Report of the
Defense Science Board
Task Force on

Department of Defense Policies and Procedures for the Acquisition of Information Technology

March 2009

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology completed its information gathering in December 2008.

This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR: Under Secretary of Defense for Acquisition, Technology and Logistics

SUBJECT: Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology

I am pleased to forward the final report of the Defense Science Board Task Force on Department of Defense (DoD) Policies and Procedures for the Acquisition of Information Technology (IT). This report examines the challenges facing the Department of Defense in acquiring information technology and offers recommendations to improve current circumstances.

The fundamental problem DoD faces is that the deliberate process through which weapon systems and information technology are acquired does not match the speed at which new IT capabilities are being introduced in today's information age. Consequently, the principal recommendation of the study is that the Department needs a new acquisition system for information technology. Roles and responsibilities for those involved in the acquisition process must be clarified and strengthened and the IT system acquisition skills required in the workforce must also be strengthened.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

William Schneider, Jr.
DSB Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology

The importance of information technology (IT) to U.S. military capability is widespread. It enables nearly all of the nation's military combat capability and has become a necessary element of our most critical warfare systems. Yet, there is growing concern within Congress and among Department of Defense leadership that the nation's military advantage may be eroding.

At the request of Congress, this task force undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The broad scope of the study touched on acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to IT acquisition.

The primary conclusion of the task force is that the conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many IT systems that require continuous changes and upgrades. Thus the task force believes that there is a need for a unique acquisition system for information technology. The task force offers the following recommendations to change the Department's approach to information technology acquisition.

- **Acquisition policies**. A new acquisition process for information technology should be developed—modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. The process should be agile and geared to delivering meaningful increments of capability in approximately 18 months or less—increments that are prioritized based on need and technical readiness.

- **Roles and responsibilities of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO).** The ASD (NII)/DOD CIO should have strong authorities and responsibilities for enterprise-wide information policy vision, architecture, infrastructure, metadata

and other standards, spectrum, interoperability, information assurance, and system engineering. Some capabilities must be strengthened in order to effectively execute these responsibilities—in particular, system engineering, information assurance, and network integration.

- **Acquisition authorities and organization.** Acquisition authority and expertise in OSD is currently spread across several organizations, resulting in a lack of enterprise-wide architecture and coordination. Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization, those elements of the ASD (NII)/DOD CIO and Business Transformation Agency organizations responsible for IT acquisition oversight. (We note that there was not a consensus within the task force concerning this recommendation; a dissenting view is included in appendix A.)

- **Acquisition expertise.** Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Acquisition leaders need proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Similarly, program managers and program executive officers need track records of proven success.

The inability to effectively acquire information technology systems is critical to national security. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future. The development of a new acquisition process, coupled with clear roles and responsibilities of key decision makers, and an experienced leadership and workforce, are important elements of the solution.

Dr. Ronald Kerber
Co-Chair

Mr. Vincent Vitto
Co-Chair

Table of Contents

Executive Summary vii

Chapter 1. Introduction 1
Chapter 2. The Information Technology Environment 6
Chapter 3. A Framework for Information Technology Acquisition 25
Chapter 4. Existing Defense Acquisition Process 29
Chapter 5. IT Acquisition Challenges and Issues 35
Chapter 6. A New Acquisition Process for Information Technology 47
Chapter 7. Summary and Recommendations 60

Appendix A. Dissent to Report 69

Terms of Reference and Legislative Directive 71
Task Force Membership 79
Presentations to the Task Force 81
Glossary 85

Executive Summary

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 Department of Defense (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 DOD's ability to field advantageous information technology in a timely and cost-effective manner.

Since the original Goldwater-Nichols legislation, DOD has made several attempts to revise acquisition policy with the hope that such changes would shorten acquisition cycle time. 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, IT 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 (DSB) undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The findings and recommendations presented in this report 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 IT acquisition.

More specifically, the terms of reference directed that the matters addressed by the task force include the following: 1) DOD policies and procedures for acquiring information technology, 2) roles and responsibilities in implementing policies and procedures, 3) application of acquisition policies and procedures to IT that is integral to critical weapons or weapon system, 4) legal requirements (U.S. Code) as they relate to the acquisition of IT, 5) DOD policies and procedures to facilitate the use of commercial information technology, 6) suitability of DOD acquisition regulations, 7) adequacy and transparency of metrics, 8) effectiveness of existing statutory and regulatory reporting requirements, 9) adequacy of operational and development test resources, and 10) appropriate policies and procedures for technology assessment, development, and operational testing.

Based on the expertise of the task force members and information briefings received during the course of its deliberations, **the task force believes that there is a need for a unique acquisition process 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 our war fighters. The 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 IT, 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 task force offers 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 5000.2) 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 USD (AT&L) should lead an effort, in conjunction with the Vice Chairman, Joint Chiefs of Staff, to develop new, streamlined, and agile capabilities (requirements) development and acquisition processes and associated policies for information technology programs.

