Testimony before the House Armed Services Committee Panel on Defense Acquisition Reform

Ronald L. Kerber

Introduction

It is my pleasure to testify before the House Armed Services Committee Panel on Defense Acquisition Reform. My name is Ronald Kerber and I am appearing before you as a member of the Defense Science Board (DSB). As a member of the Board, I led three task forces that inform my testimony today. I must also state that the views expressed today may or may not represent the official views of the Department of Defense. I was asked to pay special attention to the Defense Science Board findings "especially as they pertain to 'root causes' or system problems inhibiting our ability to effectively acquire IT systems." My testimony is supported by three Defense Science Board reports:[1]

- *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March, 2009
- *Creating a DOD Strategic Acquisition Platform*, April 2009
- *Information Management for Net-Centric Operations*, April 2007

I will break my testimony into two parts. Part 1 will deal with general issues pertaining to the Department of Defense (DOD) acquisition process. Part 2 focuses on issues peculiar to the acquisition of information technology.

General Acquisition Process Issues

Fixing the DOD acquisition process is a national security issue.

Today, the defense acquisition process takes too long to produce weapons that are too expensive and often technically outdated by the time they are fielded. Typical major system acquisitions take 10–15 years, while new product development in the commercial sector of similarly complex systems takes one third to one half of that time. Acquisition of information technology, on which many defense systems are

1. Copies of these reports have been provided to the Committee.

critically dependent, also exceeds typical commercial development time—taking three to four times as long. These development times are far outpaced by the rapid advances in technology, which means that subsystems can be one or two generations old by the time a system is provided to war fighters in the field—unless upgrades are incorporated before the system is fielded. Furthermore, programs often have large cost overruns, long schedule delays, and unsatisfactory product quality and performance.

At the same time, the nation faces very adaptive adversaries. The United States is no longer in a unique position of technological supremacy. Many types of advanced technology are readily available on the world market. Adversaries are becoming very adept at fashioning new weapon capabilities from commercially available technology—"good enough" systems are developed and fielded quickly. And, these adversaries are often far more agile in doing so than is the United States. Most military planners recognize that a robust military strategy combines a formidable offense with a capable and comprehensive defense. But some current adversaries can target U.S. vulnerabilities and time their attack without concern for the risk of U.S. offensive retaliation—as they have little of value to put at risk. Adaptive adversaries are able to identify U.S. vulnerabilities and create effective systems to exploit them—one example is improvised explosive devices that became prominent early in the Iraq conflict and continue to plague U.S. forces. When rogue states and terrorists employ this strategy, it creates a particular challenge for the nation. Thus, we too must be able to more rapidly and effectively transition commercial and military-unique products to our war fighters in the field.

While this scenario applies to all weapon systems, information technology presents a somewhat different set of challenges due in large measure to the fact that it is an important enabler for so many defense capabilities. It underlies the nation's ability to gain better intelligence, better situational awareness of the battlefield, better communications, and more precision in weapon system delivery. In fact, the use of information technology is pervasive, from administrative systems for managing business processes, to embedded subsystems in major weapon systems—comprising as much as 90 percent of the cost of some new systems.

Despite its crucial importance, the Department's ability to acquire information technology is fraught with problems. Driven by the short half-life of commercial information technology, hardware supportability, software applications, and evolving operational requirements, continuous upgrades and product improvement are a reality that must be accommodated by the acquisition process. In addition, it is often difficult to technically validate these programs to ensure that what is being delivered is in fact what is expected, raising the potential for unknown system vulnerabilities.

Furthermore, many information technology systems are managed as joint programs, ultimately used by more than one of the military services. Systems such as intelligence, surveillance and reconnaissance; command and control; and communication systems are often acquired as joint programs to ensure interoperability and common fielding dates among the user services. As a result, managing these programs requires joint cooperation among the services—something that can become a challenge to effective acquisition. Stable budgets and system interoperability—that is, systems developed to operate with many others on the battlefield—are challenging criteria that can be difficult to achieve and remain important issues.

