Testimony

Before the Senate Armed Services Committee

Subcommittee on Readiness and Management Support

Witness Statement of

HON Katrina McFarland

Assistant Secretary of Defense (Acquisition)

February 26, 2014

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 (MDAPs) and Major Automated Information Systems (MAIS) over which the Undersecretary of Defense 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 FY10 National Defense Authorization Act (NDAA) directed the DoD to develop and implement a new acquisition process for information technology systems based on the recommendations of Chapter 6 of the March 2009 Defense Science Board Report. Information technology represents a considerable portion of all acquisition programs within DoD. To help manage IT, the Department manages two fundamental types of software programs, National Security Systems (NSS) and Defense Business Systems (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.

Defense Business Systems, as defined in 10 U.S.C. 2222, are information systems, other than a National Security System, operated by, for, or on behalf of the DoD, including financial systems, management information systems, financial data feeder systems, and the information technology 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). The Department 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 the Department's Joint Capability Integration and Development System (JCIDS) 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 the Department'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 2010 NDAA.

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 decision-making 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 defense business systems 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 FY2010 NDAA, 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 FY 2011 NDAA which required DoD to develop a strategy for the rapid acquisition of cyber tools, applications, and capabilities for USCYBERCOM 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, the Department 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 Undersecretary of Defense for Policy. The CIMB membership includes the OSD Principal Staff Assistants (PSA's) to include the DoD CIO, the Services, DISA, NSA, USSTRATCOM and USCYBERCOM. Since March 2012, the CIMB addressed topics ranging from exploring the Cyber portfolios within the Science and Technology base, National Security Agency, and

USCYBERCOM; as well as Offensive and Defensive Cyberspace Operations, Defend the Nation, Cyber Situational Awareness and a holistic assessment of the cyber investment portfolio. The Department 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 Department initiative stemming from Section 933 is the Cyber Acquisition Process Pilot Plan. The plan was approved by the Undersecretary of Defense for Acquisition, Technology and Logistics 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 the Department's Better Buying Power initiative is continual process improvement. We find ourselves sustaining changes thru 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 to. Finding the expertise and skillsets 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 Defense Business Systems, 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; the Department, 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 Rep. Thornberry, Vice Chairman of the HASC. 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 (PARCA) 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 DAWDF funding, we will bring back lessons learned to the DAU to ensure we train our people on effective program management, engineering, logistics, contracting, etc.

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 the Department faces. In the last two years they have been able to help the Defense Logistics Agency (DLA) 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. The Department 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.