The task force proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities (Figure EX-1). The process is agile, 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), 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.

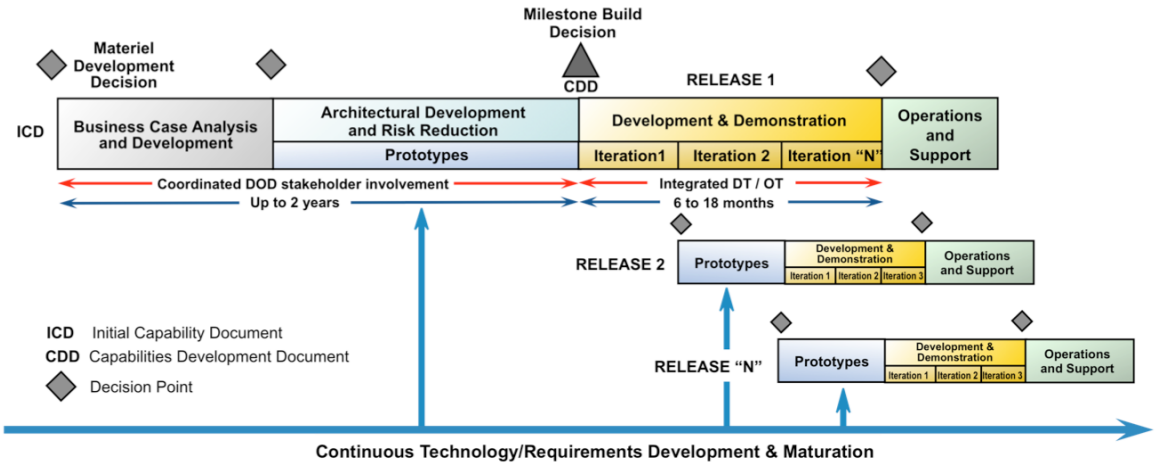


Figure EX-1. A New Acquisition Process for Information Technology

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational testing 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, 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.

The task force believes that 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 EX-2). IT is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

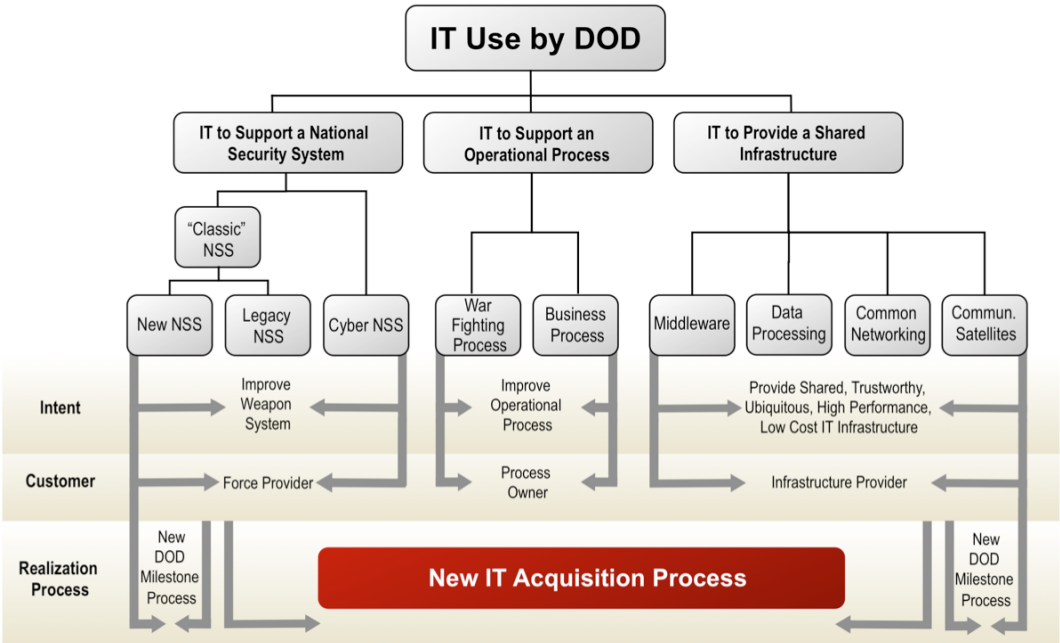


Figure EX-2. An Information Technology Acquisition Framework

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 trade-offs for hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in a 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 IT 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 IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the IT technology could otherwise be a few generations old when the system is fielded.

While one could argue that this required new decision could add confusion to the process, 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 the task force believes 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.

However, the task force believes that some of the functions delineated above need to be strengthened in order to ensure that the full responsibilities of the office can be effectively executed.

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, metadata 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.

While not the centerpiece of this report, the task force believes that information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. IT 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 not only undermine 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 operate with degraded systems.

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 to the task force, 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 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 (MDAP), major automated information systems (MAIS), 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. 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 Executive (USD (AT&L)) and the component 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, in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

Conclusion

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.