Finally, the acquisition of services receives far less attention than that of materiel, yet it is a growing part of the defense budget—representing about 50 percent of the acquisition budget. Services range from support to the battlefield, to airlift and logistics, to security services, janitorial services, studies and analysis and information technology support services. Such activities are not only necessary but also smart to contract as services so that DOD personnel can devote their time to the jobs they were trained to do. Yet it is still reasonable to ask whether all such contracts are necessary and whether they could be contracted more efficiently. Service contracts should be subjected to the scrutiny and be required to meet certain criteria similar to materiel acquisition.

The problems of acquisition execution outlined above have been well known for years. Yet an even more important deficiency is the process that determines what to buy. The strategic plan for acquiring military capabilities is only loosely aligned with national security objectives and the military missions to achieve them. The military services are tasked to train and equip the nation's forces and they often control the input into the process—defining the capabilities to be acquired. The combatant commanders, who actually use forces and equipment in the field to execute missions, have little input into what next-generation capability will be acquired. Often present programs reflect past missions and seldom adequately support joint needs, despite the fact that ongoing combat experiences demonstrate new joint needs and interoperability issues. Clearly the driving agenda item that the Department needs to address is the process that determines what to buy to support the highest priority national security mission needs.

The shortcomings addressed here point to an acquisition process that is inadequate to meet the needs of the Department of Defense. Fixing this process must become a departmental priority—led by the Secretary of Defense.

There have been many attempts to fix the acquisition process, but none, as of yet, have been successful.

The defense acquisition process has been studied for decades—by the Packard Commission, the Government Accountability Office, the Defense Science Board, think tanks, commissions, and many other organizations, including the Department itself. For decades, these studies have identified numerous flaws—problems with bureaucracy, accountability, overlap of authority, inefficient processes, and inexperienced leadership. And over the years, the Department has made a series of attempts to "fix" acquisition—usually at the direction of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Yet problems persist—major system acquisitions still take too long, costs are overrun, and concerns remain over product performance and quality.

Why have previous efforts so often failed? In part, it is because they fail to address the root causes of the problem, focusing instead on re-engineering the mechanics of the acquisition decision process. Many problems appear to be caused by the use of immature technology, requirements "creep," or funding instability. **Such problems, however, are really only symptoms of the lack of experienced judgment on the part of Department personnel who structure acquisition programs in a way that will almost certainly lead to failure.**

Moreover, many organizations in DOD are often not aligned with departmental acquisition goals and objectives. The staff of the Office of the Secretary of Defense—including the Director, Program Analysis and Evaluation; the Comptroller; the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer; Director, Defense Research and Engineering; and Director, Operational Test and Evaluation—the military services, and the Joint Staff are all power centers that not only often fail to be aligned with each other, but sometimes are not even aligned within themselves. Hence, many of the Secretary's advisory staff, who are not accountable for delivering acquisitions, can stall a program's ability to proceed through the process while awaiting their input.

Perhaps the most important reason that previous efforts have failed, however, is that the problem has been left to the Under Secretary of Defense for Acquisition, Technology, and Logistics. But the acquisition challenge is much bigger and broader than the authority or scope of power of that office. Many of the organizations, functions, and processes that support acquisition are not, and should not be, the responsibility of the acquisition under secretary. Fixing defense acquisition is a challenge that can only be successfully addressed by the Secretary of Defense, and it should be among his top priorities. The Secretary not only must lead the charge within DOD to fix the acquisition process but also must inform the Congress of

departmental actions and enlist its support for his agenda, least Congress act independently in a way that undermines his efforts.

There is no silver bullet for "fixing" acquisition. As noted previously, many studies have identified many problems and offered many solutions. One particular difference in the findings and recommendations drawn from a decade of past studies by the Defense Science Board is in how the problem is defined. Fixing acquisition challenges must begin with leadership action by the Secretary of Defense. And it must address not only "how" the Department buys material but also "what" materiel the Department buys, who is involved in the process, and whether support systems help or hinder.

The Secretary of Defense must create a strategic acquisition management platform comprised of four critical elements.

