscal Year 2010, which I know we are going to spend a substantial amount of time on today, were incorporated into the new DODI.

Despite this, I remain concerned by the GAO reports indicating that a number of DOD's IT acquisition programs have not been correctly categorized on the Government's Web site called the IT Dashboard, which tracks the progress of such programs.

Another important part of this hearing will be understanding whether DOD categorizes IT programs differently, how we can ensure that the Government's Web site employs a standardized metric for purposes of organization and transparency.

As my colleagues know, I am also very interested in ensuring that DOD is ready to be audited because this will help ensure that we can better scrutinize spending to identify and eliminate waste and duplication before it happens. It is very important in the critical juncture we find ourselves at right now with DOD to be able to distinguish between necessary defense budget cuts and cuts that would harm our troops and damage our military's readiness, which is the foundation and purpose of this subcommittee.

In that spirit, Assistant Secretary McFarland, based on your position as the Assistant Secretary of Defense for Acquisition, I also look forward to addressing some of the broader acquisition challenges that DOD faces beyond the IT issues, but I certainly think that they relate to the IT issues.

For example, from 2007 to 2013, the Air Force wasted about $6.8 billion on 12 major acquisition programs; I have a list with me of those programs. There is no doubt that the Services, including the

Air Force, are confronting difficult budget challenges. It is really hard when we see billions of dollars wasted on programs, and yet we see proposals where the Services are making proposals to cut very important programs to our men and women in uniform.

One of those programs I have been quite outspoken about is the Air Force proposing the premature retirement of the A–10s in an effort to save $3.5 billion over the Future Years Defense Program, which Secretary Hagel publicly confirmed this week. I believe that this is a serious mistake and that we will lose the ability to have close air support (CAS). Chief of Staff of the Army General Odierno said it is the best CAS platform we have today. I believe that we risk our troops not having the re-attack times and capacity that the A–10 provides, well before we will have the F–35 variant that has purported to take up this mission in the future. We will have a gap that I believe is not good for our troops and could put them in danger.

That is why I want to put this in perspective. When we look at $6.8 billion in wasted money and then we talk about having to cancel important air platforms like the A–10, that perform such an important function for our men and women in uniform and particularly those on the ground, that is why acquisition reform, I know to all of you matters, and why getting it right is critical in terms of making sure that our taxpayers' dollars are used wisely, but most importantly, that the men and women in uniform who serve us every day are able to have the support that they need, the equipment that they need, and the training that they deserve in serving our country.

I appreciate your being here today and I look forward to this important discussion. I want to thank the chairwoman again for holding this hearing.

Senator SHAHEEN. Thank you very much, Senator Ayotte.

I would ask, Ms. McFarland, if you would go first, followed by Mr. Scheid, Ms. Takai, and Mr. Powner.

STATEMENT OF HON. KATRINA G. MCFARLAND, ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION, DEPARTMENT OF DEFENSE

Ms. MCFARLAND. Thank you, Chairwoman Shaheen, Ranking Member Ayotte, and distinguished members of the subcommittee, for this opportunity to discuss IT acquisition.

I would like to submit my full testimony for the record and will summarize it in the time I have.

I am honored to represent DOD, along with my colleagues from CIO, DCMO, and GAO. My focus will be on IT acquisition policy, people, and the oversight of Major Defense Acquisition Programs and Major Automated Information Systems (MAIS).

IT represents a considerable portion of all acquisition programs within DOD. DOD manages two fundamental types of software programs: national security systems and defense business systems.

National security systems are generally information systems which involve intelligence activities, cryptological activities, command and control of military forces, and systems that are an integral part of weapons or weapons systems.

Defense business systems are information systems which include financial systems, management information systems, and IT and cybersecurity infrastructure used to support our business activities.

Section 804, as Senator Ayotte, the ranking member, mentioned of the NDAA for Fiscal Year 2010 directed that DOD develop and implement a new acquisition process for IT systems based on the 2009 Defense Science Board (DSB) report. The recommendations were to condense timelines by increasing collaboration and improve processes to deliver right capabilities to the warfighter in operationally relevant timelines.

To do this, one must start with a defined requirement or capability. The Chairman of the Joint Chiefs of Staff has modified DOD's Joint Capability Integration and Development System, which develops our requirements, by introducing the IT Box concept to support more rapid acquisition timelines.

On approval of a requirement formulated in an initial capabilities document or a capabilities development document, requirements management is delegated to an appropriate body in a sponsor's organization. The organization is not required to come back for requirements changes unless they exceed the parameters of the IT Box.

In addition to the IT Box introduction, DOD has introduced the interim DOD directive operation of the defense acquisition system, also referenced by the ranking member, issued this fiscal year. It includes guidance to adopt a modular, open systems methodology with heavy emphasis on design for change in order to adapt to the changing circumstances consistent with the agile commercial methodologies. It describes acquisition models where across each model, the policy addresses the realization that IT capabilities may evolve, so desired capabilities can be traded off against cost and initial operational capability to deliver the best product to the field in a timely manner.

In accordance with section 933 of the NDAA for Fiscal Year 2011, DOD developed a strategy for the rapid acquisition of cyber tools, applications, and capabilities for the U.S. Cyber Command (CYBERCOM) and other military cyber operation components by chartering the Cyber Investment Management Board that unites IT policy and operational requirements with identifying gaps both in resources and in capabilities.

Now, I would like to address DOD's most important asset, our people. Finding the expertise and skill sets required to develop and acquire capabilities for IT systems and cyber space operations is challenging. The talent pool is small. Industry and Government seek it, and it rarely meets the level of expertise across all areas. DOD is working on many fronts to address these challenges. For example, with the assistance of the Defense Acquisition Workforce Development Fund, DOD has established a functional area for IT acquisition to support training in the Defense Acquisition University.

DOD is working to simplify the process of IT acquisition. There is an ongoing legislative review between DOD and Congress. There is an effort to develop a cybersecurity guidebook for the program manager that assists them in understanding what cybersecurity activities are necessary to conduct at each point of the acquisition

lifecycle. The Program Assessment Root Cause Analysis Directorate contributes to our understanding of the root causes for the IT program failures in order to prevent them from reoccurring.

Finally, there is an effort to help our program management by having our cybersecurity test and evaluation procedures include early development test and evaluation involvement for all of our test activities.

I would like to conclude with the following key points.

DOD will continue its efforts to operate as affordably, efficiently, and effectively as possible. We are evolving our approach to acquisition for IT and recognize the distinct challenges that come with it. We are taking a disciplined and proactive step to improve our IT processes and compensate for them.

Thank you for your ongoing support of our men and women in uniform. I know you share my desire to ensure that they have the resources necessary to meet and accomplish their mission.

[The prepared statement of Ms. McFarland follows:]

PREPARED STATEMENT BY HON. KATRINA MCFARLAND

Thank you for the opportunity to address the Subcommittee on Readiness and Management Support of the Senate Armed Services Committee. I am honored to represent the Department of Defense (DOD) along with my colleagues. The DOD partnership among my office, the Office of the Deputy Chief Management Officer (DCMO), and Chief Information Officer (CIO), manages the DOD IT Enterprise in the areas of acquisition, policy, and the Defense Business Systems (DBS). I will focus my discussion on Information Technology (IT) acquisition policy, people, and oversight of the Acquisition of Major Defense Acquisition Programs and Major Automated Information Systems (MAIS) over which the Under Secretary of Defense (USD) for Acquisition, Technology, and Logistics (AT&L), as Defense Acquisition Executive, has Milestone Decision Authority. Ms. Takai will discuss her responsibility for overall IT Policy and as the Enterprise IT sponsor. Mr. Scheid will discuss his responsibility for the Defense Business Architecture and Defense Business Council/Investment Review Board oversight. At the Office of the Secretary of Defense (OSD) level, we oversee the planning and execution of the Services' acquisition programs and establish acquisition, logistics, maintenance, and sustainment support policies.

BACKGROUND

Section 804 of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 directed the DOD to develop and implement a new acquisition process for IT systems based on the recommendations of Chapter 6 of the March 2009 Defense Science Board Report. IT represents a considerable portion of all acquisition programs within DOD. To help manage IT, DOD manages two fundamental types of software programs, National Security Systems (NSS) and DBS. NSS as defined in 44 U.S.C. 3541, are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions. NSS includes a category of software programs called embedded software—software that operates and controls our weapon system platforms.

DBS, as defined in 10 U.S.C. 2222, are information systems, other than a NSS, operated by, for, or on behalf of the DOD, including financial systems, management information systems, financial data feeder systems, and the IT and cybersecurity infrastructure used to support business activities, such as contracting, pay and personnel management systems, some logistics systems, financial planning and budgeting, installations management, and human resource management. Because NSS tend to be broader in scope with significant interoperability needs and requirements, we use different policies and procedures to acquire these two product categories.

IT REQUIREMENT PROCESS IMPLEMENTATION

To acquire IT, one must start with defined requirements (or capabilities). DOD has worked to condense timelines, increase collaboration between communities, and

improve processes to deliver the right capabilities to the warfighter in operationally relevant timelines. The Chairman of the Joint Chiefs has modified DOD's Joint Capability Integration and Development System by instituting a major change for Information System (IS) requirements development which introduces the "Information Technology (IT) Box," enabling the delegation of authorities to specifically support the more rapid timelines necessary for IT capabilities through the Defense Acquisition System processes. The four sides of the "IT Box" include the organization that will provide oversight and management of the product; the capabilities required; the cost for application and system development; and the costs for sustainment and operations. Under this construct, upon approval of an IS-Initial Capabilities Document (ICD) or IS-Capabilities Development Document (CDD) by the Joint Requirements Oversight Council (JROC), requirements management is delegated by the JROC to an appropriate body in the sponsor's organization. The delegation of authorities and defined parameters enable faster timelines for IT programs, because the organization is not required to return to the JROC for requirements approval unless the IT Box parameters are exceeded by prescribed thresholds. The organization that requirements approval is delegated to for an IS–ICD or IS–CDD must return to the JROC to provide periodic updates.

An example of DOD's recent use of the "IT Box" was through tailoring an IT acquisition that supports the Combatant Commanders with mission planning tools through an automated and enterprise capability called the 'Integrated Strategic Planning and Analysis Network (ISPAN) Increment 2' program. The Vice Chairman Joint Chiefs of Staff delegated JROC responsibility for ISPAN non-key performance parameters to a Combatant Command (United States Strategic Command). In concert, on March 10, 2010, the USD(AT&L) approved ISPAN acquisition tailoring that included shorter development periods with multiple capability releases, early and continual user involvement, and a modular open-systems approach using successive prototyping efforts, consistent with section 804 of the NDAA for Fiscal Year 2010.

In January 2013, the Air Force completed a report after the ISPAN program had successfully delivered its increment 2 of capabilities and highlighted significant improvement in acquisition cycle-time as well as speed in decisionmaking compared to an earlier increment. For example:

- Time between Milestone B and Initial Operational Capability: ISPAN Inc. 2–15 months; ISPAN Block 1–60+ months.

This demonstrates the value of close coordination between the requirements and acquisition process for the delivery of IT capabilities.

DEFENSE ACQUISITION SYSTEM IMPLEMENTATION OF IT

On November 26, 2013, the Deputy Secretary of Defense issued an interim Department of Defense Instruction 5000.02 to implement a number of statutes and regulations that have come into existence since the last version was published in 2008. This new acquisition policy includes guidance to address the challenges associated with the different types of IT acquisition programs, such as guidance to address the fundamental challenge with DBSs where a suite of integrated applications referred to as Enterprise Resource Planning (ERP) business management software is acquired. For ERPs, positive outcomes are dependent upon understanding the needed process changes prior to starting implementation. Consistent with section 804 of the NDAA for Fiscal Year 2010, it includes guidance to adopt a modular, open-systems methodology with heavy emphasis on "design for change" in order to adapt to changing circumstances consistent with commercial agile methodologies. Finally, the new acquisition policy addresses hybrid models where significant software development is the predominant activity for a major weapon system, or in situations that combine hardware development as the basic structure with a software intensive development occurring simultaneously. Across each model, the policy addresses the realization that information technology capabilities may evolve so "desired capabilities" can be traded-off against cost and initial operational capability to deliver the best product to the field in a timely manner.

SECTION 933 IMPLEMENTATION

Following section 804 was section 933 in the NDAA for Fiscal Year 2011 which required DOD to develop a strategy for the rapid acquisition of cyber tools, applications, and capabilities for U.S. Cyber Command (CYBERCOM) and other cyber operations components of the military. It specifically requested an orderly process for determining and approving operational requirements; a well-defined, repeatable, transparent, and disciplined process for developing capabilities in accordance with the acquisition guidance and policy; allocation of facilities and other resources to thoroughly test capabilities in development, before deployment; and operational use

to validate performance and take into account collateral damage, and to promote interoperability, share innovation, and avoid unproductive duplication in cyber operational capabilities. In response to section 933, DOD chartered the Cyber Investment Management Board (CIMB). The goal of the CIMB is to unite IT policy and operational requirements and identify gaps and resources to enable the rapid acquisition and development of cyber capabilities. The CIMB is aligning existing processes and implementing new processes to:

- enable rapid cyber acquisition and balance investments based on operational need;
- align and synchronize requirements, testing and evaluation;
- facilitate oversight and improve insight of DOD cyber activities and investments; and
- enable integration and transparency among key process owners.

The CIMB is tri-chaired by the USD(AT&L), the Vice Chairman of the Joint Chiefs of Staff, and the Under Secretary of Defense for Policy. The CIMB membership includes the OSD Principal Staff Assistants to include the DOD CIO, the Services, the Defense Information Systems Agency, National Security Agency, U.S. Strategic Command, and CYBERCOM. Since March 2012, the CIMB addressed topics ranging from exploring the cyber portfolios within the science and technology base, National Security Agency, and CYBERCOM; as well as offensive and defensive cyberspace operations, defend the nation, cyber situational awareness and a holistic assessment of the cyber investment portfolio. DOD has achieved an understanding of cyber investment and mission alignment enabling future effective strategic management of total cost of ownership and return on investment.

Another DOD initiative stemming from section 933 is the Cyber Acquisition Process Pilot Plan. The plan was approved by the USD(AT&L) on July 29, 2013 and was designed to test and refine the proposed requirements, acquisition, test and evaluation processes. The goal is to select two to five capabilities and facilitate, observe and analyze as they progress through the acquisition process in order to understand where existing and dependent processes need better alignment or changes. The intended output is to refine and validate the rapid acquisition processes prior to implementation across the DOD. As you are aware, one of the tenants in DOD's Better Buying Power initiative is continual process improvement. We find ourselves sustaining changes through this process by starting with a subset of programs measuring the success of the initiatives as we execute, and introducing these changes to a larger set as they demonstrate success or reassessing the changes if they don't.

IT PEOPLE

IT has many challenges, of which cyber capabilities add complexity. Finding the expertise and skill sets required to develop and acquire capabilities for IT systems for cyberspace operations is challenging. For example, one challenge found in the cyber acquisition domain is that many cyber capabilities are not acquired or developed under a traditional acquisition program of record structure because of the funding level of the cyber development efforts. In many cases, a program manager does not exist. The talents we require span information assurance, information technology, operations, and in the case of DBSs, enterprise management. The talent pool is small and rarely meets the level of expertise across the necessary areas; those who possess the required skills are in extremely high demand. Industry faces similar challenges; DOD, other Federal organizations, and industry are all seeking the same skillsets increasing the challenge to recruit talent and retain talent.

We are working to address these IT workforce issues. With the assistance of the Defense Acquisition Workforce Development Fund, we have established a functional area for IT acquisition that is working the appropriate IT acquisition training into the Defense Acquisition University training curriculum, as an example. The USD(AT&L) chairs the Acquisition Workforce Senior Steering Board that is attended by the Service acquisition executives, the Service defense acquisition career managers, the Defense Acquisition University, and the functional career area leads. It focuses on the immediate workforce needs, challenges, and staffing levels.

We are working to simplify the process of acquisition through a legislative review in coordination with Representative Thornberry, Vice Chairman of the House Armed Services Committee. Additionally, there is also a joint effort for AT&L and the DOD CIO to develop a cybersecurity guidebook for program managers. This guidebook is being developed to provide program managers clear and concise guidance on what cybersecurity activities should be conducted at each point in the acquisition lifecycle, while emphasizing early integration of cybersecurity requirements. The purpose is to help program managers ensure cybersecurity is considered in the design of a new capability instead of later on in the process when it may be too costly or take too

long to implement it correctly. The Program Assessment Root Cause Analysis directorate works in my organization, which contributes to our understanding of the root cause of IT program failures in order to prevent them from re-occurring. Again, with the help of the Defense Acquisition Workforce Development Fund funding, we will bring back lessons learned to the Defense Acquisition University to ensure we train our people on effective program management, engineering, logistics, contracting, et cetera.

Another effort to help program managers is adjusting our cybersecurity test and evaluation (T&E) procedures to include early developmental T&E involvement in test planning and execution. The goal is to improve the resiliency of military capabilities before beginning production and deployment. Early discovery of system vulnerabilities can facilitate remediation to reduce the impact on cost, schedule, and performance.

One example of this is regression testing, which is a term for tests to ensure that software changes in one part of a system do not break or alter working functionality in another. Every software system requires regression testing. The Director for Operational Testing and Evaluation (DOT&E) is now examining regression test procedures as part of its suitability evaluations. DOT&E has also begun helping some programs convert to automated (vice manual) regression testing so as to gauge the extent of the problem DOD faces. In the last 2 years they have been able to help the Defense Logistics Agency implement automated regression testing for the Enterprise Business System.

CONCLUSION

I would like to conclude with the following key points. The DOD is evolving its approach to IT acquisition. We are off to a good start with the interim DODI 5000.02 which provides program structures and procedures tailored to the dominant characteristics of the product being acquired and to unique program circumstances, including operational urgency and risk factors. We will continue to work with the DOD CIO to implement IT Policy, and the DCMO to execute to the Business Enterprise Architecture. DOD recognizes the distinct challenges associated with acquiring IT capabilities and we are taking disciplined and proactive steps to improve our processes to compensate for them.

Senator SHAHEEN. Mr. Scheid.

STATEMENT OF KEVIN J. SCHEID, ACTING DEPUTY CHIEF MANAGEMENT OFFICER, DEPARTMENT OF DEFENSE

Mr. SCHEID. Good afternoon and thank you. Senator Shaheen, Senator Ayotte, and members of the subcommittee, my name is Kevin Scheid and I am the Acting DCMO of DOD. As the DCMO, I am the Secretary's and the Deputy Secretary's principal official for providing management oversight across DOD's military components, agencies, offices, and organizations. I report to the Deputy Secretary who is also the Chief Management Officer (CMO) of DOD.

Thank you for the opportunity to provide this update on the management of DOD's business operations.

As you are aware, DOD's basic mission is to hire, train, and equip soldiers, sailors, airmen, and marines, deploy them abroad to fight and win the Nation's wars, care for the wounded and their families, redeploy those troops home safely, and retrograde and refit the equipment capabilities to be ready and win the next fight.

DOD performs this mission through various business areas or functional areas such as human resources, logistics, acquisition, financial management, installations, and security. These are the building blocks of the defense business enterprise.

For DOD to be successful in performing these functions, my office works with DOD's senior leaders in defining the functional areas, establishing clear business goals and objectives, guiding DOD in establishing and aligning its processes, ensuring those processes are

enabled by modern, interoperable business systems, and establishing meaningful outcome-oriented performance measures.

I am relatively new in this position, having recently returned from an assignment at NATO as the Chief Operating Officer (COO) and the Deputy General Manager of a large NATO agency. On November 25, the Secretary designated me as the acting DCMO at the time of Ms. Beth McGrath's retirement.

There have been significant changes made since Ms. McGrath last testified before the subcommittee. The most important of these changes was Secretary Hagel's December 4 decision to strengthen management in DOD by directing a series of consolidations and realignments within the Office of the Secretary of Defense (OSD). My office will be consolidating with the Office of the Director of Administration and Management, a relatively small office of about 36 employees, and the Office of the Assistant Secretary of Defense for Intelligence Oversight, an office of about 9 or 10 employees.