The task force believes that 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 the task force feels that a new process is needed that better takes

into consideration the unique aspects of information technology, it 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.

Chapter 1. Introduction

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 Department of Defense (DOD) leadership that the nation's military capability 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. For purposes of clarity, IT, as defined in this report, is any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing, or communicating information or data. DOD has a very long definition of IT which is too complicated to be useful.

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, acquisition decision-making 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. 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.

According to the Defense Science Board 2006 Summer Study on Information Management for Net Centric Operations, information management in Iraq and Afghanistan was a principal concern among war fighters. Significant ad hoc activity was taking place, especially at the tactical level, to gain desired capability. To counter the interoperability problem, many approaches were used to move information from one stove-pipe to another. Especially important, according to the 2006 report, was that much of the military capability used to support the conflicts was paid with supplemental funding—programs that were not part of the Department's planned capability. This circumstance reflects the fact that the need for such programs could not be predicted during previous core

program and budget planning, and the system was not sufficiently agile to react once the need was apparent.

Yet, despite these myriad obstacles, successful programs exist that are comprised 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.

Since the original Goldwater-Nichols legislation, DOD has made several attempts to revise acquisition policy with the hope that such changes would shorten acquisition cycle time. 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 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 acquisition model for information technology 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 (DSB) undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The task force offers recommendations to change the Department's approach to acquiring information technologies. The findings and recommendations 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 IT acquisition.[1]

More specifically, the terms of reference directed that the matters addressed by the task force include the following:

1. **DOD policies and procedures for acquiring information technology**, to include national security systems, major automated information systems, business information systems, and other information technology.
2. **Roles and responsibilities in implementing policies and procedures of the**:
   - Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L))
   - DOD Chief Information Officer
   - Director of the Business Transformation Agency
   - service acquisition executives
   - Chief Information Officer of the military departments
   - defense agency acquisition officials
   - information officers of the defense agencies
   - Director, Operational Test and Evaluation and heads of the operational test and evaluation organizations of the military departments and the defense agencies
3. **Application of such policies and procedures to** information technologies that are an integral part of **critical weapons or weapon systems.**
4. **Requirements of subtitle III of title 40, U.S.C. and chapter 35 of title 44, U.S.C.** regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.

---

1. Acquisition programs under authority of the Under Secretary of Defense for Intelligence are outside the scope of this study.

5. **Department of Defense policies and procedures for maximizing the usage of commercial information technology** while ensuring the security of the microelectronics, software, and networks of the Department.
6. **Suitability of DOD acquisition regulations**, including DODD 5000.1, DODI 5000.2, and accompanying milestones, to the acquisition of IT systems.
7. **Adequacy and transparency of metrics** used by DOD for acquiring IT systems.
8. **Effectiveness of existing statutory and regulatory reporting requirements** for acquisition of IT systems.
9. **Adequacy of operational and development test resources** (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of IT systems both during development and before operational use.
10. **Appropriate policies and procedures for technology assessment, development, and operational testing** for purposes of adopting commercial technologies into IT systems.

Based on the expertise of the task force members and information briefings received during the course of its deliberations, **the task force believes 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 our war fighters.

The issues associated with the acquisition of IT systems are a subset of similar problems the Department faces in acquiring major weapon systems, most of which have a high content of embedded IT. A common theme to all is that continuous changes and upgrades are a reality and must be accommodated—a reality driven by the short half-life of commercial IT technology, supportability of hardware (which is often a commodity), software applications, and operational requirements. **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**. Many existing programs are exceeding cost and schedule baselines, which cannot continue unabated. While the task force recognizes that there is no "one-size-fits-all" solution to DOD's acquisition

problems, it also believes there is merit in minimizing the number of specialized acquisition approaches. That said acquisition of information technology represents a case that must be addressed with a process that focuses on the unique characteristics IT represents.

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 defense systems in the world, and information technology is critical to these capabilities—to command and control, decision systems, precision weapons, and situation awareness. Spending on IT is rapidly growing in both embedded and stand-alone systems. As well, IT system acquisition and IT upgrades to existing weapon systems represent a significant and growing percentage of current acquisitions. Further, inadequate attention to cyber security in the acquisition process is an Achilles heel that can be actively exploited by our adversaries. While this report does not address cyber security in any detail, it does highlight the need to keep this critical issue in mind both during IT acquisition and through operational procedures in the field. These many challenges surrounding information technology must be addressed if DOD is to maintain our national security objectives as a military leader in the future.

The chapters that follow detail the work of the task force, leading up to a set of actions for DOD. Chapter 2 begins with an overview of the information technology environment, followed in Chapter 3 by a framework for evaluating IT acquisition. Chapters 4 and 5 focus on the existing acquisition system and the problems that arise with the acquisition of IT programs. Chapter 6 proposes a new acquisition process for information technology. The report concludes in the final chapter with key findings and recommendations.