1. **Buy the right things.**

   The strategic military planning system, DOD's regime for deciding "what to buy," has a weak analytic foundation. When we buy the wrong thing, we blame the acquisition system. But that system is responsible for "how to buy." Before fixing the acquisition processes, the Secretary must reform the strategic military planning system and create a genuine "business plan" for DOD. The plan should be developed with greater involvement of the regional combatant commands and better use of systems engineering and of modeling and simulation.

2. **Select an effective leadership team.**

   Proven, relevant experience is needed in the Office of the Secretary of Defense, the military departments, and defense agencies. Today, many people are inexperienced, from leadership to program managers. Few have a personal track record of repeated successes at acquisition. Trial-and-error and on-the-job training can be really expensive. The Department needs to hire and assign individuals with proven records of acquisition success. This may mean facing the possibility of not doing a program until the right people are available. In order to determine the "right size" for the acquisition workforce, the Department can use process mapping and work flow analysis to determine the necessary functional staffing and to eliminate overlapping accountability and authority which leads to excessive bureaucracy.

3. **Reform and streamline the acquisition process.**

   A single acquisition process cannot meet the needs for acquiring major systems, commercial derivatives, and information technology systems, and to rapidly field critical war fighting needs in time of crisis. The process to buy major systems, information technology systems, and commercial derivatives

needs to be streamlined with up front, strong systems engineering support. The case of information technology presents unique challenges—in stand-alone systems, embedded systems, and net-centric infrastructure. A new system is needed that recognizes the rapid advances in information technology and plans for frequent and efficient upgrades after delivery. Fielding critical war fighting needs in time of conflict also requires a new approach—a standing acquisition capability that can fulfill these requirements in a timely way, as there is little doubt that the need will continue.

4. **Improve acquisition execution.**

   Acquisition improvements are not enabled by policy and process reforms alone. They must be coupled by efficient, effective execution. Key areas where improvement in management and execution are needed include: product development management, contract award and management, acquisition workforce, acquisition integrity, and process metrics. Central to these improvements is experienced personnel with reinforcing incentives—in leadership, in the acquisition workforce, and, equally important, in the contractor base. Up front attention to systems engineering during product development as well as keen attention to acquisition integrity are also essential ingredients.

Many may say that they are already doing what is recommended here. In fact the recommendations are essentially common sense and one may find each concept used in an isolated case. The real message presented is that a comprehensive approach must be used uniformly across the defense enterprise to be successful. In fact if "they were already doing this" comprehensively there would be no problem or need for your Panel.

Issues Peculiar to the Acquisition of Information Technology

Information technology (IT) offers immense capability in terms of agility, flexibility, responsiveness, and effectiveness. It enables nearly all of our military combat capability and has become a necessary element of our most critical warfare systems. However, there is growing concern within Congress and among DOD leadership that the nation's military advantage may be eroding. The deliberate process through which weapon systems and information technology are acquired by DOD cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States.

Certainly, barriers that preclude transformation of the U.S. national security apparatus to meet the challenges of a new strategic era are of particular concern. Nearly a decade ago the Department established a vision for the architecture and structure for information system management—a vision that is still evolving. However, it is well known that acquisition has not been well managed for these systems within this "enterprise level" construct, and the result has not served today's leaders and soldiers well. In fact, it hinders the war fighters' ability to use information technology to its fullest potential for situation awareness, collaboration, and rapid decision-making. The resulting operational impact is profound.

Yet despite the current situation, successful programs exist that comprise largely or exclusively of information technologies or are deeply dependent on information technology in execution. The question then arises as to whether there are elements common to the acquisition of these successful programs that would improve the Department's ability to field advantageous information technology in a timely and cost-effective manner.

Recently, acquisition policy was again modified in part to add more rigor and discipline in the early part of the acquisition process. Likewise, the Joint Capabilities Integration and Development System (JCIDS) Instruction and Manual are being updated with changes to the Joint Staff's oversight and governance of IT programs. These policies derive from a single acquisition model that applies to both major automated information systems and major defense weapon systems acquisition programs.