In addition, the defense field activity of Washington Headquarter Services and the Pentagon Force Protection Agency will be realigned under the DCMO's office.

Further, the Secretary directed the transfer of oversight responsibilities for the technical aspects of defense business systems from my office to the Office of the CIO. This change would realign responsibility and accountability for business systems in DOD while requiring my office to continue leading the development of requirements for those systems.

These reforms may require changes to section 2222 of title 10 and we are reviewing if that is necessary at this time.

The Secretary's goal in strengthening the DCMO's office in this way through these consolidations is best captured, I think, in the following quote from Secretary Hagel: "This consolidation enables the role of the Deputy CMO as the Principal Staff Assistant and Advisor to the Secretary and Deputy Secretary of Defense for full spectrum oversight on both the OSD and DOD levels of management administration, coordination, and collaboration across DOD components and business functions, performance improvement, and regulatory compliance."

DOD is in the midst of implementing the Secretary's direction, and all of DOD's witnesses here today are working closely together on a path forward.

While the details are still being developed, I am confident that the focus on management and oversight will help advance DOD's progress in the business operations. As we execute these consolidations, DOD continues to make progress in the selection, acquisition, and control of IT systems.

Building on the principles contained in DOD's response to section 804 of the NDAA for Fiscal Year 2010, important steps have been taken. Under Assistant Secretary McFarland's lead, lessons from the section 804 report have been incorporated in DOD's overarching acquisition policies. Under the CIO, Ms. Takai's lead, there have been lessons learned incorporated into the JIE. Under my predecessor's lead, Ms. McGrath, we have incorporated or embedded lessons learned in the business mission areas of what we call the Integrated Business Framework (IBF) for DOD.

This framework, overseen by the Defense Business Council that I currently chair, has driven quantifiable improvements in DOD's business environment. Over the past 2 years, and we have only been through two cycles of this, we have improved the alignment of our strategies, enhanced data available for decisionmaking, and rationalized our business systems environment by reducing funds certifications by over $1 billion and retiring 60 legacy systems. We have only gone through two cycles, as I mentioned, and it is early, but this process is yielding some important results.

Before I close, and in response to a topic that you specifically raised in your letter and mentioned in your opening comments, I would like to briefly discuss DOD's progress towards its audit readiness goals.

Bringing this very large Department together, applying consistent business practices, and ensuring good internal controls is difficult, as I am sure you can appreciate. But our efforts are making progress, exhibited most recently by the Marine Corps' achievement of an unqualified favorable audit of its current year appropriation. Secretary Hagel is committed to audit readiness, as is DOD as a whole. My office continues to work with the Comptroller to implement the DOD plan to achieve audit readiness. DOD has resources, governance strategy, and senior leader commitment needed for success. While it is too soon to know for sure, we expect most budget statements to be audit ready by the goal of September 2014.

In closing, I would like to reemphasize that the Secretary is strongly committed to strengthening DOD's management, and the steps he directed in December are taking shape and leading to his vision of stronger business processes, a simplified business environment, and greater oversight. Strengthening DOD's management is a high priority for the Secretary, as well as this subcommittee and the SASC. We appreciate the committee's support and guidance in meeting these priorities over the years. Together, our collective efforts are improving the support to our soldiers, sailors, airmen, and marines, while realizing greater efficiency and effectiveness for the American taxpayers. We are committed to continuing these efforts.

Thank you for the opportunity to testify. I would be glad to take questions.

[The prepared statement of Mr. Scheid follows:]

PREPARED STATEMENT BY MR. KEVIN J. SCHEID

INTRODUCTION

Senator Shaheen, Senator Ayotte, and members of the subcommittee, I appreciate the opportunity to testify before you to provide an update on our oversight of management in the Department of Defense (DOD). DOD has always taken its duty to be a good steward of taxpayer dollars very seriously and the efficient and effective management of DOD is key to accomplishing this. As the DOD's Acting Deputy Chief Management Officer (CMO), I am the Secretary and Deputy Secretary of Defense's primary agent for providing effective management across DOD's many organizations and establishing a simplified business environment that is fiscally responsible. The main focus of my office is to work with DOD's senior leaders across the enterprise to define clear business goals, create meaningful performance measures, align activities via repeatable processes, ensure that these processes are supported by modern, interoperable defense business systems, and support the Secretary of Defense's direction to implement institutional reforms, as well as simplify DOD's business environment and lower its cost.

While I have only been part of the Office of the Deputy CMO for about 6 months and in the Acting Deputy CMO position since November 25, 2013, much progress has been made since my predecessor, the Honorable Elizabeth McGrath, last testified before you. I look forward to being able to share some of this progress with you today.

SECRETARY'S ORGANIZATIONAL REVIEW

The responsibilities of the Office of the Deputy CMO were recently enhanced when, on December 4, 2013, Secretary Hagel announced a series of organizational realignments within the Office of the Secretary of Defense (OSD). While the Secretary's announcement included numerous elements, one of his primary goals was to strengthen and elevate the role of the Office of the Deputy CMO to provide, both within OSD and across DOD, full spectrum oversight of management, administration, coordination across DOD Components and business functions, performance improvement, and regulatory compliance. This will be accomplished through the consolidation of the Office of the Director of Administration and Management, Washington Headquarters Service, the Pentagon Force Protection Agency, and a few additional organizations into the Office of the Deputy CMO structure.

Another of the Secretary's primary goals was to strengthen the Office of the DOD Chief Information Officer (CIO) to address the growing information technology (IT) and cyber challenges, improve oversight of IT resources, and further enable successful implementation of the Joint Information Environment. This will be accomplished through the transfer of oversight responsibility for the technical aspects of defense business systems from the Office of the Deputy CMO to the Office of the CIO.

DOD is in the midst of implementing the Secretary's direction and the Offices of the Deputy CMO, DOD CIO, and the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) are working closely together to ensure the optimal alignment of responsibility and accountability for business processes and business systems approval and acquisition. While certain details continue to be finalized, I am confident that the renewed focus on management and oversight will help advance DOD's progress in its business operations and IT functions. I look forward to being able to share additional details about these organizational realignments, including any possible legislative changes, with the committee if and when the Secretary approves such changes.

INTEGRATED BUSINESS FRAMEWORK

In 2012, aided by changes to DOD's investment management process for defense business systems contained in section 901 of the National Defense Authorization Act (NDAA) for Fiscal Year 2012, the Deputy CMO established a new governance body, the Defense Business Council, to consolidate previously dispersed responsibilities and implement a new overarching management approach, the Integrated Business Framework. This framework is intended to align all levels of our management strategies and processes and use multiple statutory and policy levers, including investment management responsibilities, to drive positive outcomes in DOD's business operations. The framework is also aligned with the guiding principles established in the DOD's Strategic Management Plan and enables DOD business leaders to instill a cost culture, institutionalize end-to-end business processes, align business operations, and modernize and rationalize business systems.

The Integrated Business Framework is progressing. Over the past 2 years we have:

- Aligned the Strategic Management Plan and DOD's Annual Performance Plan with the National Security Strategy and Quadrennial Defense Review;
- Established, for the first time, functional strategies for each of our lines of business (financial management, human resources, etc.) that are aligned with the Strategic Management Plan and lay out the strategic vision, goals, priorities, outcomes, measures, and any mandatory enterprise initiatives for a given functional area;
- Established, for the first time, a portfolio based approach for reviewing all defense business system spending. The mechanism for achieving this, Organizational Execution Plans developed by the DOD components (the military departments, defense agencies, et cetera), include details on the component's proposed business system investments, their alignment with DOD's functional strategies and their adherence to Business Process Reengineering and Business Enterprise Architecture requirements;
- Aligned and improved budget and systems data, which has improved the visibility of our defense business systems inventory and enabled DOD business leaders to make more informed investment decisions;

• Established the Defense Business Council as the requirements validation body for defense business systems, thereby aligning strategy with investments;
• Created and implemented criteria for evaluating defense business systems spending, which resulted in not certifying obligation requests totaling $617 million, or 9 percent of the total requested amount for fiscal year 2014. During the two investment certification cycles since the NDAA for Fiscal Year 2012 was enacted, the Defense Business Council has not certified over $1 billion in requests; and
• Retired more than 60 defense business systems as legacy systems and taken steps to eliminate them from future budgets.

DEFENSE BUSINESS SYSTEMS AND IT ACQUISITION REFORM

Over the years, DOD has had many challenges with the development, deployment, and oversight of defense business systems. The Office of the Deputy CMO and its predecessor organizations have played a variety of roles in trying to address this problem from both an acquisition and an investment management perspective.

Through its hiring of recognized industry experts on large-scale IT projects and its implementation of enterprise IT solutions, the business mission area has learned many lessons about DOD's ability to agilely acquire defense business system capabilities. A primary lesson was that defense business systems required a unique approach that in many cases is different from the traditional DOD model for weapons system acquisition. Consequently, DOD began development of a tailored acquisition process for defense business systems known as the Business Capability Lifecycle.

Shortly after the Deputy CMO was established, the then-Deputy Secretary of Defense asked this new office to lead DOD's response to section 804 of the NDAA for Fiscal Year 2010, which directed DOD to develop and implement a new acquisition process for IT systems based, to the extent determined by the Secretary, on the recommendations of a 2009 Defense Science Board Report on IT Acquisition Reform. The intent was to initially focus on defense business systems and leverage progress made and lessons learned to address the full set of recommendations from the Defense Science Board Report. The broad themes contained in the 804 Report were developed in collaboration across DOD and with industry. They were sweeping in their scope and, if fully implemented, would likely require legislative changes to fully implement. In conjunction with the publication of the 804 Report, a task force was established, chaired by the Deputy Secretary and run by the Deputy CMO. Working groups established under the task force developed more detailed recommendations for implementation of the 804 Report's themes. Eventually, responsibility for the way ahead on policy implementation shifted to USD(AT&L), and they have taken important steps forward, such as incorporating aspects of the Business Capability Lifecycle into the latest release of DOD's acquisition guidance, DODI 5000.02.

Since publication of the 804 Report, the Office of the Deputy CMO has focused on further implementing the principles of the report in two primary ways for defense business systems. First, until December 2013, when USD(AT&L) rescinded its delegation of Milestone Decision Authority to the Deputy CMO for certain large defense business system acquisitions, the Deputy CMO used this delegated authority to conduct frequent oversight of these programs and cap spending authority in line with the recommendations of the report. Second, the Deputy CMO has embedded, where practicable, the principles of the 804 Report, into the execution of the Integrated Business Framework and revised investment management process as described above. The use of these principles, which include using portfolios to help govern defense business systems, use of the Defense Business Council to review problem statements of new business system investments prior to approving initiation, and review of the business process reengineering conducted on the processes systems support, is beginning to pay dividends.

CONCLUSION

DOD is committed to improving the management and acquisition of IT systems, as well as our overarching business operations. These issues receive significant management attention and are a key part of our broader strategy to build better business processes that will create lasting results for our men and women in uniform, as well as the American taxpayer. I appreciate the opportunity to discuss the Secretary's plans to strengthen management in DOD and I look forward to continuing our work with this committee in the months and years ahead.

I would be glad to take your questions.

Senator SHAHEEN. Thank you.

Ms. Takai.

STATEMENT OF TERESA M. TAKAI, CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Ms. TAKAI. Thank you, Madam Chairwoman. Thank you so much for inviting us this afternoon. I appreciate this opportunity to testify before the subcommittee on topics that are of great importance to all of us, and certainly in my world.

I provided a written statement that covers the scope of everything that the CIO does, and rather than trying to go into all of that, because I know we are very focused in a particular area, I would like to mainly focus my remarks on the JIE, if I could.

We wanted to be able to describe to you this key initiative to ensure that DOD has access to information on secure information networks—and I will come back to that because that really is pivotal in what we are doing—and also the tools necessary to execute our warfighting and business support missions.

I want to say right away that the efforts we are taking regarding the IT infrastructure is in direct support of the IT acquisition process and also in support of the business transformation efforts. It is really about being able to provide the technology that is necessary for the business systems to accomplish what they need, but also standardization to assist with the IT acquisition process in that important area.

I think our mission success depends upon the ability of our military leaders and civilians to act decisively based on the most timely and accurate information. Recognizing that information is a strategic asset pushes us to undertake a very ambitious effort to realign and restructure how our networks, hardware, and software housed in data centers is constructed, operated, acquired, and defended. This is done in order to provide better information access to our users, improve our ability to defend not only the networks and the data, but also make it responsive to our changing technological and operational factors.

This effort, called JIE, is intended to enable and empower our military's decisionmaking and our most important asset, our people, by providing warfighters and our mission partners a shared IT infrastructure that consists of federated networks with common configurations, management, and a common set of enterprise services with a single security architecture. I know that is a mouthful but it does describe what we are intending.

The ultimate benefit of the JIE is to the commander in the field. It allows for more innovative integration of ITs, operations, and cybersecurity; its related tempo is more appropriate to our fast-paced operational conditions.

Some of the other benefits are, as I mentioned, a single security architecture that enables our cyber operators at every level to see the status of the networks for operations and security, and provide standard resilience and cyber maneuver options for cyber forces. The complexity of our networks today makes it very difficult for our cyber operators to see who is on our network and be able to defend our networks as we would like them to.

As you mentioned, the consolidation of our data centers, which also includes our operation centers and our help desks, will enable

users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions regardless of their location.

Finally, a consistent DOD-wide IT architecture that defines our enterprise standards and supports fielding of DOD capabilities in support of information sharing, as well as the sustainment and integration of legacy systems, will be an important part of the way that we not only acquire systems, but the way we operate and sustain.

DOD plans on utilizing the Services' existing programs' initiatives and mainly our technical refresh dollars to deploy and migrate to JIE standards utilizing specific implementation guidance. Simply stated, JIE will help improve our ability to field capability faster and more efficiently, and allow us to be better stewards of taxpayers' resources.

Now, in line with this, it is also important that we take actions necessary to increase visibility into our IT budgets and spending patterns, and strengthen our analysis of IT investments as part of our overall governance and oversight processes. I am working very closely with my colleagues here to identify ways to leverage DOD's three core processes: our requirements, budgeting, and acquisition, to address the systemic conditions resulting in our current stovepiped IT infrastructure. This is critical if we are to achieve the agility and responsiveness from IT that our warfighters demand. Working closely not only with my colleagues here but the Comptroller and the Cost Assessment and Program Evaluation Office, we will deliver the flexible, agile acquisition processes that Ms. McFarland spoke of that really meet our requirements and budgeting processes to institutionalize the agility and flexibility necessary for this domain.

Finally, maintaining information dominance for our warfighters is critical to our national security. The efforts outlined above will ensure that DOD's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of our financial resources.

I very much appreciate your interest and your staff's interest in our efforts. I look forward to your questions.

[The prepared statement of Ms. Takai follows:]

PREPARED STATEMENT BY MS. TERESA M. TAKAI

INTRODUCTION

Good afternoon Madam Chairwoman and distinguished members of the subcommittee. Thank you for this opportunity to testify before the subcommittee today on information technology (IT) acquisition processes, business transformation, and the Department of Defense (DOD) management practices. I am Teri Takai, DOD's Chief Information Officer (CIO). My office is responsible for ensuring DOD has access to the information, the communication networks, and the decision support tools needed to successfully execute our warfighting and business support missions. Our mission is to ensure that these capabilities can be depended upon in the face of threats by a capable adversary in all conditions from peace to war, and particularly in the face of ever-increasing cyber threats. My focus in accomplishing these responsibilities is to ensure the effectiveness, reliability, security, and efficiency of DOD's IT capabilities for the warfighter, and ensure we are able to take advantage of future technology innovations to support DOD's missions.

I would like to give you a broad overview of DOD's IT landscape; summarize recent directions from the Secretary of Defense to strengthen the DOD CIO; and describe the Joint Information Environment (JIE), DOD's multiyear effort to restruc-

ture much of the underlying network, computing, and cyber security of DOD so as to make us more agile in deploying new decision support capabilities, make us better able to mount cyber defense of our core DOD missions, and make us more efficient and better stewards of taxpayer resources. I will also briefly describe some of the activities underway in my office related to my responsibilities for overseeing Positioning, Navigation, and Timing (PNT) and spectrum.

OVERVIEW OF DOD'S INFORMATION TECHNOLOGY

DOD's fiscal year 2014 IT budget request was $39.6 billion and included funding for a broad variety of IT, ranging from command and control systems, commercial satellite communications, and tactical radios to desktop computers, server computing, enterprise services like collaboration and electronic mail, and DOD business systems. These investments support mission critical operations that must be delivered both on the battlefield and in an office environment. They also provide capabilities that enable the Commander in Chief to communicate with and direct the military, and that support command and control, intelligence, logistics, medical and other warfighting and business support functions throughout DOD. Included in the overall IT budget are DOD's cybersecurity activities and efforts. These are designed to ensure that essential DOD missions work well in the face of cyber attacks. These cybersecurity efforts continue to receive the highest-level attention and support of DOD.

SECRETARY OF DEFENSE ORGANIZATIONAL REVIEW

Recently Secretary of Defense Hagel issued direction to strengthen the role of the DOD CIO. Specifically he affirmed the importance of my office as an Office of the Secretary of Defense Principal Staff Assistant with the responsibilities listed above. As well, he directed actions to add functions, expand authorities, and restore stature to the DOD CIO, with a priority focus on advancing the JIE as a special interest item for the Secretary. The Secretary also directed my office to improve visibility, oversight, and governance of IT resources. He reaffirmed the critical importance of addressing the challenges posed by cybersecurity.

My office has completed the development of a plan of action and milestones to implement the Secretary's direction. We are taking actions necessary to increase visibility into IT budgets and spending patterns, and are strengthening our analysis of IT investments and evolving our processes for IT governance and oversight. We are working closely with the DOD's Deputy Chief Management Officer (DCMO) and with the DOD Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) to strengthen the oversight and management of IT Business Systems.

INFORMATION TECHNOLOGY ACQUISITION

Consistent with the Secretary's direction, my office is working closely with others in DOD to identify ways to adapt our existing processes to ensure adaptability to technological advances and ability to defend the network against emerging cybersecurity threats. In particular, we are examining how best to leverage DOD's three core processes—requirements, budgeting, and acquisition—to address the systemic conditions resulting in DOD's stove-piped IT infrastructure. This is critical if we are to achieve the agility and responsiveness from IT systems that warfighters both demand and deserve, and improve our ability to defend against cyber attacks. My office is working closely with the offices of the DCMO, USD(AT&L), the Comptroller, the Director of Cost Assessment and Program Evaluation and others to develop a flexible, agile acquisition process that also addresses the DOD's requirements and budgeting processes to institutionalize the agility and flexibility necessary in cyberspace, while ensuring compliance with enterprise standards.

JOINT INFORMATION ENVIRONMENT

Mission success depends upon the ability of our military commanders and civilian leaders to act decisively based on the most timely and accurate data and information. Recognizing that information is a strategic asset, DOD is undertaking an ambitious effort to re-align and restructure how our many IT networks are constructed, operated and defended in order to provide better information access to the user, improve our ability to not only defend the networks and the data, but make it responsive to constantly changing technological and operational factors. The challenge is amplified because capable adversaries are extremely active in seeking to penetrate DOD systems, compromise command and control, to steal or destroy sensitive and strategic information, and to gain an upper hand on U.S. forces and warfighting capability. Consequently, DOD is pursuing the alignment of existing vast IT networks

into JIE. First and foremost, JIE will improve mission effectiveness. It is intended to enable and empower our military's decisive edge—our people—by providing warfighters and our mission partners a shared IT infrastructure consisting of federated networks with common configurations and management, and a common set of enterprise services, within a single security architecture.