Chapter 2. The Information Technology Environment

Information technology is pervasive throughout DOD systems, from infrastructure to business systems to IT embedded in weapon systems. Whereas in 1970 software accounted for about 20 percent of weapon system functionality, by 2000 it accounted for as much as 80 percent[2] and today can deliver 90 percent[3] or more of a system's functionality. While its importance is growing, the information technology environment is experiencing a disturbing set of trends (Figure 1).

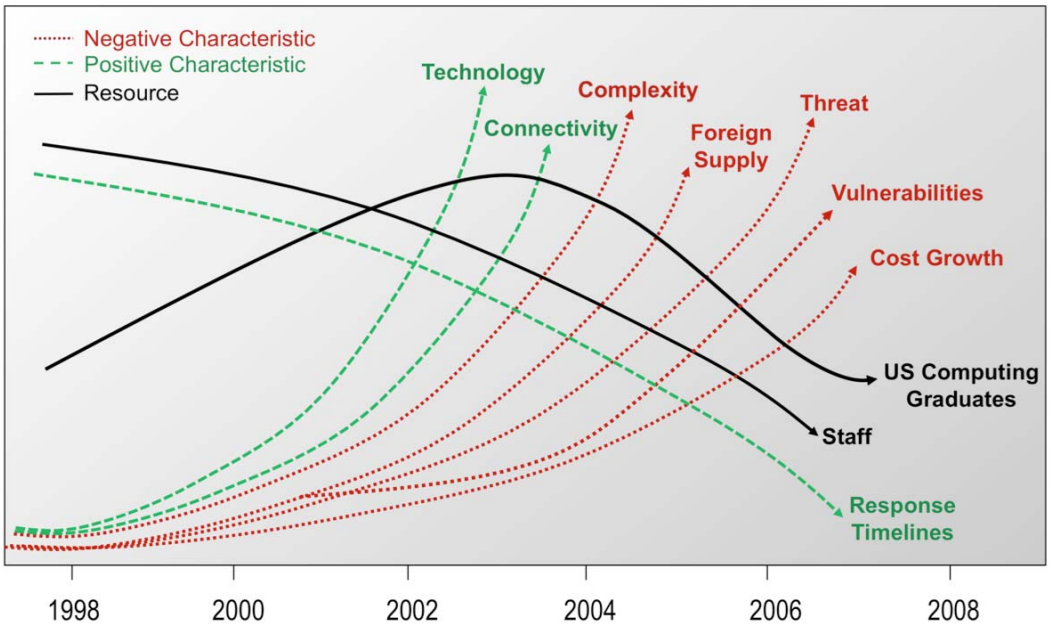


Figure 1. The Perfect IT Storm

2. Defense Science Board Task Force on Defense Software. November 2000.
3. *Program Manager's Guide for Managing Software*, October 10, 2001, Rev 2.0 https://acc.dau.mil/CommunityBrowser.aspx?id=24374&lang=en-US

These trends include an increase in IT complexity, foreign supply, vulnerabilities, threats, and cost with a concomitant reduction in the supply of U.S. computing graduates and qualified expert government staff. Simultaneously, the rate of technology change is increasing as is the interconnected nature of systems, while timelines are shrinking—circumstances that pose both a benefit and risk to DOD. Each of these key trends and their implications is detailed in the remainder of this chapter.

Technology Change

Information technology—from hardware to software to complex systems—continues to rapidly advance. Computer hardware rapidly evolved from vacuum tubes to transistors to nanotechnology. In his 1965 paper, Intel co-founder Gordon E. Moore predicted that the number of transistors on an integrated circuit board would increase "at a rate of roughly a factor of two per year." In 1975, Moore refined his projection to a doubling every two years. Still known as Moore's Law (Figure 2), this exponential growth has held for processing speed, memory capacity, and even the number and size of pixels in digital cameras.[4] While Moore's Law has held for decades, processing speed is no longer increasing at this rate. Instead the industry has moved to a multi-core approach. Unfortunately, parallel processing software has lagged behind. This will be an important trend for DOD to monitor and understand.

In addition to changes in hardware, IT architectures have evolved over the past several decades from isolated computing systems of the 1960s; to networked stovepipes in the 1970s and 1980s; to the use of message passing middleware to glue together mission applications in the 1990s; to the open, service-oriented architectures (SOA) of today (Figure 3). SOA is a method for organizing, exposing, and utilizing distributed capabilities that may be under the control of different ownership domains. This evolution toward the disaggregation of systems into distributed services promises more rapid development, reuse, and survivability, yet at the same time increases interdependencies, vulnerabilities, and complexity (and possibly impacts performance). The impact of this evolution is underestimated. It will allow substantial change in the nature and substance of IT acquisitions by further enabling the rapid development and fielding of small increments of capability.