Information technology is pervasive in weapon systems as well as defense business systems. In its contributions to both functionality and cost, information technology now represents a considerable proportion of all acquisition programs underway today—a proportion that is likely to increase in the future. Thus, whether existing DOD acquisition policies and processes provide the foundation for an effective information technology acquisition model is a critical question for the Department—one that deserves special attention from the Secretary of Defense.

At the request of Congress, the Defense Science Board undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The findings and recommendations, presented in the *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology,* are the result of a study that was broad in scope, as established in legislative guidance—covering acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to information technology acquisition.

A key finding of the DSB review is **that there is a need for a unique acquisition system for information technology**. Such a process must be designed to accommodate the rapid evolution of information technologies; their increasingly critical position in DOD warfare systems, warfare support systems, and business systems; and the ever evolving and often urgent IT needs of the war fighter. The current conventional process, with its recent improvements, would be used when a system requires significant scientific or engineering technology development, particularly hardware development or the integration of many complex systems requiring design and functionality partitioning and trade-offs.

Problems that plague IT acquisition are similar to those that plague the acquisition of major systems, most of which have a high content of embedded IT. **The conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many systems that require continuous changes and upgrades**—a reality driven by the short half-life of commercial information technology, supportability of hardware (which is often a commodity), software applications, and operational requirements. Thus, the Department's leaders must take action to address this problem. Toward that end, the DSB task force offered the following recommendations to change the Department's approach to information technology acquisition.

Statutory Restrictions

The task force believes that the statutory framework is workable and is not a major impediment to improving IT acquisition within DOD. Therefore, no recommendations are offered in this area. The main issue with regard to statutory influence is that Congress has lost confidence in DOD's execution of IT programs, which has resulted in increasing program scrutiny and budget actions (generally funding cuts) for programs that are faltering. Since DOD implementation of IT acquisition has fallen short, Congress has added additional constraints on reporting and management, these could become problematic when and if DOD begins executing programs well.

Acquisition Policies

Acquisition policies (DOD Directive 5000.1 and Instruction 5000.02) are principally designed for programs where technology development for hardware and software is a critical component. The recent revisions to DOD Instruction 5000.02, implemented December 2008, offer improvements to the process but do not address the fundamental challenges of acquiring information technology for its range of uses in DOD. Instead, a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions.

RECOMMENDATION 1. NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY

The Secretary of Defense should:

- Recognize that the current acquisition process for information technology is ineffective. Delays and cost growth for acquisition of both major weapons systems and information management systems create an unacceptable risk to national security.
- Direct the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) and the Vice Chairman, Joint Chiefs of Staff to develop new acquisition and requirements (capabilities) development processes for information technology systems. These processes should be applicable to business systems, information infrastructure, command and control, ISR (intelligence, surveillance, and reconnaissance) systems, embedded IT in weapon systems, and IT upgrades to fielded systems.
- Direct that ALL personnel within the Office of the Secretary of Defense (OSD), the Joint Staff, and the Services and agencies involved with acquisition be accountable to ensure that their efforts are focused on the improvement, streamlining, and success of the new process.

The DSB proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities (Figure 1). The process is agile, is geared to delivering meaningful increments of capability in approximately 18 months or less, and leverages the advantages of modern IT practices. Multiple, rapidly executed releases of capability allow requirements to be prioritized based on need and technical readiness, allow early operational release of capability, and offer the ability to adapt and accommodate changes driven by field experience.

The process requires active engagement of the users (requirements) community throughout the acquisition process, with requirements constructed in an enterprise-wide context. It is envisioned that requirements will evolve so “desired capabilities” can be traded off against cost and initial operational capability to deliver the best capability to the field in a timely manner. A modular, open-systems methodology is required, with heavy emphasis on “design for change,” in order to rapidly adapt to changing circumstances. Importantly, the process needs to be supported by highly capable, standing infrastructure comprising robust systems engineering, model-driven capability definition, and implementation assessments—to reduce risk, speed progress, and increase the overall likelihood of repeated successes. Early, successive prototyping is needed to support the evolutionary approach. In addition, key

stakeholders—the Chief Information Officer (CIO), Program Analysis and Evaluation (PA&E), Director of Defense Research and Engineering (DDR&E), and Operational Test and Evaluation (OT&E), the Comptroller, operational users, and others—need to be involved early in the process, prior to the milestone build decision.