The JIE will change the way we assemble, configure, and use new and legacy information technologies. It will consist of enterprise level network operations centers that will reduce the complexity and ambiguity of seeing and controlling the numerous networks within DOD; a set of core data centers—significantly reducing the current number of DOD data centers while ensuring the information is secured and available where needed; and standard, single security architecture that will reduce the number of organizationally owned firewalls, unique routing algorithms, and inefficient routing of information that currently exists today. Together with the single, authoritative identity management and access control, emerging cloud capability, mobile computing devices and data-focused applications, and common IT enterprise services, JIE will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches across the system as a whole.

The ultimate beneficiary of JIE is the commander in the field, allowing for more innovative integration of information technologies, operations, and cyber security at a tempo more appropriate to today's fast-paced operational conditions. Specific benefits include:

- A standardized information and security architecture across software, servers, the network, mobile and fixed user computing, and identity and access control systems. Users and systems will be able to trust their connection from end to end with the assurance that the information and systems involved in a mission are correct and working even during a cyber attack. The JIE architecture will enable cyber operators at every level to see the status of the networks for operations and security and will provide standard resilience and cyber maneuver options for all cyber forces. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk. Most importantly, unlike the one size fits all networks DOD has now, the JIE will provide mission commanders more freedom to take operational risk with the networks since the risks can be contained to the decision support and systems specifically needed for that mission.
- Consolidation of data centers, operations centers, and help desks will enable users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location.
- A consistent DOD-wide IT architecture that defines enterprise standards and supports effective fielding of DOD capabilities in support of information sharing, as well as sustainment and integration of legacy systems.

DOD plans on utilizing the Services' existing programs, initiatives, and technical refresh to deploy or migrate to JIE standards utilizing specific implementation guidance.

Data Center Consolidation

An important aspect within JIE is the active consolidation of DOD's numerous data centers. These efforts are consistent with and support the Federal Data Center Consolidation Initiative being led by the Federal CIO. DOD has established four classes of data centers to assist in the development and execution of our data center consolidation strategy. These four types of data centers are:

- Core Data Center (CDC)—delivers enterprise services and provides primary migration point for systems and applications; these are our most important data centers, strategically located to provide speed of access to global information requirements;
- Installation Processing Node—provides local services to DOD installations and hosting systems not suited for CDCs, these will be located at the installation level, and will consolidate the duplicative data centers at the installations;
- Special Purpose Processing Node—provides compute and storage for fixed infrastructure or facilities, such as test ranges, labs, medical diagnostic equipment, and machine shops; and

- Tactical/Mobile Processing Node—provides support to the deployed warfighter at the tactical edge; these unique "data centers" directly support the warfighter in a disadvantaged or tactical environment, but connect back into the Generating Force information sources and core data centers.

DOD's data center consolidation efforts have been aided by section 2867 of P.L. 112–81, which was originally sponsored by the Senate Armed Services Committee. We have made significant progress in our data center consolidation, and have closed 277 data centers as of the first quarter pf fiscal year 2014.

Cloud Computing

Cloud Computing is becoming a critical component of the JIE and DOD's IT modernization efforts and will enable users the access to data anywhere, anytime on any approved device. One key objective is to drive the delivery and adoption of a secure, dependable, resilient multi-provider enterprise cloud computing environment that will enhance mission effectiveness and improve IT efficiencies. Cloud services will enhance warfighter mobility by providing secure access to mission data and enterprise services regardless of where the user is located and what device he or she uses.

My office continues to investigate new ways to leverage commercial cloud computing innovations and efficiencies to improve DOD. The nature of DOD's mission, and the risk to national security if DOD information were to be compromised, requires the careful evaluation of commercial cloud services, especially in areas of cybersecurity, continuity of operations, and resilience. To improve our cybersecurity posture with regards to commercial cloud computing, we are participating in the Federal Risk Authorization and Management Program and updating our own cybersecurity policies.

There are two key components of DOD's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DOD activities in unclassified and classified environments. The second is DOD's adoption of commercial cloud services that can meet DOD's cybersecurity needs while providing capabilities that are at least as effective and efficient as those provided internally.

Enterprise Services

As previously noted, enterprise services are those global applications that can be used by many, if not all users within DOD. They are a key element of achieving more effective operations and improved security across DOD. An example of this is Defense Enterprise Email, which is an enterprise messaging tool, built by consolidating existing disparate email servers into a global capable server and operated by the Defense Information Systems Agency (DISA) on a fee-for-service basis. The result is a common DOD enterprise email and contact address list and consolidated email service.

The enterprise directory service is being incorporated by many organizations in order to provide baseline authoritative enterprise identity data that is shareable across the enterprise via an automated synchronization service. Defense Enterprise Email is currently used by DISA, the U.S. Army, the Joint Staff, the Office of the Secretary of Defense, Defense Manpower Data Center, Office of Naval Research, Navy Recruiting Command, HQ Air Force, Air Force District Washington, U.S. European Command, U.S. Southern Command, U.S. Transportation Command, U.S. Africa Command, and U.S. Forces Japan. As of February 2014, there are 1.6 million enterprise email users on DOD's unclassified network and 150,000 users on the DOD Secret network, and continued adoption and consolidation to this capability is expected in the future.

CYBERSECURITY

Cybersecurity is one of the highest priorities of the administration and DOD. The primary cybersecurity goal of my office is ensuring that essential DOD missions are dependable and resilient in the face of cyber exploits and attacks by a capable adversary. This is also a primary concern driving the other improvement efforts, particularly JIE. This focus on mission assurance, rather than on computer or system security, is one of the primary changes in DOD's cybersecurity approach. This approach enables us to move from an approach of bolting on cyber security solutions to one where resilient, mission assurance, and cyber security characteristics will be built into the total information environment.

JIE gives certain operational commanders more freedom to take operational cyber security risks. We accomplish this by using "risk zones" in the design of the JIE computing and networks; these zones help keep the risks assumed by a particular mission from spilling over into other missions. This is also a significant change from

today's DOD networks which impose more operational constraints on commanders. Other primary cybersecurity goals include improved safe sharing with whatever partners a mission requires, and a continued need to keep a secret. Through refinement of the JIE concept, including the JIE single security architecture, we have concluded that all of these cyber security goals can be achieved, and DOD will have better joint warfighting decision support, better operational and acquisition agility, and better efficiency.

Like other IT efforts, cybersecurity is a team sport within DOD, and these efforts span many organizations. In particular, I work closely with others in the Office of the Secretary of Defense, U.S. Cyber Command, the Military Departments, and Defense Agencies to ensure cybersecurity issues are being addressed.

Single Security Architecture

A key priority in the last year has been the development of a unifying, joint cybersecurity approach for the design of the JIE. This is the JIE Single Security Architecture (SSA). Although many of the DOD's cyber security initiatives are common across all DOD organizations, each Military Service has had the ability to make important decisions about how to design computing and networks and about how to structure cyber defenses. This has led to several challenges, such as diversity in the cybersecurity protections of the DOD that does not provide a common level of protection for joint missions (because the IT for these missions is designed and operated by many organizations), and sometimes interferes with the collaborative attack detection, diagnosis, and reaction so necessary in a complex organization like DOD. Finally, the challenge caused by this diversity can interfere with a joint commander's ability to share information with external mission partners.

To solve these problems, the SSA provides for a common approach to the structure and defense of computing and the networks across all DOD organizations. This engineering of the cyber security approach "end-to-end" will significantly improve DOD's ability to resist cyber-attacks; to dampen the spread of successful attacks; and to detect, diagnose, and react to attacks in ways that are optimized for joint missions. Owing to the standardization and cyber data sharing of JIE, cyber defenders will have broad visibility into the computing and networks, and via secure remote management and automation, they will be able to much more quickly construct and execute defensive actions. In addition, the risk containment zones the SSA defines in the server computing and the network will enable joint commanders to better contain cyber risk to mission while sharing as broadly with external partners as a mission requires. It will also make development of new decision support capabilities simpler and easier since many program offices will not need to worry about most cybersecurity protections, but will instead be able to build software applications on top of the standard protections and situational awareness capabilities provided by JIE.

The DOD CIO published a new Strategy for Defending Networks, Systems, and Data in October 2013. The strategy identifies strategic imperatives to ensure the protection, integrity, and assurance of DOD cyber assets. It is focused in four key areas: establishing a Resilient Cyber Defense Posture; Transform Cyber Defense Operations; Enhance Cyber Situational Awareness; and Assure Survivability against Highly Sophisticated Cyber Attacks. In the near term, we will be finalizing the Implementation Plan for the strategy. To ensure success going forward, we will collaborate closely with others in DOD.

INFORMATION TECHNOLOGY AND CYBER WORKFORCE DEVELOPMENT

A critical component of readiness is a workforce that is trained and equipped. DOD is in the process of implementing a comprehensive strategy to transform its legacy IT and information assurance personnel, as well as critical personnel in non-traditional IT occupations, into a cohesive cyberspace workforce which includes a strong cybersecurity workforce component. The DOD Cyberspace Workforce Strategy is focused on recruiting, training, and retaining the necessary workforce to build and operate our networks as well as defend U.S. national interests in cyberspace. The workforce must be properly sized and properly trained, and there must be career progression that encourages growth and development of broad ranging skillsets, such as building a defensible architecture, acquiring secure technologies, securely operating systems and networks, analyzing cyber threats, and planning cyberspace operations. We are working across DOD to realize competitive hiring and retention initiatives, and institute robust training and education programs, to achieve a world class, mission ready cyberspace workforce.

Space-based PNT provides crucial capability to military, civil, and commercial users worldwide. We are working to better integrate the services of the Global Positioning Systemas the primary means of delivering PNT which provides our Nation

and allies the ability to precisely navigate anywhere in the world. Our PNT architecture provides our Nation and allies precise target location, the ability to strike with a minimum of collateral damage, navigation capabilities that support logistics, command and control, friendly force tracking, and precise timing. This latter feature is critical to encryption, synchronization, and integration of data networks within the communications and cyber enterprises. With this understanding, we are working, as a high priority, several infrastructure upgrades to protect this critical piece of cyber terrain.

Spectrum has become increasingly important not only to DOD's missions, but to consumers and the economy of the Nation as a whole. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and DOD's cyber operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from DOD's increasing reliance on spectrum-dependent technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the DOD is fully committed to the President's 500 MHz initiative to make spectrum available for commercial broadband use, the implementation of more effective and efficient use of this finite radio-frequency spectrum and the development of solutions to meet these goals while ensuring national security and other Federal capabilities are preserved.

To that end, DOD has developed a plan that will make 25MHz of spectrum available to commercial industry on a shared basis, thus achieving a balance between expanding wireless and broadband capabilities for the Nation and the need for access to support warfighting capabilities in support of our national security.

CONCLUSION

Maintaining information dominance for the warfighter is critical to our national security. The efforts outlined above will ensure that DOD's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of financial resources. I ask that you strongly support, authorize, and fund DOD's key cybersecurity and information technology modernization programs. I want to thank you for your interest.

Senator SHAHEEN. Thank you very much.

Mr. Powner.

STATEMENT OF DAVID A. POWNER, DIRECTOR, INFORMATION TECHNOLOGY AND MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Chairwoman Shaheen, Ranking Member Ayotte, and members of the subcommittee, I appreciate the opportunity to testify this afternoon on improving IT acquisition at DOD.

Of the $82 billion the Federal Government spends on IT annually, DOD spends almost half of this, $40 billion. Of that, about $25 billion is spent on legacy systems. Therefore, it is important that DOD not only acquires new systems, on time and within budget, but that it also efficiently manages existing systems.

Regarding systems acquisitions, too often we hear of failed projects like ECSS. These complex projects, though, can be delivered successfully when there is appropriate transparency, accountability, oversight, and program management.

Starting with transparency, the IT Dashboard was put in place to highlight the status and CIO assessments of approximately 700 major IT investments across 27 departments. This public dissemination of each project's status is to allow the Office of Management and Budget (OMB) and Congress to hold agencies accountable for results and performance. Many agencies have accurate information on the Dashboard, and that information is used to tackle troubled projects. DOD does not. DOD reports 93 IT investments on the Dashboard—81 are in green status, meaning low risk, 12 are in

yellow status, meaning medium risk, and there are no projects rated as high risk, or red.

Chairwoman Shaheen, there are many problems here. First, some of these projects should be red, based on the review that you currently mentioned in your opening statement. Second, the data is not always current since CIO ratings have not been updated since September 2012. Third, there are major investments that are not even listed on the Dashboard.

Given the amount DOD spends annually on IT and its not-so-stellar track record, Congress absolutely needs a clear picture of what these investments are and how they are performing. Therefore, DOD needs to ensure that all projects are on the Dashboard and accurately updated.

Once this transparency is improved, key IT executives need to be accountable, along with the appropriate business leaders responsible for these projects.

We have seen successful oversight performed by using a tiered portfolio-based governance structure, meaning that not all DOD major investments need to be overseen exactly the same way. Some of the 93 investments can be delegated below the CIO level. Most should be overseen by the CIO, and some of DOD's major priorities likely demand oversight above the CIO level.

Turning to program management, we recently issued a report that showcases successful IT acquisitions. One of those projects was the Defense Information Systems Agency's (DISA) global combat support system. Several best practices increased the likelihood that IT acquisitions will be delivered on time and within budget. This starts with getting the requirements right by involving the right users and prioritizing those requirements. A big takeaway from these successful stories was that each of these successful investments was an increment of a larger project. Tackling projects in increments is a best practice.

We have ongoing work that is currently looking at agencies, including DOD, and how they are tackling these large investments in more manageable pieces. That report will be issued in the spring and will show that DOD is not acquiring systems in small enough increments.

Turning now to operational systems, OMB started a data center consolidation effort in 2010 to address the Government's low server utilization rates estimated on average at 10 to 15 percent, far below the industry standard of 60 percent. This effort was to result in $3 billion in savings across all departments. DOD has done a really good job when it comes to data centers, Chairwoman Shaheen. They have identified 2,000 centers, to date. They have closed over 250 centers, and they have reported $875 million in savings. They have also reported to us in the current review that their savings alone could match OMB's government-wide goal of $3 billion by the end of 2015.

OMB recently expanded the data center consolidation effort into a larger initiative to eliminate additional duplicative spending in administrative and business systems. As part of this, DOD identified 26 opportunities where duplication existed in areas like enterprise software, security infrastructure, and network operations. DOD estimates that these 26 opportunities, which include their

data center consolidation efforts, could result in savings that exceed $5 billion. Given the magnitude of DOD's potential savings associated with duplicative systems and data center consolidation, it is essential that they have support for and track these savings, and not use poor systems or processes as an excuse for not realizing billions in savings.

In summary, by tackling duplicative IT systems and consolidating data centers, DOD can save over $5 billion through 2015 alone. Systems acquisition performance can be greatly improved by reporting accurately and timely on the IT Dashboard, improving governance, acquiring incrementally, and following program management best practices.

This concludes my statement. I would be pleased to respond to questions.

[The prepared statement of Mr. Powner follows:]

PREPARED STATEMENT BY MR. DAVID A. POWNER

Chairwoman Shaheen, Ranking Member Ayotte, and members of the subcommittee: I am pleased to be here today to discuss how best practices and major information technology (IT) reform initiatives can help the Department of Defense (DOD) better acquire and manage IT investments. As reported to the Office of Management and Budget (OMB), Federal agencies plan to spend at least $82 billion on IT in fiscal year 2014. Of this amount, DOD plans to spend about $39.6 billion, or 48 percent of the government's total IT spending. Given the size of the department's investments and the criticality of many of these systems to the security and defense of the Nation, it is important that DOD successfully acquire them—that is, ensure that they are acquired on time and within budget, and that they deliver expected benefits and results.

However, as we have previously reported and testified, Federal IT projects too frequently fail and incur cost overruns and schedule slippages while contributing little to mission-related outcomes.[1] During the past several years, we have issued multiple reports and testimonies on best practices for major acquisitions and Federal initiatives to acquire and improve the management of IT investments.[2] In those reports, we made numerous recommendations to Federal agencies and OMB to further enhance the management and oversight of IT programs. Further, we highlighted several examples of DOD investments that failed to, or only partially delivered results within planned cost and schedule estimates.

As discussed with subcommittee staff, I am testifying today on how best practices and major IT reform initiatives can help DOD better acquire and manage IT investments. Accordingly, my testimony specifically focuses on the critical success factors of major IT acquisitions and their importance to improving IT investment oversight and management. I will also address several initiatives put into place by OMB to

[1] See, for example, Government Accountability Office (GAO), Information Technology: OMB and Agencies Need to More Effectively Implement Major Initiatives to Save Billions of Dollars, GAO–13–796T (Washington, DC: July 25, 2013); Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program, GAO–10–340 (Washington, DC: May 5, 2010); and Polar-Orbiting Environmental Satellites: With Costs Increasing and Data Continuity at Risk, Improvements Needed in Tri-agency Decisionmaking, GAO–09–564 (Washington, DC: June 17, 2009).

[2] See, for example, GAO, Information Technology: Leveraging Best Practices to Help Ensure Successful Major Acquisitions, GAO–14–183T (Washington, DC: Nov. 13, 2013); Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects, GAO–13–524 (Washington, DC: June 13, 2013); Data Center Consolidation: Strengthened Oversight Needed to Achieve Billions of Dollars in Savings, GAO–13–627T (Washington, DC: May 14, 2013); Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal, GAO–13–378 (Washington, DC: Apr. 23, 2013); Information Technology Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies, GAO–13–98 (Washington, DC: Oct. 16, 2012); Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed, GAO–12–742 (Washington, DC: July 19, 2012); Information Technology: Critical Factors Underlying Successful Major Acquisitions, GAO–12–7 (Washington, DC: Oct. 21, 2011); Information Technology: Continued Attention Needed to Accurately Report Federal Spending and Improve Management, GAO–11–831T (Washington, DC: July 14, 2011); and Information Technology: Investment Oversight and Management Have Improved but Continued Attention Is Needed, GAO–11–454T (Washington, DC: Mar. 17, 2011).

address the transparency of IT investments and to review troubled and duplicative existing projects. All work on which this testimony is based was performed in accordance with generally accepted government auditing standards or all sections of GAO's Quality Assurance Framework that were relevant to our objectives. Those standards and the framework require that we plan and perform our audits and engagements to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives; the framework also requires that we discuss any limitations in our work. We believe that the information, data, and evidence obtained and the analysis conducted provide a reasonable basis for our findings and conclusions based on our objectives. A more detailed discussion of the objectives, scope, and methodology of this work is included in each of the reports on which this testimony is based.[3]

BACKGROUND

IT should enable government to better serve the American people. However, despite spending hundreds of billions on IT since 2000, the Federal Government has experienced failed IT projects and has achieved little of the productivity improvements that private industry has realized from IT. Too often, Federal IT projects run over budget, behind schedule, or fail to deliver results. In combating this problem, proper oversight is critical.

Both OMB and Federal agencies have key roles and responsibilities for overseeing IT investment management and OMB is responsible for working with agencies to ensure investments are appropriately planned and justified. However, as we have described in numerous reports,[4] although a variety of best practices exist to guide their successful acquisition, Federal IT projects too frequently incur cost overruns and schedule slippages while contributing little to mission-related outcomes.

Agencies have reported that poor-performing projects have often used a "big-bang" approach—that is, projects that are broadly scoped and aim to deliver capability several years after initiation. For example, in 2009 the Defense Science Board reported that DOD's acquisition process for IT systems was too long, ineffective, and did not accommodate the rapid evolution of IT.[5] The board reported that the average time to deliver an initial program capability for a major IT system acquisition at DOD was over 7 years.

As previously mentioned, and as seen in figure 1, Defense accounts for 48 percent of the fiscal year 2014 Federal Government's IT budget.