---

4. Dale W. Jorgenson and Charles W. Wessner. 2006. (eds). *Measuring and Sustaining the New Economy, Software, Growth, and the Future of the U.S Economy*: *Report of a Symposium*. National Research Council. Figure 1, p. 6. www.nap.edu/catalog/11587.html

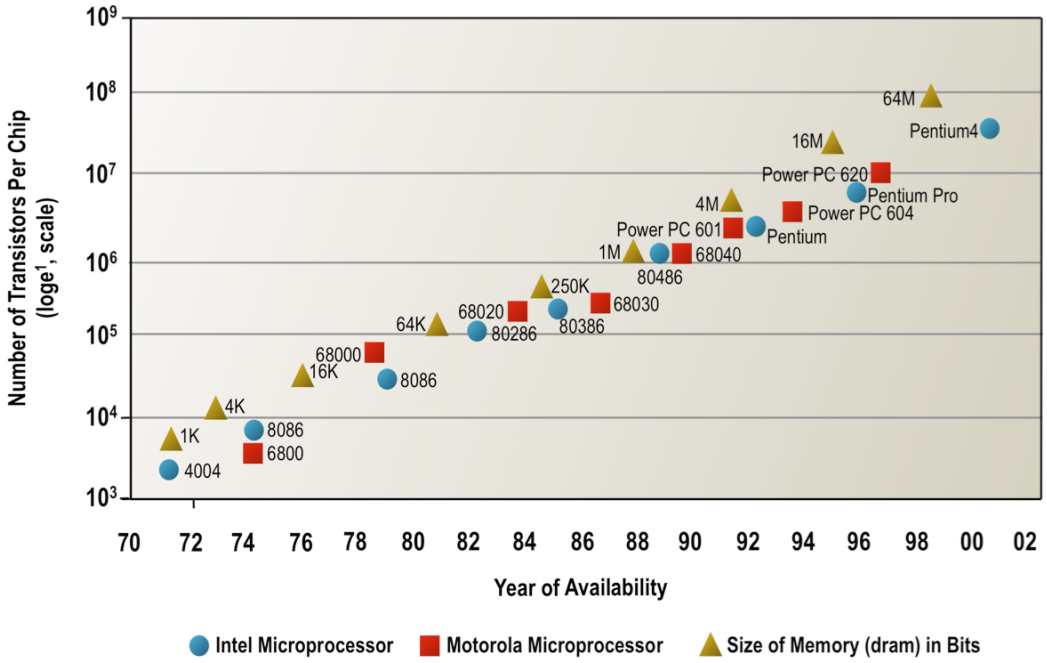


Figure 2. Moore's Law: Transistor Density on Microprocessor and Memory Chips

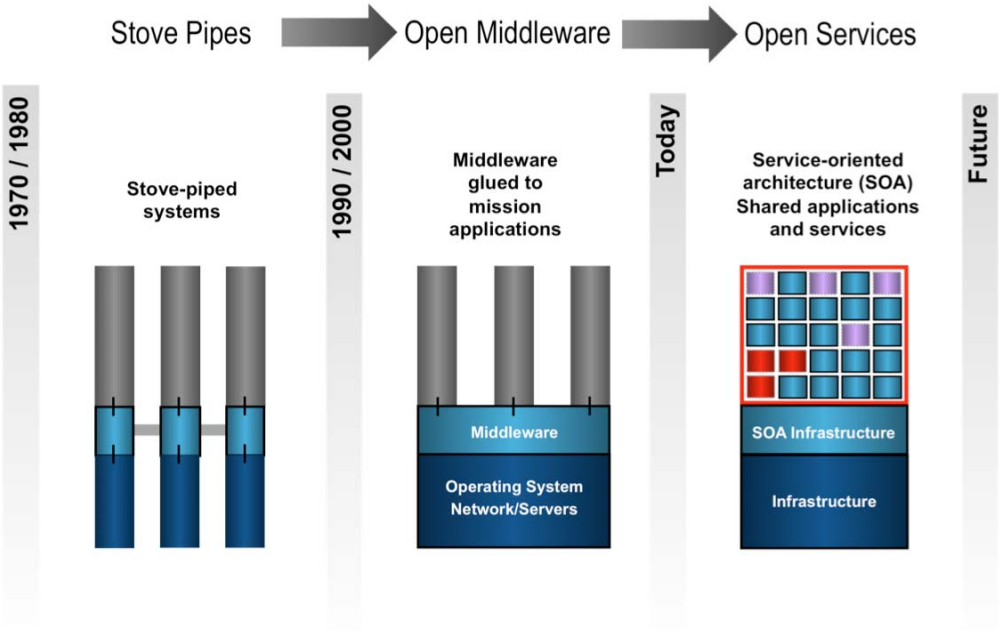


Figure 3. Evolution of Information Technology Architectures

While initial attempts to expose and standardize large amounts of data and metadata about legacy systems have proved highly complex and time intensive, one method that has successfully emerged is known as "loose coupling" in which minimal but critical data interfaces are exposed to support interoperability. For example, Cursor on Target,[5] a machine-to-machine language designed to communicate battlefield information, enables rapid but minimal integration of a few crucial data elements (e.g., position, time, object, event) across legacy systems. In summary, technology will continue to rapidly evolve, imposing challenges for personnel and programs to remain current.