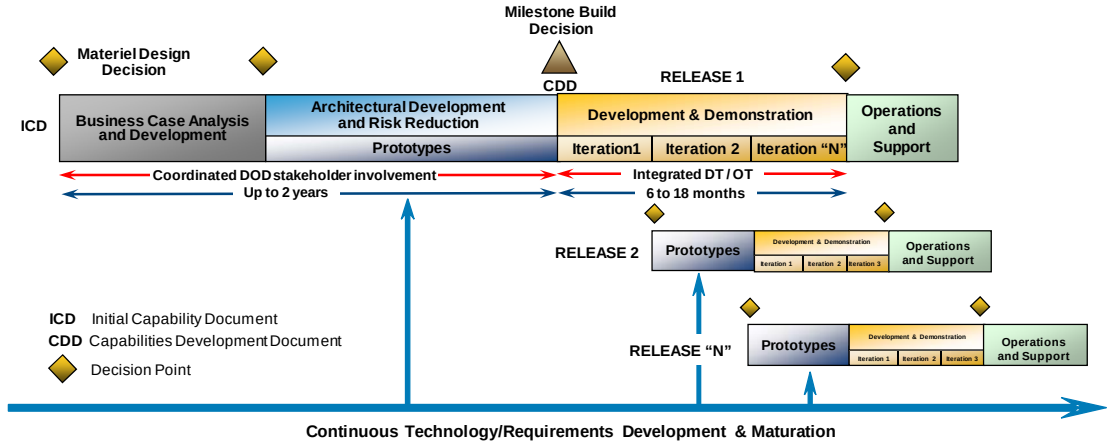

Figure 1. **A New Acquisition Process for Information Technology**

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational test practiced during the development and demonstration phase for each capability release. Contracting vehicles need to be devised that are flexible enough to support this agile process. These vehicles must allow for changes in delivered capability within a particular increment as well as allow capability to be deferred to subsequent increments if needed. Crucial to the success of a new process is continuity of funding, so as to maintain a solid funding stream for following, sometimes overlapping, capability releases.

Along with the flexibility built into the process, relevant metrics, similar to those used in commercial practice, are needed to continuously track IT acquisitions to ensure that the expected capability is being provided, costs are being managed, and the schedule to initial capability is on track. Finally, just as there is no substitute for acquisition leadership experience in DOD; the same is true for the contactor community. For contact award, program managers need to strongly consider relevant contactor experience and past performance, especially in large acquisitions, and ensure that key personnel are committed for the duration of the project.

This new process will have applicability over a broad range of new DOD IT acquisitions and upgrades to existing national security systems (including command and control systems), IT infrastructure, and other information systems (Figure 2).