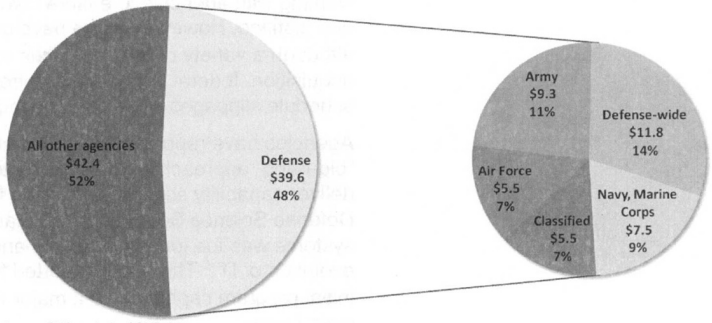
---

[3] GAO–13–524; GAO, Information Technology Reform: Progress Made; More Needs to Be Done to Complete Actions and Measure Results, GAO–12–461 (Washington, DC: Apr. 26, 2012); IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making, GAO–12–210 (Washington, DC: Nov. 7, 2011); GAO–12–7; Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy, GAO–11–262 (Washington, DC: Mar. 15, 2011); and Information Technology: OMB's Dashboard has Increased Transparency and Oversight, but Improvements Needed, GAO–10–701 (Washington, DC: July 16, 2010).

[4] See, for example, GAO, FEMA: Action Needed to Improve Administration of the National Flood Insurance Program, GAO–11–297 (Washington, DC: June 9, 2011); GAO–10–340; Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk, GAO–10–158 (Washington, DC: Jan. 29, 2010); and GAO–09–564.

[5] Defense Science Board, Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology (Washington, DC: March 2009).

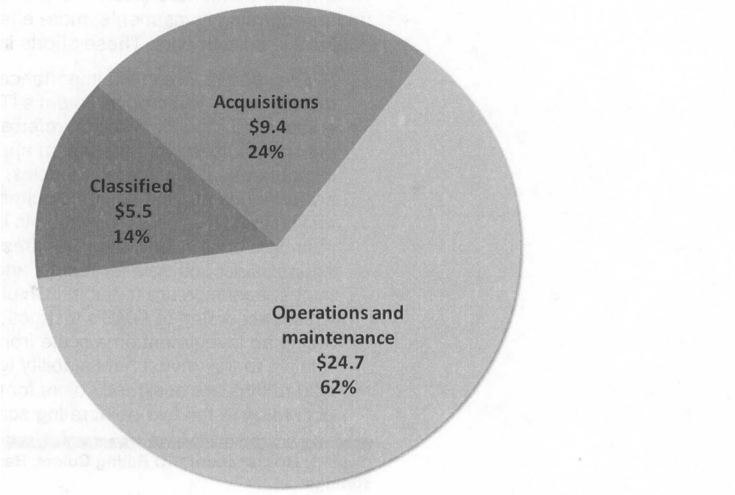
Figure 1: Defense Percentage of Federal Fiscal Year 2014 IT Spending (dollars in billions)



Source: GAO analysis of OMB data.

Of the department's $39.6 billion IT budget, approximately 14 percent is to be spent on classified systems. Of the remaining $34 billion, about one-quarter is to be spent on acquiring new investments, and the rest is to be spent operating and maintaining existing or legacy systems. This is illustrated in figure 2.

Figure 2: Defense's Fiscal Year 2014 IT Spending (dollars in billions)



Source: GAO analysis of OMB data.

Further, over the past several years, we have reported that overlap and fragmentation among government programs or activities could be harbingers of unnecessary duplication.[6] Thus, the reduction or elimination of duplication, overlap, or fragmentation could potentially save billions of tax dollars annually and help agencies provide more efficient and effective services.

[6] GAO, 2013 Annual Report: Actions Needed to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits, GAO–13–279SP (Washington, DC: Apr. 9, 2013), Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue, GAO–12–342SP (Washington, DC: Feb. 28, 2012), and Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue, GAO–11–318SP (Washington, DC: Mar. 1, 2011).

OMB Has Launched Major Initiatives for Overseeing Investments

OMB has implemented a series of initiatives to improve the oversight of underperforming investments, more effectively manage IT, and address duplicative investments. These efforts include the following:

- IT Dashboard. Given the importance of transparency, oversight, and management of the government's IT investments, in June 2009 OMB established a public website, referred to as the IT Dashboard, that provides detailed information on approximately 700 major IT investments at 27 Federal agencies, including ratings of their performance against cost and schedule targets. The public dissemination of this information is intended to allow OMB, other oversight bodies including Congress, and the general public to hold agencies accountable for results and performance. Among other things, agencies are to submit Chief Information Officer (CIO) ratings, which, according to OMB's instructions, should reflect the level of risk facing an investment on a scale from 1 (high risk) to 5 (low risk) relative to that investment's ability to accomplish its goals. Ultimately, CIO ratings are assigned colors for presentation on the Dashboard, according to the five-point rating scale, as illustrated in table 1.

Table 1: IT Dashboard CIO Rating Colors, Based on a Five-Point Scale for CIO Ratings

Rating (by agency CIO)	Color
1-High risk	Red
2-Moderately high risk	Red
3-Medium risk	Yellow
4-Moderately low risk	Green
5-Low risk	Green

Source: OMB's IT Dashboard.

- TechStat reviews. In January 2010, the Federal CIO began leading TechStat sessions—face-to-face meetings to terminate or turnaround IT investments that are failing or are not producing results. These meetings involve OMB and agency leadership and are intended to increase accountability and transparency and improve performance. Subsequently, OMB empowered agency CIOs to hold their own TechStat sessions within their respective agencies. According to the former Federal CIO, the efforts of OMB and Federal agencies to improve management and oversight of IT investments have resulted in almost $4 billion in savings.
- Federal Data Center Consolidation Initiative. Concerned about the growing number of Federal data centers, in February 2010 the Federal CIO established the Federal Data Center Consolidation Initiative. This initiative's four high-level goals are to promote the use of "green IT" [7] by reducing the overall energy and real estate footprint of government data centers; reduce the cost of data center hardware, software, and operations; increase the overall IT security posture of the government; and shift IT investments to more efficient computing platforms and technologies. OMB believes that this initiative has the potential to provide about $3 billion in savings by the end of 2015.
- PortfolioStat. In order to eliminate duplication, move to shared services, and improve portfolio management processes, in March 2012 OMB launched the PortfolioStat initiative. Specifically, PortfolioStat requires agencies to conduct an annual agencywide IT portfolio review to, among other things, reduce commodity IT [8] spending and demonstrate how their IT investments align with the agency's mission and business functions.[9]

[7] "Green IT" refers to environmentally sound computing practices that can include a variety of efforts, such as using energy efficient data centers, purchasing computers that meet certain environmental standards, and recycling obsolete electronics.

[8] According to OMB, commodity IT includes services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions).

[9] OMB, Implementing PortfolioStat, Memorandum, M–12–10 (Washington DC: Mar. 30, 2012).

PortfolioStat is designed to assist agencies in assessing the current maturity of their IT investment management process, making decisions on eliminating duplicative investments, and moving to shared solutions in order to maximize the return on IT investments across the portfolio. OMB believes that the PortfolioStat effort has the potential to save the government $2.5 billion over the next 3 years by, for example, consolidating duplicative systems.

OPPORTUNITIES EXIST TO IMPROVE DEFENSE'S ACQUISITION AND MANAGEMENT OF MAJOR IT INVESTMENTS

Given the magnitude of DOD's annual IT budget, which was $39.6 billion in fiscal year 2014, it is important that the department leverage all available opportunities to ensure that its IT investments are acquired in the most effective manner possible. To do so, the department can rely on IT acquisition best practices, and initiatives such as OMB's IT Dashboard, and OMB-mandated TechStat sessions.

Best Practices Are Intended to Help Ensure Successful Major Acquisitions

In 2011, we identified seven successful investment acquisitions and nine common factors critical to their success, and noted that the factors support OMB's objective of improving the management of (1) large-scale IT acquisitions across the Federal Government, and (2) wide dissemination of these factors could complement OMB's efforts.[10] Specifically, we reported that Federal agency officials identified seven successful investment acquisitions, in that they best achieved their respective cost, schedule, scope, and performance goals.[11] Notably, all of these were smaller increments, phases, or releases of larger projects. For example, the DOD investment in our sample, Defense Global Combat Support System-Joint (Increment 7), was a smaller portion of an ongoing investment. The common factors critical to the success of three or more of the seven investments are generally consistent with those developed by private industry and are identified in table 2.

Table 2: Common Critical Success Factors

Program officials were actively engaged with stakeholders
Program staff had the necessary knowledge and skills
Senior department and agency executives supported the programs
End users and stakeholders were involved in the development of requirements
End users participated in testing of system functionality prior to formal end user acceptance testing
Government and contractor staff were consistent and stable
Program staff prioritized requirements
Program officials maintained regular communication with the prime contractor
Programs received sufficient funding

Source: GAO analysis of agency data.

Regarding DOD's Global Combat Support System-Joint (Increment 7), officials cited six factors that were critical to this investment's success. Among others, officials noted that senior department executives supported the program, end users and stakeholders were involved in the development of requirements which were then prioritized, and government and contractor staff were consistent and stable.

IT Dashboard Can Improve the Transparency Into and Oversight of Defense IT Investments

The IT Dashboard serves an important role in allowing OMB and other oversight bodies to hold agencies accountable for results and performance. However, we reported in October 2012 that opportunities existed to improve transparency and oversight of investment risk at selected agencies, including DOD.[12] Specifically, we

[10] GAO–12–7.

[11] The seven investments were: (1) Commerce's Decennial Response Integration System; (2) Defense's Defense Global Combat Support System-Joint (Increment 7); (3) Department of Energy's Manufacturing Operations Management Project; (4) DHS's Western Hemisphere Travel Initiative; (5) Department of Transportation's Integrated Terminal Weather System; (6) Internal Revenue Service's Customer Account Data Engine 2; and (7) Veterans Affairs Occupational Health Recordkeeping System.

[12] GAO–13–98.

found that among the agencies we reviewed, DOD was unique in that its CIO ratings on the Dashboard reflected additional considerations beyond OMB's instructions. For example, briefing slides prepared for DOD's 2011 CIO rating exercise identified the need to "balance" CIO ratings, and advised that yellow or red ratings could lead to an OMB review. That report further noted that DOD did not rate any of its investments as either high or moderately high risk and that in selected cases, these ratings did not appropriately reflect significant cost, schedule, and performance issues reported by GAO and others.

We also highlighted three DOD investments that experienced significant performance problems and were part of a GAO high-risk area (business systems modernization); however, they were all rated low risk or moderately low risk by the DOD CIO. For example, in early 2012, we reported that Air Force's Defense Enterprise Accounting and Management System faced a 2-year deployment delay and an estimated cost increase of about $500 million from an original life-cycle cost estimate of $1.1 billion (an increase of approximately 45 percent), and that assessments by DOD users had identified operational problems with the system, such as data accuracy issues, an inability to generate auditable financial reports, and the need for manual workarounds.[13] In July 2012, the DOD Inspector General reported that the system's schedule delays were likely to diminish the cost savings it was to provide, and would jeopardize the department's goals for attaining an auditable financial statement. DOD's CIO rated the Dense Enterprise Accounting and Management System low risk or moderately low risk from July 2009 through March 2012.

Moreover, DOD did not apply its own risk management guidance to the ratings, which reduces their value for investment management and oversight. Therefore, we recommended that DOD ensure that its CIO ratings reflect available investment performance assessments and its risk management guidance. DOD concurred with our recommendation. Nonetheless, the Dashboard currently shows that for DOD's 93 major investments, 81 are low or moderately low risk (green), 12 are medium risk (yellow), and none are moderately high or high risk (red).

TechStat Reviews Can Help Highlight and Evaluate Poorly Performing Investments

TechStat reviews were initiated by OMB to enable the Federal Government to intervene to turnaround, halt, or terminate IT projects that are failing or are not producing results. In 2013, we reported that OMB and selected agencies had held multiple TechStats, but that additional OMB oversight was needed to ensure that these meetings were having the appropriate impact on underperforming projects and that resulting cost savings were valid.[14] We noted that OMB and selected agencies had tracked and reported positive results from TechStats, with most resulting in improved governance. Agencies also reported projects with accelerated delivery, reduced scope, or termination. We also found that OMB reported in 2011 that Federal agencies achieved almost $4 billion in life-cycle cost savings as a result of TechStat sessions. However, we were unable to validate OMB's reported results because OMB did not provide artifacts showing that it ensured the results were valid. Among other things, we recommended that OMB require agencies to report on how they validated the outcomes. OMB generally agreed with this recommendation.

We also found that as of April 2013, OMB reported conducting 79 TechStats on 55 investments at 23 Federal agencies, including DOD. The four DOD investments that were reviewed included the Expeditionary Combat Support System, which received three TechStats. We recently testified that in December 2012, DOD canceled the Expeditionary Combat Support System after having spent about a billion dollars and missing multiple milestones, including failure to achieve deployment within 5 years of obligating funds.[15] The system was to provide the Air Force with a single, integrated logistics system that was to control and account for about $36 billion of inventory. We issued several reports on this system and found that, among other things, the program was not fully following best practices for developing reliable schedules and cost estimates.[16] Among other things, we had recommended that DOD ensure that any future system deficiencies identified through independent as-

---

[13] GAO, DOD Financial Management: Reported Status of Department of Defense's Enterprise Resource Planning Systems, GAO–12–565R (Washington, DC: Mar. 30, 2012) and DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals, GAO–12–134 (Washington, DC: Feb. 28, 2012).

[14] GAO–13–524.

[15] GAO–13–796T.

[16] GAO, DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed, GAO–11–53 (Washington, DC: Oct. 7, 2010) and DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals, GAO–12–134 (Washington, DC: Feb. 28, 2012).

sessments be resolved or mitigated prior to further deployment of the Expeditionary Combat Support System.

In addition to efficiently acquiring IT investments, it is also important for DOD to efficiently manage its existing IT systems, especially since the agency plans to spend about $25 billion in fiscal year 2014 on these systems. To do so, DOD can rely on Federal initiatives designed to reduce inefficiencies, redundancy, and duplication in IT investments, as discussed in the following section.

DOD Could Consolidate Hundreds of Data Centers, Leading to Billions in Savings

In an effort to consolidate the growing number of Federal data centers, in 2010, OMB launched a data center consolidation initiative. As part of this initiative, agencies developed plans to consolidate data centers; however, these plans were incomplete and did not include best practices. In addition, although we reported that agencies had made progress on their data center closures, OMB had not determined initiative-wide cost savings, and oversight of the initiative was not being performed in all key areas.[17] Among other things, we recommended that agencies complete inventories and plans, with which most agencies agreed. Finally, as part of ongoing follow-up work, we determined that agencies closed additional data centers, but that the number of Federal data centers was significantly higher than previously estimated by OMB. Specifically, we testified in 2013 that OMB reported approximately 3,133 data centers in December 2011.[18] However, as of July 2013, 22 of the 24 agencies had collectively reported 6,836 data centers in their inventories, an increase of approximately 3,700. Of these, DOD reported 1,922 facilities. Since DOD's original goal was to consolidate from 936 data centers to 392 and to save an estimated $2.2 billion, this increase in inventory opens the possibility of consolidating even more centers and realizing billions in cost savings.

PortfolioStat Can Be Used to Address Duplicative DOD Investments and Realize Cost Savings

OMB's PortfolioStat initiative is designed to assist agencies in assessing the current maturity of their IT portfolio management process and making decisions on eliminating duplication—which we reported on in February 2012. Specifically, we found 31 potentially duplicative investments totaling approximately $1.2 billion at DOD, but that the department had begun taking actions to address this duplication.[19] For example, according to Defense officials, four of the Navy acquisition management investments—two for Naval Sea Systems Command and two for Space and Naval Warfare Systems Command—would be reviewed to determine whether these multiple support systems are necessary. In addition, DOD reported that the Air Force was in the process of developing a single contract writing system to replace the five potentially duplicative investments we had identified. Additionally, in September 2013, we found additional potential duplication within DOD's health care and dental management investments, totaling over $30 million.[20] Again, department officials described plans to address this. The existence of this potential duplication reinforces the need for the department to continue to take firm actions to address IT duplication and inefficiencies.

We recently reported[21] and testified[22] on PortfolioStat, including DOD's efforts to address duplication through the initiative. Specifically, we noted that, although OMB had previously stated that PortfolioStat was expected to result in savings of approximately $2.5 billion through fiscal year 2015, the 26 DOD PortfolioStat initiatives alone, including data center consolidation, were expected by the department's CIO to save between $3.2 billion and $5.2 billion through fiscal year 2015, and to result in efficiencies between $1.3 billion and $2.2 billion per year beginning in fiscal year 2016. However, DOD was unable to show support for how all of these savings were calculated, citing a variety of reasons such as dependence on accurate reporting by departmental components and the lack of granular information from accounting systems. While recognizing the challenges the department faces in obtain-

---

[17] GAO, Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings, GAO–11–565 (Washington, DC: Jul. 26, 2011) and Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed, GAO–12–742 (Washington, DC: Jul. 19, 2012).

[18] GAO–13–796T.

[19] GAO, Information Technology: Departments of Defense and Energy Need to Address Potentially Duplicative Investments, GAO–12–241 (Washington, DC: Feb 17, 2012).

[20] GAO, Information Technology: Key Federal Agencies Need to Address Potentially Duplicative Investments, GAO–13–718 (Washington, DC: Sep. 12, 2013).

[21] GAO, Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings, GAO–14–65 (Washington, DC: Nov. 6, 2013); and GAO–13–378.

[22] GAO–13–685T and GAO–13–627T.

ing the support for consolidation opportunities identified by its components, we also noted that obtaining this information is critical to ensuring that planned savings and cost avoidance are realized.

Accordingly, we recommended that DOD take steps to improve its PortfolioStat implementation. The department concurred with our recommendation to obtain support for estimated savings, but disagreed with our recommendation to fully describe the consolidation of commodity IT spending under the CIO in future OMB reporting. The department stated that it did not intend to follow OMB's guidance to consolidate commodity IT spending under the CIO. However, by not following OMB's guidance, DOD is missing an opportunity to achieve additional cost savings across the department.

To manage its annual investment of over $39 billion in IT, DOD needs to leverage best practices, improve transparency of its major investments, and review troubled projects through TechStat reviews. To do so, DOD can use the common factors critical to the successful management of large-scale IT acquisitions, which should result in the more effective delivery of mission-critical systems. Further, DOD needs to continue to improve the accuracy of its information on the Dashboard in order to provide greater transparency and even more attention to the billions of dollars invested in troubled projects. In addition, more departmental TechStat reviews are needed to focus management attention on additional troubled projects and establish clear action items to turn the projects around or terminate them.

With the possibility of over $5.3 billion in savings from the data center consolidation and PortfolioStat initiatives, DOD should continue to identify consolidation opportunities in both data centers and commodity IT. In addition, better support for the estimates of cost savings associated with the opportunities identified would increase the likelihood that these savings will be achieved.

Chairwoman Shaheen, Ranking Member Ayotte, and members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO CONTACT AND STAFF ACKNOWLEDGMENTS

If you or your staffs have any questions about this testimony, please contact me at (202) 512–9286 or at pownerd@gao.gov. Individuals who made key contributions to this testimony are Dave Hinchman (Assistant Director), Rebecca Eyler, and Kevin Walsh. (311404)

Senator SHAHEEN. Thank you all very much both for being here and for your testimony, and for what I know will be a good discussion.

I know that Senator Ayotte is going to address some of the questions that Mr. Powner raised in his testimony. When Mr. Powner says that none of the projects that are on the Dashboard—none of those are listed as high risk, is that because there is a genuine belief that none of them are high risk? I assume that means at risk of not coming to successful conclusion. Are you suggesting, Mr. Powner, that those projects are not working in the way they should when you describe high risk?

Mr. POWNER. I think in order to manage problem projects, you need to acknowledge you have a problem. So if you look at our review of the MAIS programs, there are 40 MAIS programs, I can identify several of those MAIS programs that clearly, I believe, should be red and should be managed aggressively as red projects so you get them back on track. They are overrunning. The schedules are being pushed out. I think if you acknowledge they are red, you govern those projects differently if you acknowledge that you have a problem. So that is what we would like to see. We would like to see more of those projects as red.

