Statement of

The Honorable Peter Levine
Deputy Chief Management Officer
Department of Defense

before the

House Armed Services Committee
Subcommittee on
Emerging Threats and Capabilities

On

“Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network”

March 22, 2016

Good afternoon Chairman Wilson, Ranking Member Langevin, and Members of the Subcommittee. Thank you for this opportunity to discuss the information technology (IT) budget and the work the Department is doing to improve the effectiveness and security of IT systems in the Department.

My name is Peter Levine, and I have served as the Deputy Chief Management Officer of the Department of Defense since last May. Before that, I spent 28 years working for Senator Carl Levin of Michigan, the last two as Staff Director of the Senate Armed Services Committee.

As the DCMO, I provide direction and advice on improvements to business processes and practices in the Department with a particular emphasis on overhead and mission support functions. Soon after I started last year, the Deputy Secretary asked me to put together a package of efficiencies initiatives that would help free up needed funds to meet emerging needs in the current budget constrained environment. The initiatives that I am currently working on include headquarters reductions, service contract requirements reviews, and business optimization of the commissaries and exchanges. I have also been working on improving business processes, including the hiring process, the conference approval process, and the process for coordinating and issuing DOD directives and other guidance documents.

Two years ago this committee enacted legislation establishing a new Under Secretary for Business Management and Information, which will merge the offices of the DCMO and the CIO. However, the legislation does not take effect until the beginning of the next Administration. Until that time, the CIO – Mr. Halvorson – remains the responsible OSD official for the Joint Information Environment, information assurance activities, and other IT program and budget issues addressed in your letter of invitation.

The DCMO does, however, play a key role in reviewing investments in IT business systems. About two years ago, the Department restructured the Defense Business Council – the body that approves business system investments – so that it is now co-chaired by the Department

DCMO and CIO. The membership of the DBC includes both the DCMOs and CIOs from each of the military departments. This gives us an opportunity to look at investment decisions both in the context of business process improvements and technical compliance with IT standards, to include compliance with cyber security requirements.

Last year's NDAA includes a provision – section 883 – that substantially streamlines legislative requirements addressing the investment review process administered by the DBC. I thank you and your staff for that provision: it will enable us to avoid getting mired in small detail and focus instead on broader issues.

We intend to use the new flexibility in three important ways.

First, we intend to change our focus from the discrete review of each small investment to broader and more comprehensive portfolio reviews. We have designated portfolio managers for key investment areas. These portfolio managers are developing strategic plans, which will be used to guide and evaluate business system investment decisions. This approach has already yielded positive results in the military departments; we hope to achieve similar benefits by applying the same methodology to investments by OSD and the defense agencies and field activities.

Second, we plan to focus more closely on Return on Investment. The Department has long required that a business case analysis be developed for each major business system investment. Unfortunately, we didn't always pay enough attention to what was in these analyses. When we make a major new business system investment, we should have a plan for turning off legacy systems. We should also have a plan for reducing manpower requirements where we can implement more efficient and less manpower-intensive business processes. Some past business case analyses didn't address these issues. Even where they were addressed, we didn't always follow through and ensure that the projected efficiencies and resulting savings were actually achieved. We are working to change that.

Finally, the new statutory flexibility provides an opportunity for the Department to harmonize separate DCMO, CIO, and AT&L approval reviews for business systems investments. The current lack of coordination between these processes often means that business portfolio managers identify a problem, build a business case for the best solution, and then have to hand off to acquisition officials – who start the analysis all over from the beginning. In some cases, I am told that the business case analysis recommends a small tweak to existing systems, but the acquisition system responds by establishing a program office, which may develop an entirely new and expensive solution.

We are currently working with the Under Secretary of Defense for Acquisition, Logistics, and Technology to address this problem by developing a streamlined and coordinated process for business system investments. We believe that our reengineered process should be able to align acquisition oversight, Defense business system certification and CIO technical requirements beginning in the requirements process, carrying through the consideration of alternatives, and supporting the actual acquisition of a final IT capability. Our goal is to better deliver capability, with appropriate oversight, while removing many of the burdens levied on the IT functional and program managers.

Mr. Chairman, the DCMO is firmly committed to closely partnering with the CIO, the USD(AT&L), and other key DOD officials to improve the processes and practices by which the Department acquires and deploys business IT capabilities. By doing so, we hope not only deliver improved mission performance at reduced cost, but also to "bake in" cyber security and information access control from the beginning of the requirements process. I look forward to working with your committee as we continue this effort.