Information technology is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

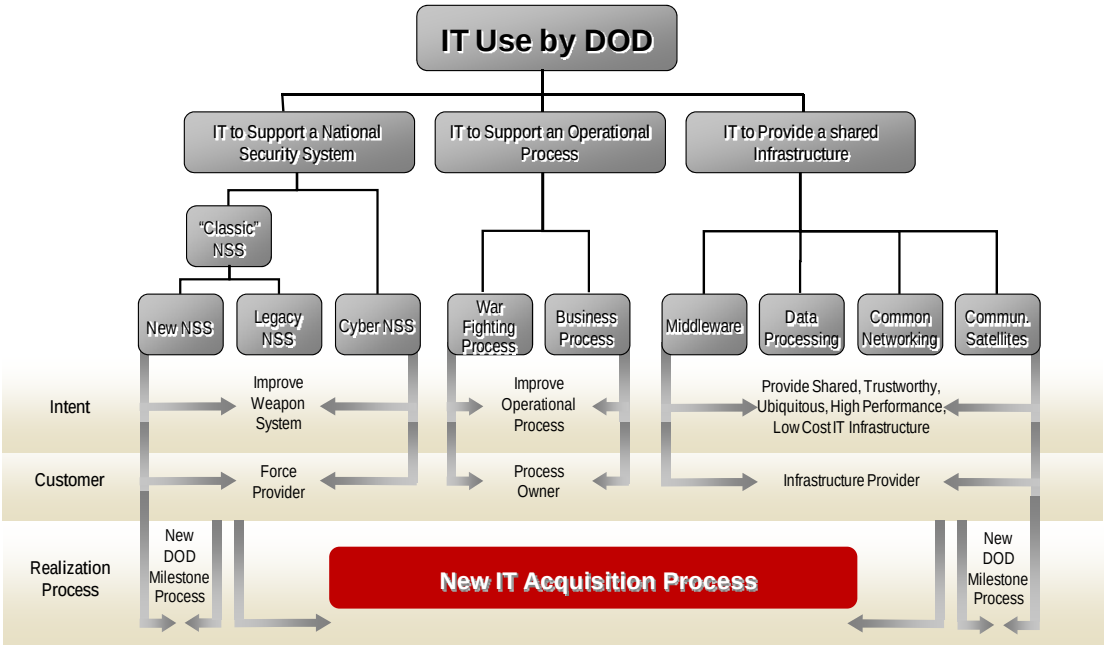

Figure 2. An Information Technology Acquisition Framework

Deciding When to Use the New IT Acquisition Process

It is important to clarify when to use the new IT acquisition process versus the improved DOD 5000.02 process for major weapon systems and communication satellites. In addition, it is also necessary to reduce potential confusion about technology development.

The use of the improved DOD 5000.02 process for major weapon systems is required when there are many design tradeoffs for both hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in the new system, while assuring interoperability and network compatibly with the larger enterprise. At the same time there are likely to be areas of needed technology development that require advances in science and engineering that have little or nothing to do with IT—such as new material properties, increased speed, or stealth. This later scientific and engineering technology development should not be confused with the traditional jargon of the IT community that defines technology development nearly interchangeably with software development and hardware integration.

The use of the new information technology acquisition process is for new or replacement stand alone IT systems and subsystems, or for replacement IT systems embedded in existing weapon systems that are to be upgraded when there is little or no change in the hardware not associated with IT. It may also be appropriate to use the new IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the information technology could otherwise be a few generations old when the system is fielded.

While one could argue that the required decision as to which acquisition process to use could add confusion, one could also argue that if the leadership and program managers cannot sort out this high-level decision they have no chance of effectively managing or overseeing the program.

Roles and Responsibilities of the ASD (NII)/DOD CIO

Developing and implementing an acquisition process for information technology is an important step toward reducing delays and cost growth in information technology programs, as well as providing capability more rapidly to the war fighter. Perhaps equally important, however, is clarifying roles and responsibilities of the key players in the process—chief information officers and those individuals who hold milestone decision authority (discussed in the next section).

The DOD CIO function is currently housed in the Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (OASD (NII)/DOD CIO). DOD CIO responsibilities are delineated within titles 10, 40, and 44 of the U.S. Code. As designated in legislation, the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO) reports directly to the Secretary of Defense—a reporting chain that is critical and must continue in order for the ASD (NII)/DOD CIO to have the necessary authority to carry out important department-wide functions.

The ASD (NII)/DOD CIO should have strong authority and responsibility for information policy vision, architecture, infrastructure, standards, spectrum, information assurance, interoperability, and enterprise-wide systems engineering. The ASD (NII)/DOD CIO should be the Department's single authority for certifying that IT acquisitions comply with an enterprise-wide architecture and should continually review ongoing programs for architectural compliance. He or she should also be a ruthless designer of "the enterprise" infrastructure and should approve IT program manager training and certification.

These functions are also applicable to CIOs at the Service and agency level. To execute the above responsibilities, Service and agency CIOs should also directly report to the head of the Service or agency, as required by legislation.