There are 93 major investments. There are a lot of complex projects there. It is not that they are doing a bad job that they are red. There are red projects across programs. There are red projects

in the private sector. But you cannot fix the problems unless you acknowledge you have a problem.

Senator SHAHEEN. So can I ask if you would respond to that?

Ms. TAKAI. Let me respond as it relates to the reporting on the Dashboard, and then Ms. McFarland can speak to some of the acquisition processes.

First of all, I think I want to make sure that we acknowledge that there is a challenge for us in actually getting a clear rating in terms of a red, yellow, and green. I certainly do not want to walk away from the fact that it is a very difficult situation for us in terms of being sure that we have the right categorization and we are communicating that categorization correctly. So I want to make sure I make that statement.

Second of all, I think to answer your question, certainly because of the categorization issues, I would not necessarily depict our current ratings that are out on the Dashboard as being 100 percent correct. That is right. We are now working on trying to do two things: number one, to get a better alignment of the way that we have been doing the ratings with the way the ratings have been defined in the OMB Dashboard. That is something, again because some of the complexities, we have not done. Ms. McFarland's organization and mine have been working on a new directive that will better define exactly what the status is.

The second challenge and a part of doing——

Senator SHAHEEN. Can I interrupt just a minute?

Ms. TAKAI. Sure.

Senator SHAHEEN. Are you in agreement with Mr. Powner that accurately reflecting the level of risk involved in a project is helpful in managing it properly?

Ms. TAKAI. Yes, ma'am. Certainly it is important that we understand what the challenges are. However, I would add though, as Mr. Powner said, we do often recognize that our programs need attention. That is actually one of the big benefits of our current DOD 5000 process. It really does highlight where we have issues and where we need to take action. I think we need to make sure that the actions that we are taking are accurately reflected in our ratings, so that we have visibility of the actions we are taking going forward.

Senator SHAHEEN. Is there something with respect to the way the ratings are done that make it particularly challenging for DOD, or will the 5000 process help identify that? What do you see as changing in order to more effectively be able to rate the risk involved with those projects?

Ms. TAKAI. One of the challenges that I will comment on, I know Ms. McFarland will have a comment as well, is the way we rate programs and the judgments that we make on programs today are really driven by the 5000 process. They do not necessarily fit well with the quarterly reporting process that is part of what OMB and the OMB Dashboard have. Consequently, it tends to result in us having the same rating for a longer period of time. One of the things Ms. McFarland and I are working on is how to make sure that we have a rating structure that does not appear to be different from what is being reported in our milestone decision process in the DOD 5000. That has been one of our challenges to this point,

and I think it is the effort that her organization and my organization are working together or to make sure we have better clarity.

Ms. MCFARLAND. Yes. Frankly, what Teri was talking about is what we are trying to change. When we just changed the 5000 over the last couple of months, released the interim, some of the things that you have been highlighting, along with the ranking member, in terms of how to do IT acquisition, is changing our culture internally on how we look at risk.

The challenge we have right now is that we have a system called the Defense Acquisition Management Information Research (DAMIR). It reports based on a very distinct approach from weapons systems. For us, we focus on cost, schedule, and performance. Risk is embedded in each, and we have multiple players who come in, the program manager, the OSD functional staff, and we all rate on a program. Those two from the standpoint of IT have to be aligned. Right now there is a difference in lexicon and how we think. We drafted a first effort to try to look at how we take and make those risk factors look the same so we do not report on two metrics and confuse people even more.

Senator SHAHEEN. Do you work with the GAO as you are trying to make some of these alignments to best assess what is going on?

Ms. TAKAI. Yes, ma'am. One of the things that we have been discussing is the way that we are looking at some of the ratings to make sure that they are aligned with the way the GAO is looking. Also, OMB is actually looking at those ratings because it is really a GAO reporting of what is in the OMB Dashboard. It is very important that we are consistent because otherwise the other concern I have is that if we are different, then if you go and look at another agency and you see a rating. You certainly do not want to hear DOD's ratings are a little different, which I am sure you hear a lot from us on other things.

Senator SHAHEEN. No, we never hear that. [Laughter.]

Ms. TAKAI. That is an important thing not only from the standpoint of us being aligned with OMB, but also so there is consistency of reporting so that when you look at the reporting, you are getting an accurate picture.

Senator SHAHEEN. Thank you.

Mr. Powner, did you want to add something to that?

Mr. POWNER. I would just add that the interim 5000 guidance, I think, where you could tailor it to different types of acquisition software, intensive hardware, using an incremental approach, and the Dashboard were put in place to change culture and Government. Monthly ratings by a CIO is something that is a challenge for not only DOD but for others, but it is a good challenge. If you cannot do it in a month, strive to do it in a quarter, strive to do in 6 months. That is better than what we have gotten historically. It was a push, but I think it is the appropriate push.

I would add that DOD has large acquisition in IT. There are a lot of IT acquisitions that are large and complex that need to follow the rigor of a 5000. Other IT can be acquired more incrementally. You still want rigor, but you do not necessarily have to have the exact rigor that you have with all the details in the 5000. Having that flexibility in the current interim guidance is very good. You hear about agile development or going incrementally.

We have a report that I know Senator Ayotte is very involved with for the Senate Homeland Security and Governmental Affairs Committee, where we are looking at incremental development across the Federal Government. We took 37 investments at DOD. OMB has some guidance that said everyone has to do everything in 6 months. One out of 37 at DOD is going to deliver in 6 months. DOD said that is unrealistic. I agree, but they said we will strive for 12 to 18 months. We said let us bump it up to 12 months. Of those 37 investments, only 10, so about a quarter of the investments, are going to deliver something in a year. So you still have a lot of projects that do not deliver anything for years, and that is the mode we need to get out of in the Government.

Senator SHAHEEN. Thank you.

Senator Ayotte, we have been talking about the IT Dashboard.

Senator AYOTTE. Thank you. I apologize, I had to leave for a minute.

On the Dashboard issue, as I read the GAO report, I see that essentially we can save a pretty substantial amount of money. Then when I look at it, we are spending $39 billion on IT systems for DOD in fiscal year 2014. That is a huge amount of money. I see in your report, I am really fascinated, page 5 where you basically say we have overlap, fragmentation, and we have unnecessary duplication so that there could be much more taxpayers' dollars saved if we could get that one issue right. You have probably already addressed this to some extent, but what do you think is the number one priority to get at at that issue, which is an issue rampant across Government? But here, we are talking about $39 billion just in 1 fiscal year, and that is a substantial amount of money that can go to other things.

Mr. POWNER. There is that initiative. It is called the Portfolio Stat that came out of OMB, and I believe DOD is probably one of the model agencies. They identified 26 initiatives in all these categories that they claim can save between $3.2 billion and $5.2 billion by 2015. That is right around the corner, and that is a lot of money.

The number one initiative out of those 26, Ranking Member Ayotte, is data center consolidation. To date, they have closed over 250 centers. Now, some of these are small closets and things like that, but there are some large centers that are closed. I can give you examples of those. They claim they have saved $875 million to date. By the end of fiscal year 2015, $3.1 billion. By the end of 2017, it approaches about $7 billion. It is the model data center consolidation effort, if, in fact, they carry it through.

I made a comment in my statement about how they need to track savings. There are always these comments that come up that we do not have the appropriate accounting systems, ways to calculate savings, and that kind of stuff. Use a cuff system. These numbers are so large. That cannot be an excuse for not tracking those savings. There are over $5 billion that we can save by the end of 2015. That is a lot of money that you can reinvest in other systems that are important or something else that is a priority for DOD.

Senator AYOTTE. Secretary McFarland, where are we in terms of tracking these savings? Or maybe Ms. Takai. Sorry if I am asking the wrong person.

Ms. TAKAI. Yes, Senator. We are actually tracking the savings. We are tracking the data center closures, and we are tracking the savings on an ongoing basis.

I will just give you an example of an area where NDAA language that we received actually is helping us. We are reviewing all data center expenditures, and they have to be approved by my office. It is not just a question of saving by closing down a data center, but we are actually eliminating some of the redundant spending that you just talked about. I will give you an example.

In the first quarter of this year, Navy achieved a cost avoidance of $3.4 million by disapproving three requests. They would not have even known that those dollars were going to be spent if we did not have a very tight approval process right now. As you can see, if you just take three requests versus the number, quite frankly, that come across my desk on a daily basis, we are going to be achieving the savings.

But I think the other thing I want to mention here is that in some cases these are cost avoidance, number one. They are not necessarily savings off the top line. Effectively, we were stopping spending.

The second thing I would note is that some of these savings, as we are looking at them, are being included in the efficiencies numbers that you are already seeing as the Services are coming in to report on their budget. Perhaps they are not calling them out directly because they are not thinking of IT as being a big part of their expenditure. We are tracking it in a number of different ways.

I will close by saying it is a challenge to track the savings because the expenditure at DOD is very decentralized and it is actually done at the point that the equipment is being purchased or the data center is being equipped. So one of our challenges is to be able to collect those dollars. But having said that, the fact that it is a challenge does not mean that I do not agree that we should be tracking it and that we should be racking it up.

Senator AYOTTE. It seems to me a priority, given the setting we find ourselves in, because the tracking of it is the motivation so that we have more accountability. Then we know that those dollars can be used for other, more viable purposes.

So, Mr. Scheid, I wanted to ask you. When you testified, you talked about the situation of the audit readiness of DOD. I think you said that most will be audit ready by 2014. So is the Air Force still the problem child? Are they the worst offender? Can you break it down by Services?

Mr. SCHEID. I would not characterize it as a problem child or worst offender. I can go through the Services. In the testimony, I said while it is too soon to know for sure, we expect the budget statements to be auditable by September 2014.

The Marine Corps is the pacesetter. They are out in front. They have already achieved a clean audit of their financial statements. The Department of the Navy follows right behind. They are best positioned or at low risk and have a mature system in place. The Army has installed probably the most comprehensive and modern automation through its Enterprise Resource Planning (ERP), and they are trying to leverage the investments to support the audit.

The Air Force is, as you indicated, still struggling, and attempting to assert audit readiness with largely legacy systems. They are working through those legacy systems.

Where we see a great deal of risk or more risk is in what we call the fourth estate, the fourth estate being the defense agencies and activities that are not particularly in a Military Service or attached to a Military Service. There we have, I think, 44 different entities, and half of them have already had a clean audit at one point or another. That would be like the Defense Finance and Accounting Services (DFAS), for example. But the others are all struggling with legacy systems and trying to just achieve the readiness.

We work with the Comptroller very closely on this. I co-chair the Financial Improvements Audit Readiness (FIAR) Council. As I indicated, I am new to this area, but we are working with them to ensure that in particular, and this is my predecessor's work, the systems that support audit readiness are on track. We have had these authorities to monitor, track, and work on those systems for a few years and have done work with the Services to improve that.

On the audit readiness, may I add one comment to the previous discussion? You indicated $39 billion of investments across DOD, which is a huge responsibility. About $7 billion of that are business systems that we have identified. They break down into about 1,200 individual systems.

My predecessor and the office I am in now have instituted what we call the IBF to help bring some discipline to this business space. We align it or arrange it through functional strategies, which each have functional owners, functions as in human resources, acquisition, and so forth. Then we organize these systems into portfolios. The portfolios are reviewed annually in an investment review board.

This process has helped the team reduce redundancies, identify where there are redundancies, reduce them, and identify where we should not be obligating funds. I indicated in my testimony, I think, we had cost avoidance of about $1 billion through these two cycles, and we have stopped funding 60 legacy systems. Of that $39 billion, the business systems has had increased scrutiny through this IBF that we have established and is getting some results. It is early days still and there is a lot of work ahead, but we are working in that direction.

I hope, Senator, that answers your question also on the FIAR.

Senator AYOTTE. Yes, thank you. My time is up and I know we will have a chance for follow-up questions. Thank you.

Senator SHAHEEN. Thank you.

I would like to point out, relative to the consolidation of data center discussions, that in addition to the cost savings, part of that cost savings is significant energy savings, and so that is another benefit for doing the consolidation.

Senator Donnelly?

Senator DONNELLY. Thank you, Madam Chairwoman.

Mr. Powner, we talked about 93 projects on Dashboard. Secretary McFarland, are there goals and metrics for each of those 93 projects month-by-month where we are, how we are doing, and are we on target? Could I pull up a booklet and see exactly where we are in that project?

Ms. MCFARLAND. I will share this with Teresa.

Of those 93, there is a certain number of them which we call MAIS, and for them, there are metrics. For the balance, I will turn it over to Teresa.

Ms. TAKAI. Yes, sir, there are metrics for all of the projects that are on Dashboard. We do not necessarily track month-by-month. We track major milestones for each one of those projects, and the frequency of the milestones is dependent upon the size of the project and when they will have met particular deliverables.

Senator DONNELLY. Mr. Powner, do you think we have sufficient metrics in place on these projects to make sure that we are on target and on time?

Mr. POWNER. I believe DOD has internal metrics. I do not think where we are at on those metrics is transparent necessarily on Dashboard because the data is not updated.

The other thing I would add, Senator Donnelly, is that there are some MAIS projects, nine of them that we are aware of, that are not on Dashboard. So, for instance, there is Navy Common Ground System. I do not see that on Dashboard. There is an Army Tactical Mission Command program. We did a scrub because we are doing the MAIS work for this committee right now, and it will be out at the end of the month. So I think there is a fundamental question. Have we captured all the investments and then do we actually have the right status of how they are performing? I think the answer to both those questions is no.

Senator DONNELLY. Let me ask this: in terms of best practices, I was just sitting here jotting down some names. I know DOD has concerns about security and stuff. Do folks from Amazon, Google, GE, Apple, or Microsoft come in and say, "here are our best practices"?

Ms. MCFARLAND. Yes, we do. In fact, much of what we have been doing over the last couple of years to understand best practices has been through the industry consortiums, to understand what goes on and how to perform inside of acquisition better.

Mr. SCHEID. The DSB has been helpful in the past. They worked on the 804 report. Also, the Defense Business Board is composed of CEOs, COOs, and others that have insights into these programs. They do projects, studies, and analyses, and we benefit from that.

Senator DONNELLY. This may sound like a little bit of an offbeat question, but that is okay. Is there a need for all of this to be focused or located at DOD? Would it be disadvantageous if it were spread throughout the country or that we had some computer operations, for instance, in California, New Hampshire, Indiana, Pennsylvania, or other places?

Ms. TAKAI. Actually, a very small, minute part of what we do is actually focused at DOD. Our data centers are spread throughout the country, which is actually part of the challenge of getting them consolidated, quite frankly, sir. Because they are at each base, post, camp, and station, and that is a bit of our challenge. The development processes, Ms. McFarland can speak to this, in fact, are not at DOD. They are most often near where the major focal point is as it relates to the business operation that is going to be benefiting from that system.

Senator DONNELLY. Okay.

As we look at the systems going forward, one of the concerning things is counterfeit electronic parts, electronic chips, et cetera, and I was wondering what is being done in that area.

Ms. MCFARLAND. If you are not aware, sir, we actually have a Federal Acquisition Regulation——

Senator DONNELLY. I am.

Ms. MCFARLAND. Okay. We are doing quite a bit of work in that area. I came originally from the Missile Defense Agency which really brought to bear a lot of attention on that issue. For contractor accountability, we are holding them accountable for providing spare parts or any part that is counterfeit.

Senator DONNELLY. Okay. So there is identification on all of the parts that are going into the process.

Ms. MCFARLAND. That is the requirement.

Senator DONNELLY. Thank you, Madam Chairwoman.

Senator SHAHEEN. Thank you, Senator Donnelly.

Assistant Secretary McFarland, I want to go back to section 804 that Senator Ayotte and I talked about, and you all have referenced. I am interested in the extent the efforts that are being undertaken now, with respect to trying to improve our acquisition programs, to build on what was done with section 804. Can you, or Ms. Takai, talk about the extent to which your belief, that the reforms requested under section 804 have actually been implemented and how the current process builds on that? What was done? What was not done, maybe?

Ms. MCFARLAND. Yes, ma'am. I would say about 75 to 80 percent of what the report to Congress discussed has been initiated and implemented. "Implemented" is not complete. As you are aware, the system has a slow progress, and many of the items within section 804 regard the early onset or the initiation of the program. So we have programs that did not benefit from those specific initiatives that are very important to make the products what we want them to be. We will be continuing to do cleanup in a lot of those areas.

The programs that are coming forward I mentioned in my written testimony are programs that have shown success. We have demonstrated that we can reduce by 45 months the timelines for requirements by using IT Box compared to an earlier increment. A lot of the programs are now coming forward for our review that have demonstrated that they are taking a very close and precise look at what size of an increment they can build and field.

One of the biggest hurdles that we had over the last few years was that people did not understand the full complexity of what they had to build, particularly in business systems where all of the interfaces and the exchange are very large. The enterprise exceeds the boundaries of just DOD. We interoperate with a lot of different agencies and activities. When we look through the lens of what section 804 put into place, I am seeing, and I am very cautiously optimistic, that those implementations will continue forward. They are strengthened in the new DOD 5000 directive, and we are seeing products and programs coming forward where we can actually review and institute them.

On the second note, the Services are also very interested in this. You have probably paid attention to the news. There is a lot of activity within the Services that recognize the challenges in IT and

they are putting their own personal focus on looking through what they have for those investments, where they are putting their people, and how they construct the programs. The Air Force just stood up a new board specifically to do that. We are putting emphasis on it. Can I say we are complete? No. We have a long way to go. The enterprise is huge.

Senator SHAHEEN. To make it more concrete for my understanding, can you describe a particular project that you think, as a result of the section 804 changes, has characteristics that you are translating now as you are looking at the 5000 process and adopting some of those characteristics or guidelines?

Ms. MCFARLAND. Yes, I can. The integrated pay and personnel system for the Army came forward originally with a very complex, big bang theory on how it was going to deliver capability. After we went through the process with them, they reduced that sizing of increments to be discrete elements that show a manageable and deliverable product within each of these releases. They are short form. They have very distinct parameters that they can measure and identify and have been able to control costs that way.

We have many different metrics that we are now putting in place related to this. One of the questions during program review I ask is: how many interfaces do you understand and what is it that your people will have to do to address the change? Much of what we do, particularly in defense business systems, is related to the people operating those pieces of gear. It is like using my kitchen sink for umpteen years and I am very familiar with it and you just put something in front of me that I do not understand, it still does everything according to the written requirement, but it is not familiar. I used to reach here and now I have to reach there. That is one of the biggest pieces for the success and failure of these systems.

Another one, just from memory here. We have also rolled in on top of the section 804, the Better Buying Power initiatives. Are you familiar with those?

Senator SHAHEEN. No.

Ms. MCFARLAND. One of the things that we have asked them to take a look inside of when they execute a program is once you have established what you think is the appropriate cost for delivering that, we build that into the independent cost estimate. We also ask the program managers and their teams to come in with what efforts they can do to take costs out of the program. As we look at their execution, they have to show discrete efforts that demonstrate some actual activity to look at reducing costs. It can be anything as simple as using a different contract type because it is more effective when I incentivize this contractor to deliver that methodology. We have a huge effort working with our people to change the culture to make it cost-effective.

Another aspect is simply affordability. We have a lot of challenges explaining to people what affordability is. Affordability is not making it cost avoidance or savings. Affordability is understanding how much you have to spend on something, staying within that, and understanding the total ownership cost of something when you deliver it. Even though you may wish to deliver a capability inside of IT within a certain period of time, if you cannot af-

ford it, look to find what you can afford that is meaningful that you can deliver.

Senator SHAHEEN. What kind of educational development efforts go along with the kind of program implementation that you are talking about?

Ms. MCFARLAND. Prior to this position, I was the Defense Acquisition University's president, and one of the things that I did, because I had just come off of the team for Mr. Kendall and Dr. Carter, was trying to change the curriculum in the university to focus on how to build in cost consciousness. Oddly enough, this is a trip to the past. When I entered government service in the 1980s, we had much of what is considered today the new look at acquisition that is ongoing. It was post-Cold War thinking; how do I get money out of the system? We were working on things that I have an excellent book on called "Design to Cost," for example. Myself and others were also focused on cost avoidance, and how you look at how to construct a cost-effective system. We are building that back into our training curriculum. It is not just for those students that come through because of the mandatory certification they have to take. We actually have mission assistance teams and rapid training teams that reach out to the major systems and commands to educate them.

