

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

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES
HEARING ON CREATING A FLEXIBLE AND EFFECTIVE INFORMATION
TECHNOLOGY MANAGEMENT AND ACQUISITION SYSTEM

April 26, 2017

Chairman Stefanik, Ranking Member Langevin, and Members of the Subcommittee, thank you for this opportunity to appear before you this afternoon.

My name is Peter Levine, and in 2015 and 2016, I served in the Department of Defense, first as Deputy Chief Management Officer (DCMO) and then as Acting Under Secretary for Personnel and Readiness. Before that, I spent 28 years working for Senator Carl Levin of Michigan, the last two as Staff Director of the Senate Armed Services Committee.

The views I express are entirely my own, and should not be interpreted as reflecting any position of my new employer, the Institute for Defense Analyses (IDA). IDA is a government contractor. However, I am testifying in my individual capacity, and as such, I do not have any federal contracts or grants, or any contracts or payments from a foreign government, to report.

I understand that you have invited the three of us here in our capacity as former DoD officials to discuss the manner in which the Department organizes and manages its information technology (IT) and cyber programs and workforces. It's a big subject. Information Technology is everywhere in the Department. It's not just in our core C3I systems – our communications systems, our command and control systems, and our intelligence systems. It runs our logistics systems, our acquisition systems, our financial systems, and our HR systems. And of course it central to the operation of every one of our weapon systems.

This makes for an exceptionally complex governance problem. With regard to the acquisition of new or upgraded business systems, for example, the Chief Information Officer (CIO) has a vital role in ensuring compliance with IT

architecture and cyber requirements, but others have equally important roles. The Chief Management Officer is responsible for ensuring that business case analyses have been conducted and appropriate business process reengineering will take place, while the Chief Acquisition Officer (AT&L) is responsible for ensuring the use of appropriate procurement mechanisms and providing effective oversight of contractor cost, schedule, and performance.

It would be nice to think that we could make the Department more efficient by giving all of these authorities to a single official or office, but experience shows that it is just too big of a job. When AT&L tried to run business system acquisition by itself, it lacked both expertise in business process reengineering and the authority to insist that requiring the components – their customers – get it done. When the DCMO tried to take charge, it became bogged down in technical minutiae and lost track of the big picture. I do not believe that the CIO has the expertise and authority needed to do the job by itself either.

For this reason, all three offices need to play a continuing role. The key to making this work is ensuring that each office stays in its appropriate role of providing policy guidance and oversight, rather than trying to run the programs directly out of the Office of the Secretary of Defense (OSD). Policy and oversight reviews are a lot easier to coordinate than day-to-day management decisions. If business system programs are run by program offices in the components as they should be, the CIO, the DCMO, and AT&L can all provide oversight in their appropriate lanes.

Of course, there will always be substantial overlap: a business case is likely to address many of the same issues as an acquisition plan, and an acquisition plan won't be complete unless it addresses cyber and architecture requirements. If the Department isn't careful, program offices could be whipsawed back and forth, as they have to comply with different review processes, at different times, for the same issues.

When Terry and I were the CIO and the DCMO, we had a smooth coordination process: major decisions on business systems were approved by both of our offices, as well as AT&L. However, that the process can and should be made more efficient by better sequencing the acquisition review process, the architecture review process, and the business case review process.

When I testified before this Subcommittee a year ago, I promised to take on this project. Although I left to take a new job as Acting Under Secretary for

Personnel and Readiness two weeks later, I understand that the effort culminated with the issuance of a new DoD Instruction 5000.75, which was jointly approved by the AT&L, CIO, and DCMO on February 2, 2017. I urge you and your staff to have the Department brief you on this new policy.

The effort to coordinate the positions and activities of the DCMO, the CIO, and AT&L also dovetails with the requirement that Congress established, under sections 901 and 902 of the FY 2017 NDAA, for the Department to reexamine the roles of the DCMO and the CIO.