RECOMMENDATION 2. ASD (NII)/DOD CIO RESPONSIBILITIES

The ASD (NII)/DOD CIO should actively exercise his or her authority to certify that all IT acquisitions are consistent with the Department's net-centric architecture.

The ASD (NII)/DOD CIO should have strong authority and responsibility for enterprise-wide information policy vision, architecture, infrastructure, meta data and other standards, spectrum, interoperability, information assurance, and system engineering.

Certain capabilities in the OASD (NII)/DOD CIO must be strengthened in order to more effectively execute these responsibilities—in particular, system engineering, information assurance, and network integration.

In the Services and agencies, the CIOs should also have strong authorities and responsibilities for system certification, compliance, applications development, and innovation.

All CIOs should approve IT acquisition program manager training and certification and advise the personnel selection process.

The DOD CIO, supported by CIOs in the Services and agencies, should be responsible for certifying that systems and capabilities added to the enterprise do not introduce avoidable vulnerabilities that can be exploited by adversaries.

Both system vulnerability to sophisticated adversary threats and information and mission assurance should be addressed throughout program development, particularly in the early stages during the business case analysis and development phase. As new capabilities, infrastructure, and applications are added to a system, this same assessment should be continuously monitored with particular emphasis on source code analysis and supply chain risk assessment. A robust testing program must also be established to minimize the introduction of new vulnerabilities. New capabilities need to be tested in realistic test beds under a variety of threat scenarios.

Information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. Information technology is far too important to the Department's war fighting and business endeavors to neglect information and mission assurance, as the consequences of doing so can undermine not only the current system but also other connected capabilities as well. In this context, it is instructive to remember that there is no way to test a large IT system to assure that

you "got what you wanted" and only what you wanted. **Thus, since it is not possible to assure that an IT system is entirely safe and reliable, operators (combatant commanders) must develop field testing procedures; tactics, techniques, and procedures; and concepts of operations to test system authenticity and operate with degraded systems. Exercises must include and test these concepts of operation.**

Milestone Decision Authority Roles and Responsibility

Clear roles and responsibilities of those with milestone decision authority are essential if a new acquisition process is to be successful and the desired outcomes achieved. The lack of clarity in this regard is one of the most significant impediments to successful implementation of the current process. The task force believes that the preferred approach should be delegation to the lowest level acquisition decision authority consistent with program risk.

Furthermore, acquisition authority and expertise within OSD is currently spread across several organizations—under the USD (AT&L), in OASD (NII)/DOD CIO, and in the Business Transformation Agency. At the Service level, similar disaggregation of responsibility also exists. This disaggregated approach seems inefficient, resulting in a lack of enterprise-wide architecture and coordination. Qualified IT acquisition and systems analysis and architecture personnel are scarce and should not be spread among separate OSD organizations. Given the speed with which information technology advances, this disaggregation exacerbates the ability to maintain currency and coordination within the acquisition workforce.

It is important to recognize that IT acquisition requirements are different and, because IT touches nearly everything acquired by the Defense Acquisition Executive (the USD (AT&L)), it is more than a side consideration. Bringing together the expertise from many organizations into a single one will help to ensure that the unique attributes of IT programs are better understood. In addition to the milestone decision authority responsibilities and organization, the Defense Acquisition Executive advisory staff (DDR&E, PA&E, OT&E, Comptroller) issue definition and resolution process often contributes to extended IT acquisition times.

RECOMMENDATION 3. ACQUISITION AUTHORITIES AND ORGANIZATION

The USD (AT&L) is responsible for all acquisitions, the acquisition workforce, and is the Milestone Decision Authority for all major defense acquisition programs, major automated information systems, and special interest programs. The USD (AT&L) should:

- aggressively delegate milestone decision authority commensurate with program risk
- consider a more effective management and oversight mechanism to ensure joint program stability and improved program outcomes

Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization, those elements of the OASD (NII)/DOD CIO and Business Transformation Agency responsible for IT acquisition oversight. The remainder of OASD (NII)/DOD CIO is retained as it exists today, but should be strengthened as indicated in the previous recommendation.