In addition, Dr. Carter, when he was the Under Secretary of Defense for Acquisition, Technology, and Logistics, Mr. Kendall, myself, and Alan Esteves actually go out to centers of excellence and centers of mass when it comes to acquisition. For example, last week I was down at Naval Air Station Patuxent River talking on a hot topic forum for about 2 hours with about 350 acquisition professionals going through what they have to think about because it is truly critical thinking. The attitude of cost has to be thought of when you are doing a very complex system. In addition to all the demand signals we put on them for how to do acquisition, they have to also put that additional equation together.

Senator SHAHEEN. I am over my time, but since it is just Senator Ayotte and I, maybe she will not mind if I ask a follow-up question.

So given all that, the training that people are undergoing, and the focus, how is it that we can have a contract like the Air Force had that is $1 billion in and no deliverables?

Ms. MCFARLAND. This is an incredible human endeavor. That program was started around 2002 and it was done during a period of time when we were waking up to the huge investment in IT. At that time, it was the tail end of when we were thinking of acquisition through the large systems integrator, where we had decided that it was more useful to put essentially the business of doing acquisition in industry's hands. In other words, we had decided that industry could do it better.

Unfortunately, that did not work. There was also a great deal of perverse incentives in that program. If you had an opportunity to read the root cause assessment that was submitted to Senator McCain, it talks about this. If you were to take the Weapons Systems Acquisition Reform Act, it talks about six parameters and a seventh called "other," and effectively it is what could go wrong on a program, and every one of them was met. Very negative.

There was a lot of accountability across the entire spectrum of their program. It did not do business process reengineering. It gave the contractor the responsibility to develop the requirements and then build to them. In terms of how you manage constructively and contain constructively requirements, it was completely set wrong.

Have we learned from that? Oh, yes. There is nothing more humbling than to see something like that happen and have it go on as long as it did. Have we rolled it into our business process engineering lessons? Yes. Have we rolled it into the school? Yes. Have we a long way to go? Yes.

Senator SHAHEEN. Thank you.

Senator Ayotte.

Senator AYOTTE. Thank you.

In following up to that, we are talking about the ECSS system, and I wanted to get your impression, Mr. Powner, having just finished this draft GAO report, the impression of having heard about this one system. But we know that is not the only example. I want to just restate this is not an issue that is unique to DOD in terms of these systems, particularly with regard to IT systems. I wanted to get any thoughts you had on this.

Mr. POWNER. I think it is great that we are building into the curriculum, we are looking at lessons learned, and all those things. But this is where governance plays a factor. You have an investment board and you have executives who are in charge of these programs; Mr. Scheid mentioned the IBF. The IBF is darned good. It is a portfolio-based approach and if you followed it, less programs would fail.

But someone at some high level on these boards needs to ask questions. Is the Government defining the requirements and not the contractor? Are we going with an incremental approach? Are we validating those requirements? Is the business on board? Because the business was not on board for ECSS. These are basic, fundamental questions that do not really have a whole lot to do with IT. It is more management stuff, and that is what governance is all about. We see, not only at DOD but across the Federal Government, poor governance in an executive level and program offices start doing things at this detailed level without the appropriate executive oversight. This is an executive issue. That is why we fully endorse putting the CIO picture next to each investment on the Dashboard, and if the CIO is not the appropriate person, put the appropriate person who is the right executive of that department or agency.

Senator AYOTTE. As I understand it, in 2011, the Institute for Defense Analyses wrote a report titled: "Assessment of DOD ERP Business Systems." One of the primary findings spoke to this issue of leadership, that acquisition programs require that a single accountable leader has the span of control to define, implement, and execute the end-to-end business process the IT investment is intended to support.

I think I have asked this in the larger hearing as well. For a system like ECSS, was there one accountable leader? Was anyone held accountable for the failures? Because it seems to me that you have these major systems and how often are saying you are responsible and then holding people accountable? Can you speak to that, Sec-

retary McFarland, and how that culture obviously helps get better results for the taxpayers?

Ms. MCFARLAND. In terms of who and what was held accountable, obviously the contractor was one of the principal people held accountable. In terms of us, yes. We reconstructed that organization. When the program was terminated, the Air Force took it very seriously, and they are now trying to reorganize to determine how to execute a follow-on system because the ECSS's capability is still required.

In terms of how you are setting yourselves up for the future, it was an integral part of why we made the changes. In terms of how we are looking at changes since the 2010 implementation of section 804, a lot of those obviously problematic areas were incorporated into what we are doing in terms of business process reengineering in terms of governance.

Senator AYOTTE. I wanted to follow up, Mr. Scheid, as well on the audit issue. Certainly on this issue, when you listed the Services and where they were with regard to the audit situation, as well as the 44 entities that are outside the Services, you had the Air Force fourth in terms of the Services. So how are we going to get the Air Force up to speed to be audit ready.

Next, I think it would be helpful for this subcommittee to understand the 44. I know you know them. I do not know them. I would like to have a list of the 44 that are not in an update. You said half of them have actually been able to meet an audit in the past. Which ones do you feel are most at risk? Understanding that each Service Chief is going to have responsibility for the Services, certainly the Secretary as a whole and DOD is responsible for these other entities. I can understand why they would be even more vulnerable. I think a report to us on that would be helpful for us to understand, as we look at this audit issue.

Senator SHAHEEN. I agree. Perhaps you could provide that to the subcommittee.

Mr. SCHEID. Yes. I will provide the list. Now that I am thinking about it, some of those 44 may be captured in the Washington Headquarters Services (WHS). That is that one entity that works for many offices.

Senator AYOTTE. In DOD?

Mr. SCHEID. In DOD, yes. They are outside the OSD.

Let me provide that list. They are agencies and activities, and some of these activities are small and for audit purposes they are rolled up into other entities like WHS.

But an agency like DFAS is not in a Service. It is outside and it is in this fourth estate that we call it. They have been audited. I believe the number of years is 14 years. They are largely personnel. It is salaries. In terms of meeting the audit requirements, it is relatively simple as compared to a large organization with different activities.

[The information referred to follows:]

We maintain a list of 46 Department of Defense entities that fall outside the Military Services. We informally refer to this grouping as the "fourth estate."

Office of the Secretary of Defense:

1. Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD(AT&L))

2. Office of the Under Secretary of Defense (Comptroller) (OUSD(C))
3. Office of the Under Secretary of Defense (Intelligence) (OUSD(I))
4. Office of the Under Secretary of Defense (Personnel and Readiness) (OUSD(P&R))
5. Office of the Under Secretary of Defense (Policy) (OUSD(P))
6. Office of the Deputy Chief Management Officer (DCMO)
7. Office of the General Counsel of the Department of Defense (OGC)
8. Office of the Inspector General of the Department of Defense (OIG)
9. Director of Cost Assessment and Program Evaluation (D,CAPE)
10. Director of Operational Test and Evaluation (DOT&E)
11. Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))
12. Assistant Secretary of Defense for Legislative Affairs (ASD (LA))
13. Assistant to the Secretary of Defense for Public Affairs (ASD (PA))
14. Department of Defense Chief Information Officer (DoD CIO)
15. Director of Administration and Management (DA&M)
16. Office of the Director of Net Assessment (ONA)

Defense Agencies:

17. Defense Advanced Research Projects Agency (DARPA)
18. Defense Commissary Agency (DeCA)
19. Defense Contract Audit Agency (DCAA)
20. Defense Contract Management Agency (DCMA)
21. Defense Finance and Accounting Service (DFAS)
22. Defense Health Agency (DHA)
23. Defense Information Systems Agency (DISA)
24. Defense Intelligence Agency (DIA)
25. Defense Legal Services Agency (DLSA)
26. Defense Logistics Agency (DLA)
27. Defense Security Cooperation Agency (DSCA)
28. Defense Security Service (DSS)
29. Defense Threat Reduction Agency (DTRA)
30. Missile Defense Agency (MDA)
31. National Geospatial-Intelligence Agency (NGA)
32. National Reconnaissance Office (NRO)
33. National Security Agency/Central Security Service (NSA/CSS)
34. Pentagon Force Protection Agency (PFPA)

Department of Defense Field Agencies:

35. Defense Acquisition University (DAU)
36. Defense Human Resource Activity (DHRA)
37. Defense Media Activity (DMA)
38. Defense Prisoner of War/Missing Personnel Office (DPMO)
39. Defense Technical Information Center (DTIC)
40. Defense Technology Security Administration (DTSA)
41. Department of Defense Consolidated Adjudications Facility (DoD CAF)
42. Department of Defense Education Activity (DoDEA)
43. Office of Economic Adjustment (OEA)
44. Task Force for Business and Stability Operations (TFBSO)
45. Test Resource Management Center (TRMC)
46. Washington Headquarters Service (WHS)

The Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, and National Reconnaissance Office received favorable audit opinions for fiscal year 2013. In addition, the Military Retirement Fund, Medicare-Eligible Retiree Health Care Fund, and the Defense Health Agency-Contract Resource Management also received favorable audit opinions. In fiscal year 2012, the Defense Information Systems Agency and the Office of the Inspector General received favorable financial audit opinions.

Mr. SCHEID. On the status of the Air Force, I would prefer to take that for the record, if I may.

Senator AYOTTE. Sure.

[The information referred to follows:]

The Air Force is working hard to become audit ready. As Comptroller Hale relayed in his November 2013 Financial Improvement and Audit Readiness (FIAR) Plan Status Report, we do expect most of the Department's budget statements to be asserted as audit ready or be under audit by September 30, 2014. Significant challenges to audit readiness remain across the Department, while the Air Force is

particularly impacted by the challenge of having to work largely in a legacy environment. The long-term plan to mitigate legacy system challenges is the full deployment of Defense Enterprise Accounting Management System (DEAMS). DEAMS will be fully deployed by 2017. Further exacerbating the Air Force challenges is the fact that its FIAR consulting contract was under protest for nearly 8 months, so the 2014 goal for Air Force is particularly challenging.

Although the Air Force is arguably the Service with the most risk, it is also sprinting to put itself in position. Air Force senior leaders have committed to doing everything possible to be audit ready by the end of fiscal year 2014. In order to minimize delays resulting from the FIAR support contract protest, the Air Force implemented a rigorous and systematic process for testing key financial controls throughout the year. Each month, it is testing various controls within its various business areas. In fiscal year 2013, the Air Force tested over 10,000 transactions, applying over 57,100 test attributes. It saw its success rates improve from 40 percent to 90 percent or better on many of the samples. These overall test results demonstrate the Air Force is developing controls to sustain audit readiness beyond 2014.

The Air Force has also refined its FIAR execution strategy to focus on tracing a financial transaction from origination through reporting for each assessable unit—a "walkthrough" of the financial transaction process. The walkthroughs entail visits to the originating bases through the major commands and the Defense Finance and Accounting Service. This allows the Air Force to leverage existing process documentation and control testing prepared by these command echelons, saving time and resources. The teams are able to identify and implement corrective actions and test mitigating or compensating controls early in the process.

Mr. SCHEID. One, because of my lack of experience just being in the seat for a few months, and two, to make sure you are not misled in any way by something.

Senator AYOTTE. I appreciate it.

I have a specific question about audits. As I understand it, the NDAA for Fiscal Year 2010 charges the CMO of DOD, in consultation with the Comptroller, with revising a FIAR plan which describes that specific actions must be taken to ensure that the financial statements of DOD are validated and ready for audit by no later than September 30, 2017.

As I understand it, there is an argument going on right now in DOD as to whether to include valuations of property as part of the audit which is required to be completed by 2018. Though establishing the value of a company's property certainly is very critical in the private sector, as I understand the argument within DOD right now, some are arguing that it may be less necessary to ascertain the value of property owned by DOD.

I am not taking a side. I just want to get your opinion of what you think. What is your view on this debate? How significant of an additional undertaking is it to establish the values of property? How many additional auditors does it take? Does that take us down every M–16, every rucksack, if this requirement were lifted? I am not taking a position one way or the other. I want us to get the best information we can to make decisions on behalf of the taxpayers. Is this something that would help you meet your audit deadlines? I just want to hear the opinions of the group on this, particularly Mr. Scheid, and obviously if Mr. Powner has any opinion, I would be happy to have him weigh in as well. Is this a debate that you are aware of?

Mr. SCHEID. No, I am not aware of it. I would be glad to get more information on it.

Senator AYOTTE. Okay.

[The information referred to follows:]

I am not aware of a debate or argument going on within the Department of Defense (DOD) related to valuations of defense property.

In order to achieve a clean opinion, DOD must adhere to federal financial accounting standards, which require that capital property be fairly valued. These current standards mandate that federal agencies report property and equipment assets at full acquisition cost. DOD recently published equipment valuation guidance, which provides options for valuing our assets and costs associated with this effort. The Comptroller will meet with each of DOD's components to determine which options work best within their standard business processes.

DOD is committed to meeting its audit goals to include existence and completeness of all equipment assets. This will provide assurance of physical stewardship, control of assets, and information that is most meaningful to the management and our stakeholders. DOD is studying the cost of making and auditing property and equipment values; however, those costs are not yet known. We remain committed to becoming audit ready in a way that is cost effective.

Mr. SCHEID. I am aware that in the audit readiness timeline that I believe has been briefed to the subcommittee and others by Secretary Hale, that the mission critical asset's existence and the completeness audit readiness, the critical asset existence is part of this taking account of the physical properties, facilities, trucks, everything from aircraft to fire trucks and so forth.

Senator AYOTTE. Sorry to interrupt. I have had some people ask me if that means we have to get down to every screw. At least as I understand this debate, there is some consternation there.

Mr. SCHEID. I am not auditor. I am not an accountant. But there must be a limitation to that, particularly in such a large organization trying to get to an audit.

Senator AYOTTE. We are not trying to ask you to do something that would be unreasonable. What we want is things that would be helpful to the taxpayers.

Mr. SCHEID. Yes. This is part of the plan. I believe it is reasonable to expect us to deliver that account.

If there is a debate in DOD, I do not want to speculate on it or contribute one way or the other to it. I would rather get you the facts on it.

Senator AYOTTE. Okay. I appreciate the follow-up on that. Thank you.

Mr. POWNER. I am not aware of the issue, but I have a colleague on our financial management team. If I could take that for the record, we can get back to you on that.

Senator AYOTTE. That would be great. Thank you.

[The information referred to follows:]

See answers to Questions for the Record 11–16.

Senator SHAHEEN. Can I just ask Secretary McFarland or Ms. Takai, are either of you aware of this issue?

Ms. MCFARLAND. No, but it is fascinating.

Senator SHAHEEN. Yes, it is.

Ms. TAKAI. No, I am not aware either.

Senator SHAHEEN. I want to go back to the issue that you raised, Ms. Takai, about the JIE because I am not sure that I quite understand either what this idea is, or what it is designed to do and how it should work. I wonder if you could talk a little bit more about that. Is this viewed as an agency-wide or a DOD-wide effort? Who is in charge of it, and how is it supposed to work?

Ms. TAKAI. Perhaps I can start out with just a description, perhaps in a little bit more detail in terms of what it is.

The effort is really around being able to take the money that we spend today, because I think as Mr. Scheid said, out of our $40 billion a year, a fairly large proportion of that is spent on just maintaining and upgrading our networks, our data centers, our servers that sit within those centers, as well as buying a fair amount of services from other companies. Then, of course, we have software purchases, which is software that basically runs the computers all the way up to the way we do email. The line, which gets a little bit fuzzy, is it falls short of, for instance, an ECSS or an equivalent system or financial system. What is it that is underneath it that, first, makes it run and, second, means that you can connect it? That connection means not only from a computer terminal but also how do you connect it from a mobile device and some of the newer technologies coming in? So, I think it is important to set that context.

The next thing is that our infrastructure is, obviously, from a multiplicative standpoint, bigger than any industry. I was talking to some folks from AT&T the other night, and we concluded that AT&T and their worldwide network was probably maybe close to the equivalent of the Navy if you think about the size. So when we talked about the number of data centers, I think we also have to recognize that we have a U.S. number but we also have a deployed force and that exacerbates the issue.

The challenge that we have with that is multiple. Today, we have what I would call fairly loose standards. In other words, my office puts out standards, but the way that the technologies are implemented can vary significantly not only from Service to Service, but because of our size, we are very decentralized. Each location will actually set up their own computers. They will set up their own firewalls and so on. All of that, I think, back to Senator Ayotte's point, is a part of what can certainly lead to redundancy. It can lead to competing technologies, and certainly that has multiple ramifications.

Let me just say what the ramifications are. First of all, it means that when we try to defend our networks, that means that we have to see when there is an adversary on our network, and we have to be able to trace back and see where that adversary has gone. The way we are set up right now, you have to understand all of our networks to be able to actually do that, which of course is an impossible task. I think you have heard General Alexander say, given the way we are operating today, that is just impossible.

The second thing is, we have different ways of operating our networks. We have some big operation centers, some small operation centers, and the same is true of help desks and so on, which again is redundancy and it also makes it very difficult to run.

So the effort around JIE, as you mentioned, is not what we would call a program of record because, again, we are not suggesting that we need new money for this. We are suggesting that we need to take the money that we spend today and use that money to drive towards this standardization, this communization, this ability to eliminate the redundancy and to operate in a single way.

The overall responsibility for that program is mine. The Secretary has designated that I am responsible for working with not

only the Services but all of the component organizations in order for them to implement the JIE. As you could well imagine, that is a daunting and challenging task. We are part-way through that. The data center consolidation is one of our efforts in doing that. Our defense enterprise email that you may have heard is another area that we are focused on. But we have a suite of things in terms of the way we are doing some of our fairly detailed network configurations and so on that we are in the process of specifying and rolling out.

The Services have just delivered to me, in fact, at the end of February their implementation plan because the challenge is just like all of the issues we have been talking about here. I can lay out ground rules, but clearly each of the Services has to have a plan for how they are going to implement because each of them are in different places in terms of how much they have standardized. Those plans have come back in and we are currently in the process of bringing those together.

We also are expecting from all of our components plans to be completed at the end of March. We are going to actually look at how we are going to operate that.

Let me give you a couple of concrete examples. We started with a concept of operations in Europe because Europe, between our U.S. European Command and U.S. Africa Command, as well as Navy support, had actually started down a path of doing consolidation. Through that, we have been able to bring up one single enterprise operation center, and they are in the process of shutting down. I do not have the exact number, some number of centers. This, of course, helps CYBERCOM because they will be able to work through that operation center, as well as we have a plan for which of the data centers in Europe will be closing as part of our data centers and then how it will be consolidating.

Our second geographic area is U.S. Pacific Command (PACOM). Admiral Locklear has asked to be the second area. We have a set of workshops that are scheduled for the end of March/early April that will take advantage of the work that they have already started but make sure that the work in PACOM is aligned with the work that is happening in Europe.

The complexity is that in PACOM we have every Service, and each Service has their own way of doing networks and data centers, and so they are going to come together in PACOM to actually come together on how they will do a joint implementation.

The real complexity that we have here is that the funding sources come in from the Services. They each have a specific way of doing things. But the real benefit, in many ways, of JIE, which is why it is called "joint," is actually in the combatant commanders who have to deal with the technologies coming in from each of the Services, and through the standardization, the concept is to ensure that we are operating in a much more uniform way than we are today.

It is a huge effort. I do not want to minimize it at all. Many major corporations have done this. I can certainly cite many in Silicon Valley. Hewlett Packard has a major effort in this area. Oracle has internally. IBM, in fact several years ago, just went through the same kind of consolidation and bringing together. My back-

ground is State government, and State government is challenged as well, within their internal operations with every agency having their own.

Senator SHAHEEN. Yes, we have experienced that.