With regard to those provisions, the Committee made the right decision in keeping the DCMO and the CIO as separate offices. When we looked at planning a merger between the two offices a year ago, we found very few areas of overlap. We were basically pasting together two organizational charts without change. The DCMO plays no role at all in IT other than business systems, and even with regard to business systems, the DCMO and the CIO have completely different areas of expertise.

The new Chief Management Officer (CMO) should maintain the role that the DCMO currently plays in reviewing investments in IT business systems. When I was DCMO I tried to focus these reviews on Return on Investment. When we make a major new business system investment, we should have a plan for turning off legacy systems and for reducing manpower requirements based on new, less manpower-intensive business processes. The new CMO will be a success if he or she can ensure not only that these plans are developed, but that they are carried out and the savings actually achieved.

Beyond that, the Department would do well to consider an additional role for the new CMO as a resource that other elements of the Department could turn to for assistance in organizational streamlining and process improvement. The DCMO engages in some of these activities now, but their effectiveness is limited by the fact that the requirements tend to be imposed from the outside. The office would get more cooperation and achieve better results if instead of seeking to impose savings initiatives on the components, its role were to assist the components in their own efficiencies efforts.

When I was serving as Acting Under Secretary for Personnel and Readiness, I asked the DCMO for assistance on process improvements and organizational streamlining on several occasions. Of course, since I was still the Senate-confirmed DCMO, they were pretty good about giving me the help that I needed.

It would require some new resources and capabilities, but the Department could really use an internal management consultant, and the new office of the CMO would be the ideal place to put it.

At the same time, it would be a mistake to give the CMO responsibility for overseeing the management of Defense Agencies like DLA, DFAS, and the Defense Health Agency, as some have suggested. If management oversight is divorced from policy responsibility, both functions are likely to be less effective. Moreover, these added responsibilities would overwhelm the resources and capabilities of the DCMO, making it unlikely that the new office would be able to serve the more important function of driving organizational improvement throughout the Department.

I urge you to consult with some of the capable career officials in the Department about these issues before you proceed. When I was DCMO, Dave Tillotson served as my deputy; he is now acting DCMO and will undoubtedly play a key role in getting the CMO legislation off the ground. Nobody is more familiar with the office and what it is (and is not) capable of.

You have asked what the Department could do to improve its IT acquisition processes and better leverage commercial industry best practices. This issue was thoroughly explored in a March 2009 report by the Defense Science Board, which recommended the development of a separate acquisition process for IT systems. The DSB recommended a process that incorporated early and continual user involvement; multiple, rapidly executed increments or releases of capability; early, successive prototyping to support evolutionary acquisition; and a modular, open-systems approach.

Section 804 of the FY 2010 NDAA directed the Department to develop an IT acquisition policy along these lines, but I do not believe that the Department met the intention of the provision. For this reason, Section 804 of the FY 2015 NDAA directed the Department to revisit the requirement. I still believe that the DSB recommendations were sound. Sometime in the near future, the Department should have a new acquisition policy team in place; I would encourage you to take up the DSB recommendations with them and see if more progress can be made.

Finally, I would like to turn to the IT and cyber workforces. When Terry and I were in the Department, we greatly appreciated the new authority that the Department gave us for the cyber workforce in section 1107 of the FY 2016 NDAA. The Under Secretary for Personnel and Readiness teamed with the CIO

and the Principal Cyber Advisor to implement this legislation. Before we left, we had an approved plan in place to establish a new personnel system that should make it easier to recruit and retain the talented personnel the Department needs to protect our information systems.

However, the new personnel system is just step one of a broader plan. It isn't enough to have the authority to hire capable people – the Department needs to know where the gaps are in its workforce and what kind of people it should hire to fill those gaps. In other words, the Department needs a strategic workforce plan for its cyber workforce. We initiated this effort last year, but we didn't get very far before the end of the Administration. I think it would be helpful for the Subcommittee to call this issue to the attention of the new team as well.

Thank you again for inviting me to testify today. I look forward to your questions.