Acquisition Expertise

A high degree of relevant technical and proven management capability is needed for IT system acquisition leadership. In addition, a set of IT domain experts are needed within the acquisition community to support acquisition oversight and decision-making. OSD and the Services need IT acquisition staff with extensive experience in large-scale, embedded, and commercial IT.

Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Skills in program administration are confused with skills in operational process design and/or with skills in IT. Contracting, budgetary, and organizational design debates crowd out concepts of operations and system engineering debates. Further, architecture is too often viewed as a paper exercise rather than a model-driven, analytically supported, and rigorous engineering process incorporating enterprise-wide considerations for functionality and interface definition. Within the Department, IT expertise is scarce and the competition for talent is increasing.

There is no substitute for experienced program managers with track records of proven success. In a review of major IT acquisition programs where cost, schedule, or quality and performance were issues, three root causes emerged. First, senior leaders lacked experience and understanding. Second, the program executive officers and program managers had inadequate experience. Third, the acquisition process was bureaucratic and cumbersome, where many who are not accountable must say “yes” before authority to proceed is granted. Some of these issues have been discussed previously in this testimony, but among these problems, lack of experience dominated.

The experience and qualifications of OSD and Service leaders, and program executive officers and program managers is critical to making the **right judgments** to begin a program with executable objectives and then manage it to successful completion.

RECOMMENDATION 4. ACQUISITION EXPERTISE

The Secretary of Defense shall require that the defense acquisition executives have proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Such qualifications apply to the ASD (NII)/DOD CIO and Service and agency CIOs as well.

The USD (AT&L) must work with Service and agency acquisition executives to improve the capabilities and selection process for program executive officers and program managers.

The USD (AT&L) shall direct the Defense Acquisition University (DAU), in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

The DAU must staff with faculty knowledgeable and capable in contemporary product development management and acquisition practices versus individuals trained in only the old system.

Bottom Line Regarding IT Acquisition

The bottom line is that the inability to effectively acquire IT systems is critical to national security. Today the United States has the most capable fielded war fighting systems in the world. Information technology is critical to a wide range of capabilities: command and control, decision systems, precision weapons, and situation awareness. The task force found that performance of the Department's current IT acquisition process is not acceptable. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future.

For information technology, actions in the four areas discussed above—acquisition policies and process, roles and responsibilities of the CIO, milestone decision authority roles and responsibilities, and acquisition leadership expertise—will improve the acquisition of information technology in DOD. But caution is offered that emphasis and focus only on the acquisition process is not enough. While a new process is needed that better takes into consideration the unique aspects of information technology, process improvements alone will not yield success. If the

matters associated with responsibilities and authorities, organization, and expertise are not also addressed, the new process proposed here is likely to meet with the same outcomes as process improvements recommended by other groups who have studied this issue. This set of recommendations is designed to both streamline the IT acquisition process and address the fundamental problems that exist in the system today.

Overall Conclusion

Even if all the recommendations put forth in this testimony are implemented, it is recognized that unanticipated problems will arise during the course of any acquisition or product development managed by experienced and well intentioned people. The only way to minimize the unintended and potentially disastrous consequences of such problems is to quickly recognize and deal with them. If the culture is to use problems as a stick to punish people, then issues will not likely be brought to the forefront in a timely manner and the problems that follow will escalate. DOD acquisition programs are executed on an open stage—creating a difficult job for the best leaders. It is critical that all stakeholders align to deliver our best national security potential.

As has been mentioned, there is no "silver bullet" to fixing defense acquisition. But, in the view of the DSB, the Department can improve its acquisition processes—with the Secretary of Defense in the lead, supported by Congress. The Department must focus on four key areas:

1. **Buying the right things**
2. **Selecting an effective leadership team**
3. **Reforming and streamlining the acquisition process**
4. **Improving acquisition execution**

All of these elements are essential, none can achieve results alone. With a growing deficit, rising costs, and declining output, it really is not an option to let the status quo continue. Fixing acquisition is a national security issue. We do not want to find ourselves wringing our hands over the state of our national security because we chose not to act.