Disaggregated Architectures

DOD's IT vision includes one very special feature—the separation of data from services and applications. This separation provides two high-priority benefits.

- It supports the introduction of new applications and/or services without requiring a lengthy, expensive N-squared, application-to-application integration.
- It enables operators to discover, use, publish, and govern data in ways that were not planned or anticipated on an operational, as-needed basis.

While the introduction of disaggregated architectures and the separation of data from applications and services will provide significant benefits to the Department in both development and operations, the planned outcome is a very different environment. Reaping these benefits will require rethinking and modifying the Department's processes.

From an architecture perspective, it is likely that the disaggregated model will not directly support all of the Department's low latency requirements in the near-term. The solution to this appears to be relatively straightforward. Simply allow low latency applications to receive data on a "push" rather than a "pull" basis, while at the same time, require the data sources to post their data in parallel for other uses/users. This approach will require: 1) development of the criteria for deciding which systems have such stringent low latency requirements (e.g., fire control systems) that they will be allowed to obtain data on a "push" basis, and

5. Miller, R. and Winkowski, D. *Loose Couplers as an Information Design Strategy*. www.ffrdc.org/work/tech_papers/tech_papers_07/07_0802/07_0802.pdf

2) sorting out which systems are expected to provide data for use by these same systems.

This solution is not ideal for this set of systems, as it will not provide all of the benefits of a disaggregated environment where data is separated from applications, services, and governance. It is also clear that not all of the information security requirements will be addressed by the IT infrastructure; some of these requirements must be addressed within the mission applications or services. While this should not be a surprise, it is worth noting since the goal is to have as many of the enterprise functions performed by the infrastructure as possible, in order to facilitate the introduction of new applications and services.

There are also some implications from acquisition and implementation perspectives. While there are significant benefits to being able to implement new applications and services quickly, the acquisition process will need to support these quick turn efforts more easily than it does today (which will be discussed in more detail in later chapters of this report). To deliver acceptable quality of service and to support the information and the network security required by DOD in an enterprise-wide SOA, with enterprise-wide access to data by authorized users, a well engineered and governed enterprise IT infrastructure is essential.

However, creating an enterprise infrastructure is not trivial. Transitioning from the existing platform/system and occasionally enclave-based environment, to an enterprise IT infrastructure will put additional stress on the Department, especially on the technical management and acquisition process. For example, the test process will have to change to allow DOD to speed application and service implementations. At the same time there will be differences for the test function, as tests must be performed on both the infrastructure and on the individual applications/services. Both are required to deliver capabilities, but the test timelines should be very different.

There will also be funding challenges. The Department's three core processes—requirements, acquisition, and resourcing—are just starting to move from platforms to capabilities, although the focus on individual capability delivery increments still dominates. Adoption of a service-oriented architecture and institutionalization of an enterprise-wide IT environment will require a significant investment in the infrastructure itself. The good news is that implementation can be segmented over time and purpose. Individual applications

and services that will ultimately rely on the infrastructure must trust that it will be successfully funded and developed.

Two additional matters relate to funding this "common good." One is the need to expose and maintain data for unanticipated users, which is necessary to avoid an erosion of confidence in the enterprise-wide environment. A second is that building and delivering a reusable service clearly provides a cost benefit if the service is reused, but can require additional funds for the developer that must increase support for unplanned users from other parts of the organization.

Connectivity

Just as we are experiencing rapid technology change, we are also facing rapid global increases in connectivity among computers and, consequently, among people. There are already nearly one and one half billion Internet users. By 2012, one quarter of the world population will have regular access to the Internet.[6] Brazil, Russia, India, and China are experiencing some of the highest growth rates.

More important than growth in the raw numbers of users is the belief that their collective power increases exponentially with the number of nodes. Robert Metcalf, founder of 3Com Corporation, noted that the value or utility of a network is equal to the square of the number of nodes (e.g., the number of connected individuals)—the so called Metcalf's Law (Figure 4). Whether the value grows as Metclaf's law, as n(log(n)) as some researchers now believe, or as Reed's law, which states that it grows faster due to forming communities of interest as is beginning in DOD, is not as important to understand as the fact that the value is growing in a highly nonlinear way with respect to size.