Ms. TAKAI. So if you think about what the challenges were at the State government level, which I know very well from my Michigan and California days, then you blow that up. My IT spend in California was about $5 million, and I had about 110 CIOs that I was trying to bring together. Multiply that by our numbers here. I think you can see the size. But I think to Senator Ayotte's point, you can also see the opportunity if we can continue to move this forward.

I really would come back to the comments that were made by GAO. This is not going to be a perfect process. It is not going to be a march that looks really exact and pretty, but it is, to some extent, to his point we are putting pressure on the organization to get better.

I will make one last point. If we cannot get to some level of operating in a much more standardized fashion, it makes it so much harder, if not impossible, for us to move to new technologies like the cloud technology. I have often said that if I replace all of my disparate data centers with disparate clouds, I am actually not any farther ahead. I am actually in some ways increasing my complexity because now data centers that I own and run today, I will either be using a commercial cloud capability or a different cloud capability. It is really important that we get the standardization to happen so that then, to the point, I think, that Mr. Scheid made, we can move our business systems into cloud technologies. We can get the efficiencies, but we can also ensure that we have security in those solutions so that we do not have to be concerned about, not only the fact that we are getting more efficient, but we do not want to do that at the sacrifice of security.

Senator SHAHEEN. That is helpful. Let me see if I can restate what I understand you to have said about the JIE now.

It is an effort to standardize IT systems throughout DOD so that they are more efficient and better coordinated. Is that essentially what it is?

Ms. TAKAI. That is correct.

Senator SHAHEEN. It is under your portfolio.

Ms. TAKAI. That is correct.

Senator SHAHEEN. You talked about the consolidation. Is there a list of initiatives as part of that that you hope to accomplish and a timetable to do that?

Ms. TAKAI. Yes, ma'am.

Senator SHAHEEN. Different people are in charge of that. You said the budget for all of this will come through the various Services.

Ms. TAKAI. That is correct.

Senator SHAHEEN. So I assume that they have bought into this effort either directly or indirectly.

Ms. TAKAI. We are working on that now, ma'am.

Senator SHAHEEN. As you look in the short-term, say, over the next 2 years, 5 years, and 10 years, what are you hoping to accom-

plish within the next 2 years and where do you hope to be 5 years from now?

Ms. TAKAI. In the next 2 years, we are intending to implement two or three areas in the network, and certainly we can provide more detail. I do not want to get too technical in this discussion, but it is really to standardize the networks and certain areas of the networks. That is one of the things in the 2-year period.

We will have a plan to finish on defense enterprise email.

Senator SHAHEEN. Thank you very much.

Senator Ayotte.

Senator AYOTTE. Thank you for working so hard on these issues. Thank you.

Ms. TAKAI. Thank you.

So those are a couple things in the 2-year period.

In the 5-year period, I think as we mentioned, we are projected to close over 800 additional data centers by 2021. Actually, the rest of the figures that you have asked for are what I am expecting to get out of these implementation plans because I have asked each Service to come in. I have to take each Service's plan and then lay it out by geographic area so that I do not have conflicts between that. I think once I have all the implementation plans, I will have a better ability to tell you when, but I certainly can share with your staff today what our target numbers are for the categories that we are looking at. We have that and we are very happy to share that with you.

Senator SHAHEEN. How is this effort integrated with the IT Dashboard and the work that OMB and GAO are tracking?

Mr. POWNER. Clearly this effort is integrated with the data center consolidation effort. I think that is one of the big parts of JIE. Again, just to reiterate, I think DOD has gotten off to a great start looking at data center consolidation, but again, it is just really important that we track those savings because they have already had significant savings to date. In some of the centers that I looked at that have been closed, there is some good stuff going on where you have centers that had 450 servers and you shut down 440 of them, all but 10. There are several stories like that. That is where we had unused capacity.

When we do ask DOD, what is your average server utilization, they can answer the question. Many agencies cannot. Frankly, their average server utilization is higher than most, and they got the most savings. I know they are big, but there is a good news story here on data center consolidation. That is the one area on legacy spending I think needs the most focus and continued focus.

Senator SHAHEEN. Good. That is encouraging, and it is a message that we should probably do a better job of trying to get out.

I think one of the things that has been hard, certainly for me and I think it is true of some other Members of the Senate and Congress to understand, is why we have duplicate systems being built within the Air Force and the Army. I appreciate that some of that is history and tradition, but I think given the resource challenges that we are facing in the future, the effort to be more efficient with those systems is very important. I very much appreciate what you all are doing to accomplish that and hope that we can continue to

help track those efforts so that we are better informed, and also so that we can look at how we can be helpful in that effort.

I think given that we are hoping to be out by 4:30 p.m., the one area that I would like to ask about has to do with the House of Representatives passing the Federal Information Technology Acquisition Reform Act (FITARA) because it is legislation that is designed to address some of the IT challenges that we are facing in the Federal Government. I wonder if you all could speak to what is in the FITARA legislation. It is my understanding that DOD already performs many of the requirements that are in that legislation. We already have a single Department CIO within DOD and whether this is legislation that would be helpful in the efforts to address the IT challenges that you are facing at DOD or whether you see it as redundant to what is already going on.

Ms. TAKAI. Yes, ma'am, if I could speak to that. First of all, we certainly applaud the legislation from the standpoint of intent. I think again to the comments that Mr. Powner made, it is important to have transparency. It is important to have visibility even for us as CIOs in order to be able to better manage the overall expenditures. Again, we want to make sure that the intent of the bill, we think, is very good.

Unfortunately, I think a couple of things. It looks to try to manage that by virtue of additional oversight. I think what you heard from my colleagues and I today is that we very strongly feel that it is in the processes that are implemented and it is in the measurements of how we are actually managing the process as opposed to an additional oversight. Many of the areas of oversight that were suggested in the bill are actually things that we report to OMB on today, and so additional reporting, I think, is a concern.

Many of the items that were in that bill are actually the things that the Secretary has tasked us to do already in his direction that Mr. Scheid spoke of in his reorganization effort. Obviously, our concern is that if, in fact, those reporting requirements do not fit, then we could be in a very difficult situation of an oversight from the OMB Office of CIO, oversight as a result of this bill, and then oversight as it relates to the way we are fitting into what the Secretary has asked us to do.

We are, again, more concerned about the implementation than the intent. We mentioned to your staff there are some areas where we believe that we could move forward with the intent, but do it in a little different way than the level of oversight that is suggested in the bill.

Senator SHAHEEN. Mr. Powner, do you share that view of how the House-passed legislation might affect DOD?

Mr. POWNER. Yes. I think you need to be careful on the reporting. I agree with that because we want to get into good, solid management and not just reports. There are aspects of the bill that are very solid-like data center consolidation. There are separate bills on data center consolidation. The Dashboard is in there in a small way such as encouraging the movement to cloud. I think the CIO authority thing is a big issue because CIOs do not have the appropriate authority across the Federal Government. There is a fundamental question if you grant them authority by giving them budget authority, or do you make the CIOs earn it through having certain

responsibilities associated with Dashboard and the like. That was the intent of Dashboard. If we get CIOs more engaged on all these major investments, they will be even more of a player at the table on the management team.

Again, I think there are aspects of that bill that are very solid, and I think the question on oversight is basically to cut right to the chase, what happened. A lot of things that are in that bill are exactly what Ms. Takai is saying you are already doing because OMB put in place policies to do that. There is a fundamental question of whether OMB is doing the appropriate oversight of those policies. We have some issues with that. So I think Congress is saying if OMB is not going to oversee it, then we are going to oversee it.

Bottom line on all this, let us make sure that we better manage IT acquisitions and have the right transparency and oversight, whether it is Dashboard or a similar mechanism, and let us manage the inefficiencies out of the legacy bucket because DOD spends $25 billion on legacy systems out of an $80 billion spend. That is huge. You can see here that there are a lot of inefficiencies that we can tackle through duplicate systems and data center consolidation. That intent of the bill is spot-on to try to tackle those issues. How do you go about doing it? There are many ways of doing it. But let us not lose sight of the big things there.

Senator SHAHEEN. I appreciate the comments that everybody has made. Is the reason to pass something like FITARA to address administrative changes that are going happen when we have a new Secretary of Defense, when we have a new CIO, when we have new leadership at DOD, GAO, and OMB? Is there a concern that the efforts that are underway now will change direction, will not go to completion? Is that something we should be concerned about as we are thinking about how to fully implement some of these efforts?

Ms. TAKAI. I will speak for DOD, and certainly the other agencies are in a different situation. But it is really not a concern at DOD because the functions that the Secretary has tasked me for are actually incorporated in my ongoing charter and the charter for my organization. So the next person who comes into the position will start with a set of responsibilities. I think that there is a continuity from there.

I will, though, make the comment, and I do want to follow up on an item that Mr. Powner spoke of and I think you spoke of as well, that the strategic relationship between the CIO and the head of the agency. Mr. Powner spoke about the importance of not only the CIO ownership but also of the ownership of senior executives in the organization. I think that is something that is important to reinforce in anything that we are looking at because I think we have seen with Clinger-Cohen that giving the CIO responsibility is great, but it needs to have that relationship.

Certainly, I can speak for myself that Secretary Hagel has fully endorsed the JIE. He has issued that as part of his tasking to us in terms of what we are supposed to do. That kind of involvement, back to your question about getting everyone signed up, quite frankly without that, it would be potentially close to impossible, but having his endorsement and his involvement in it, as well as our Deputy Assistant Secretary and our former Deputy Secretary, has been really pivotal for us. So I think that that is an important

part, and I think Mr. Powner spoke about that. But I would not want to lose that in this overall dialogue. It is really very critical.

Senator SHAHEEN. Thank you all very much. I very much appreciate your testimony and look forward to continuing to work with you as you make these changes. Thank you very much, Mr. Powner, for your insights.

We will keep the record of this hearing open until close of business on Friday for any other questions.

The hearing is adjourned.

[Whereupon, at 4:21 p.m., the subcommittee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTION SUBMITTED BY SENATOR TIM KAINE

INFORMATION TECHNOLOGY WORKFORCE EFFORTS

1. Senator KAINE. Secretary McFarland and Ms. Takai, my first bill, the Troop Talent Act of 2013, provides avenues for Active Duty servicemembers to receive certifications for the skills they acquire through their military training as they transition to civilian life. As you both highlighted in your testimony, the Department of Defense (DOD) faces significant challenges finding and retaining personnel with sufficient training and expertise in information technology (IT). What specific efforts are being taken by DOD to ensure a mission-ready IT workforce?

Ms. MCFARLAND. Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L) Frank Kendall and DOD Chief Information Officer (CIO), Teresa Takai, jointly signed the IT Acquisition Workforce Strategic Plan in April 2012. The partnership aligns the IT acquisition workforce improvements to the larger and ongoing strategic efforts to strengthen and improve the entire Defense acquisition workforce.

A key tenet of Under Secretary Kendall's Better Buying Power 2.0 framework is to improve the professionalism of the total acquisition workforce; with respect to the IT segment of the total acquisition workforce, we have been working hard to accomplish that goal. Certification levels for the IT workforce improved from 39 percent in fiscal year 2011 to 61 percent in fiscal year 2013. In addition, as part of rebuilding the total acquisition workforce, DOD has deliberately increased the size of the IT (acquisition) workforce by 49 percent since fiscal year 2008. Turnover rates have decreased by 2 percent from fiscal year 2011 to fiscal year 2013.

In addition to increasing the size of the workforce and improving certification rates, DOD has used the Defense Acquisition Workforce Development Fund (DAWDF) to fund the DOD Information Assurance Scholarships to create a cadre of cyber-informed IT acquisition professionals with degrees.

As part of Secretary Kendall and Ms. Takai's partnership to continuously improve the workforce, they sponsor a standing joint working group that performs ongoing workforce planning, gap assessments, training reviews, and initiatives to enhance the IT workforce managing acquisitions. In 2012, the working group completed a competency model update and workforce competency assessments. The results are being used to improve training and planning for the workforce. Currently, the working group is partnering with the DOD engineering workforce working group and the Defense Acquisition University to ensure cyber competencies are integrated into training.

Ms. TAKAI. Several strategies are in place to aid DOD in recruiting and retaining a skilled workforce. DOD currently uses a suite of civilian hiring authorities: the Federal Direct Hire Authority for the IT Management 2210 series, instituted by the Office of Personnel Management (OPM), which provides DOD and other Federal agencies some flexibility in recruiting information security professionals; Expedited Hiring Authority for the Defense Acquisition Workforce (including IT acquisition workforce professionals), provided by Congress to DOD through 2017; and DOD-specific, Cybersecurity Schedule A Hiring Authority, provided by OPM through December 2014, for select IT and non-IT civilian job series. These civilian authorities, along with military and civilian recruiting and retention bonuses, are used to recruit and retain IT personnel and are essential to maintaining the health of this community. In addition to these programs, DOD has used the Information Assurance Scholarship Program for over a decade to award scholarships in IT/cybersecurity disciplines to almost 600 individuals in exchange for service to DOD.

DOD is currently in the initial stages of migrating its IT/cybersecurity workforce into a broader cyberspace workforce framework, which is aligned to the specialty areas established by the National Initiative for Cybersecurity Education. As part of this migration, DOD will work to achieve an integrated learning continuum that provides a variety of academic environments, including traditional classroom training; virtual training; hands-on laboratories; realistic, operational exercises using Information Assurance (IA) and cyber ranges; and postgraduate education opportunities in a variety of IT-associated disciplines. DOD is leveraging established training and education venues both internally and externally to maximize professional development opportunities for its evolving cyberspace workforce, and determining where gaps exist. One new initiative is our collaboration with the Joint Staff and the National Defense University on a cyber-centric Joint Professional Military Education program to educate military and civilian leaders on key cyberspace tenets.

QUESTIONS SUBMITTED BY SENATOR JOE MANCHIN III

MILITARY HEALTH RECORDS

2. Senator MANCHIN. Secretary McFarland, last year the committee expressed concerns with the progress made on military electronic health records. It is my understanding that DOD has created a new acquisition process to prepare for the next generation of health record systems for the military. Please outline DOD's new acquisition framework currently underway, along with your expected timeline, and how this new process will ensure success and efficiency.

Ms. MCFARLAND. DOD has updated the DOD Instruction (DODI) 5000.02 acquisition policy that replaced the Business Capability Lifecycle (BCL) Model that was previously used for the modernization of the military Electronic Health Records (EHR) but ensures rapid, tailored processes to deliver capabilities in keeping with the BCL concept. However, the DOD Healthcare Management Systems Modernization (DHMSM) Program's acquisition strategy remains unchanged. The program's acquisition strategy was approved on March 17, 2014. The strategy supports a full and open competitive approach for acquiring a replacement for the Military Health System legacy systems to include the DOD's interoperability objectives. The DHMSM acquisition strategy is consistent with the DODI 5000.02 and capitalizes on the robust and highly competitive health IT commercial marketplace.

3. Senator MANCHIN. Secretary McFarland, I understand that you have held 2 industry days to gauge interest and assess capabilities. Do you have concerns with industry's capability to deliver the necessary capabilities required with this system?

Ms. MCFARLAND. Since October 2013, the DHMSM Program Office has conducted 3 well-attended and highly anticipated Industry Days (October 31, 2013; December 4, 2013; February 19, 2014). The last 2 Industry Days were hosted at the Ronald Reagan Building and International Trade Center in Washington, DC, with each attended by over 500 interested health care professionals representing over 200 companies and Government organizations.

The intent of these Industry Days is to interact frequently with interested healthcare companies to gauge and enhance their understanding of the DHMSM requirement; which includes the replacement of DOD's EHR system. These Industry Days are strategically aligned with the release of an iterative set of draft Request for Proposals (RFP) which provide interested contractors and healthcare providers early and frequent exposure to the Government's evolving DHMSM requirements. These early introductions to our ongoing requirements development efforts, in advance of a final RFP, will serve to greatly enhance prospective offerors and/or interested parties understanding of the Government's future requirements while reducing ambiguity. This draft RFP process also affords industry an opportunity to offer comments, suggestions, and/or pose questions regarding any element of the RFP. Additionally, in conjunction and coordination with the draft RFP release process, the Government has issued a number of targeted Requests for Information to industry to support the technical and functional viability determinations regarding industry capablilities in delivering a commercial EHR platform in fulfillment of DOD objectives. Finally, extensive market research and product assessments/demonstrations have been performed by the DHMSM team to ensure alignment of DOD requirements with market capabilities. The totality of the aforementioned assessment lends for the programmatic certainty that the commercial market is more than capable of delivering the requisite and desired capabilities.

At the end of March, the DHMSM Program Office will release its second draft RFP and is committed to the continued release of drafts, and the holding of Industry

Days until the Government is satisfied that industry has the requisite grasp of the DHMSM requirement; and is capable of accurately bidding to said requirement—the foundation of a successful competitive acquisition.

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

PROGRAMS THAT USE AN INCREMENTAL APPROACH

4. Senator AYOTTE. Mr. Powner, in your written testimony, you state that many "poor-performing projects have often used a 'big-bang' approach—that is, projects that are broadly scoped and aim to deliver capability several years after initiation." By contrast, you noted when Federal agencies used "smaller increments, phases, or releases of larger projects" they were far more successful. What DOD programs are using this incremental approach?

Mr. POWNER. Congress and the Office of Management and Budget (OMB) have called for agencies to deliver investments in smaller parts or increments. In 2010, OMB called for IT investments to deliver capabilities every 12 months, and since 2012, has required investments to deliver capabilities every 6 months. The preliminary results of our ongoing review of selected agencies' implementation of incremental development indicate that only 1 of 37 selected DOD investments plans to deliver functionality every 6 months and 10 others plan to deliver functionality every 12 months. In May 2014, we plan to issue a report requested by the Chair and Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs that will contain greater detail. Once our report is released, we can provide further detail and brief your staff.

5. Senator AYOTTE. Mr. Powner, what programs are not using this incremental approach?

Mr. POWNER. As previously noted, the preliminary results of our ongoing work on selected DOD investments show that several investments have not implemented OMB's guidance on incremental development. These investments likely did not plan to deliver functionality in 6–12 months because DOD's budget guidance encouraged 12–18 month deliveries.[1] While DOD's recently issued acquisition framework calls for investments to use incremental development, it does not specify how frequently functionality should be delivered.[2] According to officials at DOD's Office of the CIO, longer increments better align with DOD's acquisition framework. While we did not examine DOD's entire portfolio of IT investments, such guidance increases the likelihood that many of DOD's other investments are not following an incremental approach. We would be pleased to provide further detail and brief your staff once our report is issued in May 2014.

6. Senator AYOTTE. Mr. Powner, how does DOD determine which approach to use for which program?

Mr. POWNER. DOD's acquisition framework includes incremental approaches to software development, but does not mandate its use or specify timelines for delivery of functionality. Instead, it offers a series of basic models which are to be tailored to the unique character of the product being acquired. All of the models contain requirements and product definition analysis, risk reduction, development, testing, production, deployment, and sustainment phases punctuated by major investment decisions at programmatic and contractual decision points.

PROPER TRAINING OF ACQUISITION PROFESSIONALS

7. Senator AYOTTE. Secretary McFarland, in November 2012, DOD launched its Better Buying Power 2.0 initiative. One of the most important changes from Better Buying Power 1.0 was greater emphasis on improving and professionalizing the acquisition workforce. Ensuring that DOD has a "knowledge[able] and experienced IT workforce" was also one the "guiding principles" of the 2010 DOD report to Congress titled, "A New Approach for Delivering Information Technology Capabilities in the Department of Defense." However, the Omnibus Appropriations legislation only allocated approximately $51 million for DOD's Acquisition Workforce Development Fund, whereas section 1705 of title 10 authorizes the fund at $800 million for fiscal

[1] See, for example, Office of the Secretary of DOD, Guidance for fiscal year 2013 IT Budget Submissions, Aug. 9, 2011.

[2] Defense Instruction Interim 5000.02, Operation of the Defense Acquisition System, Nov. 26, 2013.

year 2014. Isn't investing in our acquisition workforce likely to pay for itself many times over in lower acquisition costs?