The Department of Defense has recognized and capitalized on the potential of net centricity. The Global Information Grid (GIG) is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand for the Department of Defense. As of 2008, the GIG incorporated 21 satellite communications networks; 65 nations; over 3,500 bases/posts; approximately 15,000 networks; thousands of applications; 120,000 commercial telecommunications circuits; and 7 million DOD computers (twice

6. Sehgal, V. June 3, 2008. *Concept Report*. Worldwide Online Population Forecast, 2007 to 2012. JupiterResearch.

as many as in 2005). While the size and ubiquity of this ever growing enterprise is a challenge in itself, additional IT functionality and increased cross-organization, coalition, and security boundary connectivity further exacerbates the enterprise challenge.

Most importantly, but easily overlooked, is that achieving "the power of networks" requires the elements of the network to be constructed according to widely accepted and adopted standards, and executed in accordance with an overarching network architecture concept and design. Chaotic creation of "networks" and/or "network nodes" will not yield the benefits promised by Metcalf's Law. The underlying proposition is that adoption of standards increases the ability to "connect," which gives encouragement to increase the number of connectors. In turn, this enables an increase in the information exchanged as well as the utility and value of information exchanged within and among the network(s).

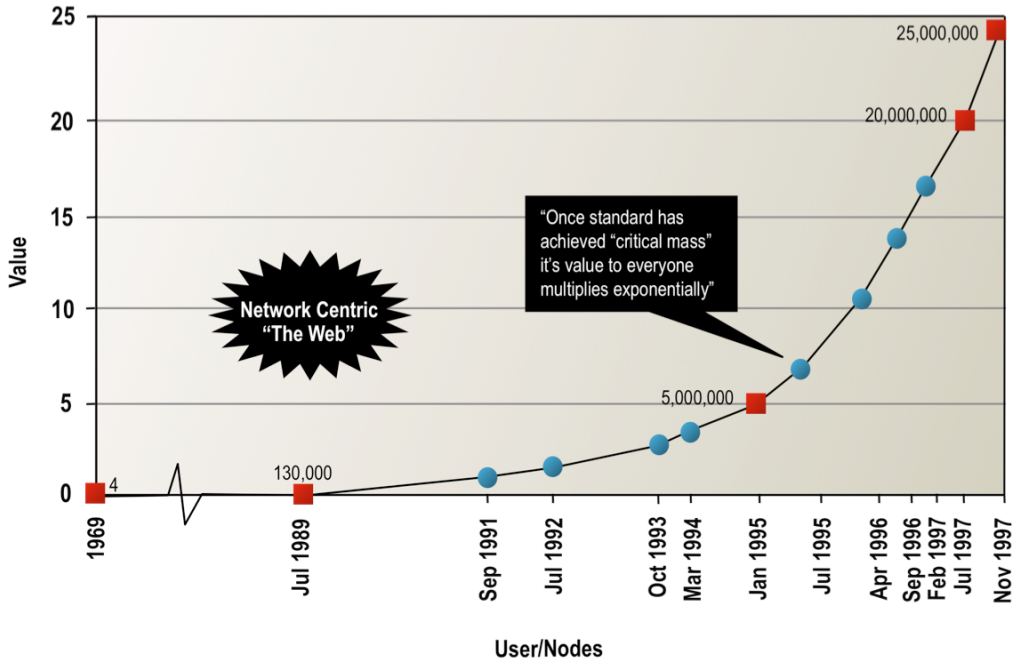


Figure 4. Metcalf's Law: The Power of a Network

Size and Complexity

While the sheer number of nodes (computers, routers, business systems, weapon systems) and connections among nodes in the GIG is increasing dramatically, the underlying software code base is growing, driving complexity of design, operation, protection, and maintenance. This is occurring both in infrastructure software, as well as in weapon systems software. For example, the most ubiquitous commercial operating system (Microsoft Windows) has grown from thousands of lines of code (LOC) to tens of millions (left graphic below)[7] and popular open source operating systems (e.g., Debian) (right graphic below)[8] have similarly grown rapidly (Figure 5).