Ms. MCFARLAND. Yes. DOD supports Congress' continued and sustained investments in the defense acquisition workforce through the DAWDF. Even in the current austere fiscal environment, maintaining a cadre of highly qualified acquisition workforce is essential to executing critical missions in support of our Nation's defense. Reducing investments in the DAWDF and allowing our workforce and their skillsets to atrophy compromises our ability to effectively execute essential missions and may lead to long-term acquisition costs. For these reasons, continued investments in the defense acquisition workforce is the right strategy to improving acquisition outcomes, increasing buying power, and ensuring technological superiority for the warfighter.

8. Senator AYOTTE. Secretary McFarland, given some of the major acquisition failures in recent years, is $51 million a sufficient level of funding to ensure our acquisition workforce is sufficiently trained, especially in such technical areas as IT acquisition?

Ms. MCFARLAND. No, this level is not sufficient. The DAWDF, created by this committee, has been a major enabler of acquisition workforce improvements, including IT. We must sustain these recent workforce improvements and especially during austere times, we must continue training and efforts to strengthen the workforce we have. The President's fiscal year 2015 budget request of $212.9 million, in combination with other planned funding, is required to sustain and continue improvements. We appreciate the committee's longstanding record of support for a highly qualified acquisition workforce.

INTELLECTUAL PROPERTY

9. Senator AYOTTE. Secretary McFarland and Ms. Takai, one of DOD's most costly oversights has been the failure to secure data rights of the systems being acquired. The result is that DOD must pay significant sums to gain those rights in order to perform maintenance of upgrades to the system. I understand that the new interim DODI 5000.2, "Operation of the Defense Acquisition System," includes an Intellectual Property (IP) strategy and a preference for open systems and architectures. Please explain the importance of the IP strategy and a preference for open systems and architectures.

Ms. MCFARLAND. IP issues present significant challenges for DOD programs in a variety of ways. For example, when acquiring commercial or proprietary technologies, the standard DFARS license rights do not permit DOD to use detailed technical data or computer software source code for competitive sustainment activities. In addition, even when DOD funds technology development that results in license rights sufficient for competitive sustainment, DOD has often been unable to realize an appropriate return on that investment by securing the necessary data deliverables at competitive prices. These adverse effects are exacerbated further in major system acquisitions involving a complex mix of DOD-funded and commercial/proprietary technologies that cannot readily be segregated from one another—resulting in the entire data package being effectively restricted as if it were all proprietary/commercial.

Open Systems Architecture (OSA) describes a technical approach to system design that not only facilitates more effective operational configurations for systems, but also directly supports more effective management of the associated IP issues. More specifically, OSA focuses on modular system design, wherein discrete, functional components are linked to one another through well-defined interfaces, preferably using open standards to allow vendors and suppliers to offer competing solutions for the functional modules in a "plug-and-play" paradigm. This approach to technical design naturally results in the technical data and computer software code for the modules being more readily segregable from one another, avoiding or mitigating cases in which a commercial/proprietary module will restrict the use of a DOD-funded module.

The IP strategy required by DODI 5000.02 will serve as a foundational mechanism to help identify and manage IP issues throughout the entire program life cycle. A key element in this approach is to take advantage of the inherent benefits of modular design approaches, such as OSA, to better maintain appropriate distinctions between DOD-funded technologies and proprietary/commercial technologies. This allows programs to implement an "open business model" approach, to proactively manage technology investments both from a legal standpoint (e.g., data rights), as well as a technical/operational standpoint (e.g., data deliverables, modular compo-

nents linked through defined interfaces), ensuring the use of appropriate contractual mechanisms that will better achieve the programs' business objectives.

In addition, the IP strategy will address one of the most challenging elements of managing IP issues—the timing. IP rights are allocated early in the process, when the technology is first developed or first delivered (e.g., at development or initial production); however, DOD might not have an operational need to exercise those IP rights (which requires the appropriate data deliverables) until much later in the program life cycle (e.g., reprocurement, technical upgrades, depot level maintenance). Historically, programs have not been equipped to plan effectively for such downstream needs, electing instead to delay the acquisition of data deliverables, or additional data rights to allow competition, until those later life cycle phases when the specific needs are more well-defined. This approach typically results in DOD seeking to acquire those data deliverables and/or license rights in noncompetitive environments.

The IP strategy seeks to eliminate, or at least mitigate, these barriers to competition by requiring programs to initiate the IP strategy at the earliest stages in the program, requiring coordination and consistency with life cycle sustainment planning, and ensuring that the IP strategy is continuously updated throughout the entire program life cycle. With this overarching IP strategy in place, our programs will be better able to implement tactical measures (e.g., contract requirements, including priced options) to manage IP issues and remove barriers to downstream competition. DOD is working on a variety of mechanisms to provide training and guidance for the acquisition workforce on these considerations.

Ms. TAKAI. IP issues can be best managed by addressing them as early in the acquisition process as possible. Within our Enterprise Software Initiative (ESI), we provide broad terms and conditions as part of a master software agreement for software acquired through ESI procurement vehicles. These broad terms and conditions can then be tailored and expanded to include specific requirements related to the software acquisition. The IP strategy in DODI 5000.02 is extremely important in that it will enforce the rigor of addressing IP issues early in the lifecycle to ensure the appropriate terms and conditions are established.

OSA is an important aspect of addressing IP issues in that it relies upon non-proprietary interface standards that preclude the need to develop unique data exchanges. This requires that developers comply with the non-proprietary standards in the management of data associated with a capability thereby not locking DOD into a specific vendor solution for exchanging data.

PAST REFORM

10. Senator AYOTTE. Secretary McFarland, Ms. Takai, and Mr. Scheid, DOD has made numerous efforts in the past to overhaul and improve its IT architecture, including the establishment of the Business Transformation Agency (BTA), by then Deputy Secretary of Defense Gordon England in 2005. Please describe what stumbling blocks these past DOD efforts encountered and what steps you are taking to eliminate them for the future.

Ms. MCFARLAND. DOD's report, "A New Approach for Delivering Information Technology Capabilities in the Department of Defense", from November 2010, identified a number of strategic initiatives that have been initiated or implemented in the areas of requirements, acquisition, and portfolio management intended to improve the delivery of IT capabilities. A summary of the DOD accomplishments in several areas related to IT acquisition are:

- Requirements: For warfighting requirements, DOD developed and matured the Joint Capability Integration and Development System IT box. The IT Box represents a major change for Information Systems (IS) requirements development by enabling the delegation of authorities to specifically support the more rapid timelines necessary for IT capabilities through the Defense Acquisition System process. For business system requirements, the Chairman of the Joint Chiefs of Staff delegated requirements validation authority to the Defense Business Council (DBC) providing DOD with a forum to align business system requirements with business strategies as well as laws, regulations, and policies that are unique to acquiring Defense Business Systems (DBS).
- Acquisition: Many of the acquisition-centric initiatives were included in the interim DODI 5000.02 released by the Deputy Secretary on November 26, 2013. Significant 5000.02 changes include:
    - Acquisition Models: The interim DODI 5000.02 explains common models of acquisition in order to provide program structures and procedures tailored to the dominant characteristics of the product being acquired and to

unique program circumstances (e.g., risk and urgency). The models are: Hardware Intensive Program, Defense Unique Software Intensive Program, Incrementally Fielded Software Intensive Program, Hybrid Program A (Hardware Dominant), Hybrid Program B (Software Dominant), and an Accelerated Acquisition Program.

- Short Duration Projects: The templates in the interim DODI 5000.02 aligned to acquisition models and will enable and encourage shorter duration projects.
- Tailoring: The interim DODI 5000.02 includes guidance to adopt a modular, open-systems methodology with heavy emphasis on "design for change" in order to adapt to changing circumstances consistent with commercial agile methodologies.

- IT Infrastructure: DOD is moving towards a common IT infrastructure known as the Joint Information Environment (JIE). Through the development of common architectures and standards and smart implementation of JIE, DOD is striving to improve mission effectiveness, increase cybersecurity, and realize IT efficiencies. Increment 1 of JIE is focused on establishment of core data centers operating behind approved single security architecture under the direction of enterprise operations centers.
- Portfolio Management: DOD has taken initial steps to organize IT systems into portfolios of capabilities starting with DBS. Section 901 of the National Defense Authorization Act (NDAA) for Fiscal Year 2012, codified at title 10, U.S.C., section 2222, established DOD's single Investment Review Board (IRB), known as the DBC to manage DOD business operations including DBS spending. The DBC is managing a portfolio of approximately 1,180 DBS with an annual cost of $6.7 billion. The DBC continues to align planned DBS spending with business strategies and requirements retiring 60 DBS over the past 2 years and identifying an additional 150 legacy DBS that are planned to retire over the next 3 years. For fiscal year 2014, the DBC decided not to certify for obligation requests totaling $617 million. Additionally, in response to section 933 of the NDAA for Fiscal Year 2011, DOD established the Cyber Investment Management Board to integrate processes, align strategies, assess resource requirements, and rapidly provide acquisition governance and portfolio management for cyber capabilities.

Ms. TAKAI. Our existing IT environment consists of "stovepipes of excellence" where we have systems and infrastructure that have been designed to satisfy specific functions, but not necessarily designed and built to integrate or interoperate with other systems that do different functions. This has resulted in network and architectural complexity that is inefficient and hinders our ability to defend against cyber attacks.

My office is leading a multi-year effort to restructure much of DOD's underlying network, computing, and cybersecurity so as to make us more agile in deploying new decision support capabilities, improve cybersecurity of our core DOD missions, and make us more efficient and better stewards of taxpayers' resources. This effort, the JIE, will improve the agility and responsiveness of our IT systems in support of our warfighters, and improve our ability to defend against cyber attacks. We are implementing JIE through and with the Services using DOD's existing core—requirements, budgeting, and acquisition process.

This effort is based on DOD's leadership understanding that our IT infrastructure and systems are critical enablers for DOD operations. The support of both the Secretary of Defense and the Chairman of the Joint Chiefs of Staff has been, and will continue to be, critical to the success of this effort.

Mr. SCHEID. DOD continues to improve its business operations through efforts to better modernize, integrate, and govern its business IT systems. Over time, it became clear that the stumbling blocks to success in these improvements were related to the need for more comprehensive systems oversight and establishment of Department-wide governance. Recognizing these problems, in 2005 DOD created the BTA to provide oversight and establish governance mechanisms, including the Defense Business Systems Management Committee. Following enactment of the NDAA for Fiscal Year 2008, DOD created the position of the Deputy Chief Management Officer (DCMO), which further increased the oversight and level of visibility on DOD's business systems and processes. Changes to the law governing oversight of DBS through enactment of the NDAA for Fiscal Year 2012 further enhanced the governance of these systems.

Currently, DOD is considering its next steps forward. As Secretary Hagel announced in December 2013, he wants to better align responsibility and accountability for IT systems under the CIO; while strengthening the role of the DCMO

across DOD. These steps are intended to drive more efficient and effective business practices and make better use of scarce resources.

PROPER CONDUCT OF THE AUDIT

11. Senator AYOTTE. Mr. Scheid, section 1003 of the NDAA for Fiscal Year 2010 charges the Chief Management Officer of DOD, in consultation with the Comptroller, with devising a Financial Improvement and Audit Readiness plan which describes the specific actions which must be taken to ensure that the financial statements of DOD are validated as ready for audit by no later than September 30, 2017. Currently, there is an argument within DOD over whether to include valuations of property as part of the audit which is required to be completed in fiscal year 2018. Though establishing the value of a company's property is critical in the private sector, some argue it may be less necessary to ascertain the value of property owned by DOD. They argue that the benefits of knowing the value of a destroyer, for example, does not warrant the amount of resources required to establish this value. What are your views on this debate?

Mr. SCHEID. There is no internal DOD argument or debate about whether or not property, plant, and equipment (PP&E) valuation should be undertaken. DOD intends to be compliant with the spirit and intent of the law to be audit ready in order to achieve a clean opinion. To do that, current Federal financial accounting standards require DOD to report PP&E assets at full acquisition cost. Given this, DOD has gone ahead and published equipment valuation guidance, with various options for valuing assets and costs associated with the audit effort. Components will determine which options work best within their standard business processes.

A macro perspective would suggest that providing the value of DOD assets is prudent. The current value of DOD's PP&E represents more than 71 percent of the PP&E values reported for fiscal year 2012 for the entire Federal Government. To omit DOD's valuations ignores a large portion of Federal PP&E.

However, at a department level, it is questionable whether or not DOD would ever use valuations of its PP&E in future decisionmaking, to the extent that the practice would yield more worth or benefits than the cost of carrying out and maintaining these extremely complex enterprise-wide valuations themselves. DOD is not like the private sector, where a company's asset value plays an important role in characterizing its financial position. Further, it is not likely we would, for example, make operational judgments to send a task force into action based on the value of task force assets. DOD does believe, however, that there are certainly other elements of a PP&E audit, such as existence and completion, that could benefit DOD.

12. Senator AYOTTE. Mr. Scheid, would DOD use valuations of property?

Mr. SCHEID. At a department level, it is questionable whether or not DOD would ever use valuations of its PP&E in future decisionmaking, to the extent that the practice would yield more worth or benefits than the cost of carrying out and maintaining these extremely complex enterprise-wide valuations themselves. DOD is not like the private sector, where a company's asset value plays an important role in characterizing its financial position. Further, it is not likely we would, for example, make operational judgments to send a task force into action based on the value of task force assets. DOD does believe, however, that there are certainly other elements of a PP&E audit, such as existence and completion, that could benefit DOD.

13. Senator AYOTTE. Mr. Scheid, how significant of an additional undertaking is it to establish values for property?

Mr. SCHEID. The valuation aspect of auditability will require a significant investment of time and resources, one that DOD has never undertaken in full. Participation is not just by auditors, but by many people across DOD, in every functional area of the Defense business space, both horizontally and vertically. That said, I recognize how important this information is in reaching full auditability, as required by law. DOD is looking into the most cost effective approach to establishing values and complying with standards.

14. Senator AYOTTE. Mr. Scheid, how many additional auditors are required to establish these valuations?

Mr. SCHEID. DOD is studying the cost of making and auditing property and equipment values. Valuation is only one element in the audit of PP&E. The valuation effort will require not only auditors but also program managers, asset owners, and all other stakeholders to be accountable and determine a reasonable methodology of establishing values for their assets. This effort will require a significant invest-

ment of time and resources across DOD. The auditors will verify not only the estimated value, but also the existence of our property, whether we have inventoried and reported all of our equipment and property, and whether we own or have the right to use that property. Given the complexity of this effort, a large number of audit staff will likely be required to validate the existence of the property and assess the reasonableness of the valuation methodology developed by DOD.

15. Senator AYOTTE. Mr. Scheid, are we talking about every M–16 and rucksack, or are we talking about larger items, like F–16s and M–1 tanks?

Mr. SCHEID. In most cases, we do not need to know the value of every item of equipment to perform our mission. Our current plan is to first compute values on our newer, high-value assets using actual costs or estimating methodologies that are permitted. Older assets will be valued, if deemed necessary. We do need to know depreciated value and remaining useful life of an asset as we make decisions that will shape valuation outcomes, such as disposition of equipment in theater.

16. Senator AYOTTE. Mr. Scheid, if this requirement were lifted, would it allow DOD to achieve key audit deadlines sooner and then to maintain that audit readiness less expensively?

Mr. SCHEID. Lifting the requirement would help but would not accelerate the target date, as there are other elements and processes associated with the financial statements that DOD is readying for audit. Less stringent requirements will certainly help with sustaining an audit ready environment once achieved.

5000.02 REISSUANCE AND THE SECTION 804 REPORT

17. Senator AYOTTE. Secretary McFarland and Ms. Takai, section 804 of the NDAA for Fiscal Year 2014 required the Secretary of Defense to develop and implement a new acquisition process for IT systems based upon the 2009 recommendations of the Defense Science Board (DSB). This resulted in a report from then Deputy Secretary of Defense, William Lynn, titled: "A New Approach for Delivering Information Technology Capabilities." The report listed five Guiding Principles for crafting a new acquisition system. Those Guiding Principles included:

- Deliver Early and Often: on shifting the acquisition culture from one which focuses on a single delivery of a system to one which comprises multiple deliveries every 12 to 18 months;
- Incremental and Iterative Development and Testing: which is very similar to "deliver early and often" but also calls for the use of prototyping and moving away from the deployment of a "Big Bang" approach;
- Rationalized Requirements: which seek to move away from customized solutions toward systems using open modular platforms based on established standards to ensure interoperability and seamless integration;
- Flexible/Tailored Process: specifically an acquisition process optimized for IT; and
- Knowledgeable and Experienced Workforce.

Which of these Guiding Principles were incorporated in the DODI 5000.02 reissuance and which were not?

Ms. MCFARLAND. The interim DODI 5000.02 issued on November 26, 2013, includes a series of models that serve as examples of program structures tailored to the dominant characteristics of the product being acquired. One of those models is a very flexible process designed specifically for Incrementally Fielded Software Programs. As implied by the title, the model provides capability via a multi-increment approach. Each increment provides rapid delivery of capability through several "limited fieldings" in lieu of a single full deployment. Each limited fielding provides the user with mature and fully tested sub-elements of capability. Several limited fieldings will typically be necessary to satisfy requirements for an increment and several increments will be required to achieve the required capability. This model will apply to many IT programs and particularly to cases where commercial off-the-shelf software, such as commercial business systems with multiple modular capabilities, are acquired and adapted for DOD applications. I believe this model, combined with our continued commitment to acquire, train, and sustain a first-class acquisition workforce is consistent with the five Guiding Principles.

Ms. TAKAI. The interim DODI 5000.02 includes guidance reflecting each of the five Guiding Principles and is consistent with the intent of the 2009 DSB recommendation. An overarching theme of the policy is that acquisition program strategies and oversight should be tailored to the unique characteristics of the product being acquired. The policy describes several acquisition models that accommodate

a range of IT from command and control systems to those types of IT systems that require delivery of capability early and often. Model 3, Incrementally Fielded Software Intensive Program, specifically addresses the need to quickly deliver incremental and iterative IT capability that satisfies DOD's requirements. To meet the increased flexibility of the acquisition process, it is critical that the acquisition workforce continues to improve. The interim DODI 5000.02 includes minimum standards and expectations for the program management office and the entire acquisition chain of command.

18. Senator AYOTTE. Secretary McFarland and Ms. Takai, what more needs to be done to ensure these Guiding Principles guide DOD acquisitions?

Ms. MCFARLAND. We believe our acquisition policy is well-designed and consistent with the Guiding Principles. Our objective is to ensure that the policies are institutionalized, effectively employed, and achieve the outcomes expected. We will closely monitor and make adjustments, when needed.

Ms. TAKAI. DOD recently issued guidance that establishes a policy framework consistent with the five Guiding Principles. My office will work with the office of the USD(AT&L) to ensure this new framework is incorporated into new IT acquisition programs and adjusted as necessary to ensure IT acquisitions are successful. Additionally, we will be working to ensure these concepts are integrated into our workforce training efforts.

19. Senator AYOTTE. Mr. Powner, to what degree do you believe these Guiding Principles are guiding DOD's IT acquisition processes?

Mr. POWNER. While DOD policies reflect its guiding principles, we have found that DOD's implementation of these principles needs to be more consistent. For example, as discussed earlier, the preliminary results of our ongoing work on selected agencies' implementation of incremental development indicate that DOD was lacking in areas related to two of these guiding principles ("Deliver Early and Often" and "Incremental and Iterative Development and Testing"). Specifically, only 1 of 37 selected DOD investments was delivering functionality every 6 months and departmental guidance was not consistent with OMB's guidance. We would be happy to share further details and brief your staff once our report is issued in May 2014. Similarly, our work on DOD's business systems modernization has found that DOD needs a more strategic approach to managing its human capital, which corresponds to the "Knowledgeable and Experienced Workforce" guiding principle.[3]

[3] GAO, DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability, GAO–13–557 (Washington, DC: May 17, 2013).