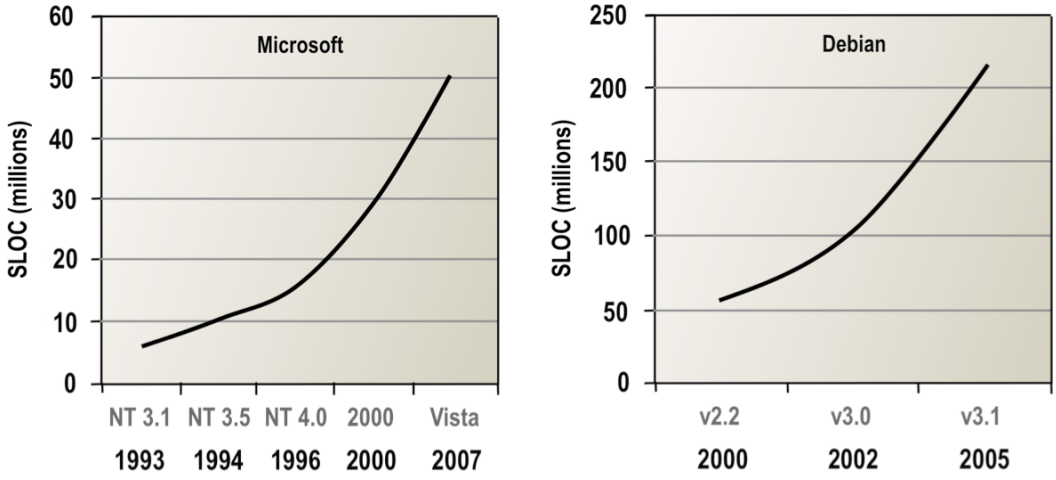


Figure 5. Source Lines of Code (SLOC) for Windows and Debian Operating Systems

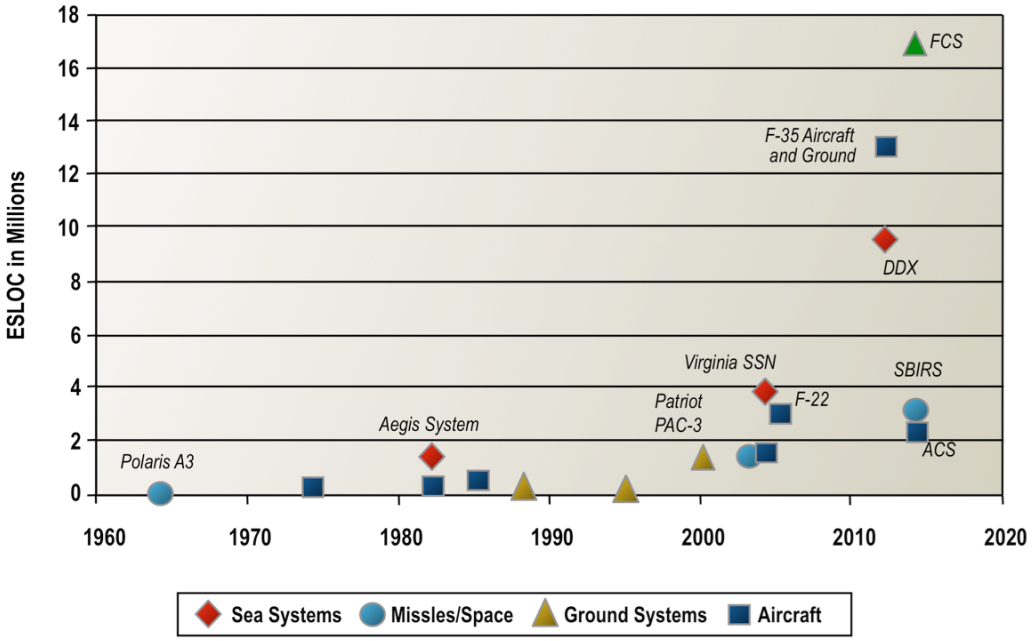
Figure 5 also implies that DOD's total life cycle expenditures for software maintenance could grow, perhaps at a similarly exponential rate. Even more interesting, is that annual cost of maintaining the Department's software-enabled capabilities could not only rise exponentially but, where the capability is enabled by open-source software, could increase by ten times the cost of similar

7. "How Many Lines of Code in Windows?" Knowing.NET, December 6, 2005. See also Richard MacManus. 28 March 2006. "Measuring Source Lines Of Code (SLOC)—there are bigger birds than Microsoft's albatross" http://blogs.zdnet.com/web2explorer/?p=148.
8. en.wikipedia.org/wiki/Source_lines_of_code

capability provided by the established and structured commercial software industry. This conclusion assumes that the cost of maintaining a single line of code is relatively constant over time and the maintenance cost (per SLOC) is the same for both commercial off-the-shelf and open source software. Clearly, the Department will have to develop a strategy to control this growth in a reasonable and practical way. That the majority of commercial code, such as for example Microsoft Windows, has grown exponentially while the cost has been nearly constant and has not tracked the lines-of-code metric, gives an even more compelling reason for DOD to develop standards and processes to use and acquire as much commercial-based code as possible.

Software has spread well beyond defense infrastructure into the very heart of weapon systems. For example, thousands of microprocessors, linear electric drive controllers, dynamic sensors, and millions of lines of sophisticated code enable the startling capabilities of the F-22 and Joint Strike Fighter, as well as quantum increases in the sensitivity achieved using pre-existing sensors. Several years ago a handheld grenade launcher was created with smart projectiles guided by 2,000 lines of code.[9] Moreover, the software code base within mission systems is growing rapidly from generation to generation. The executable source lines of code (ESLOC) within weapon systems, such as missiles, ships, and aircraft have grown from a few thousand to tens of millions (Figure 6). For example, the 1.8 million LOC basis for the Navy's DDG 1000 is growing over 36 percent to 5 million LOC in the evolution to the Aegis 7.1R baseline.[10] In addition, the FA-18 with approximately 10 million LOC is growing to over 15 million in the Joint Strike Fighter.

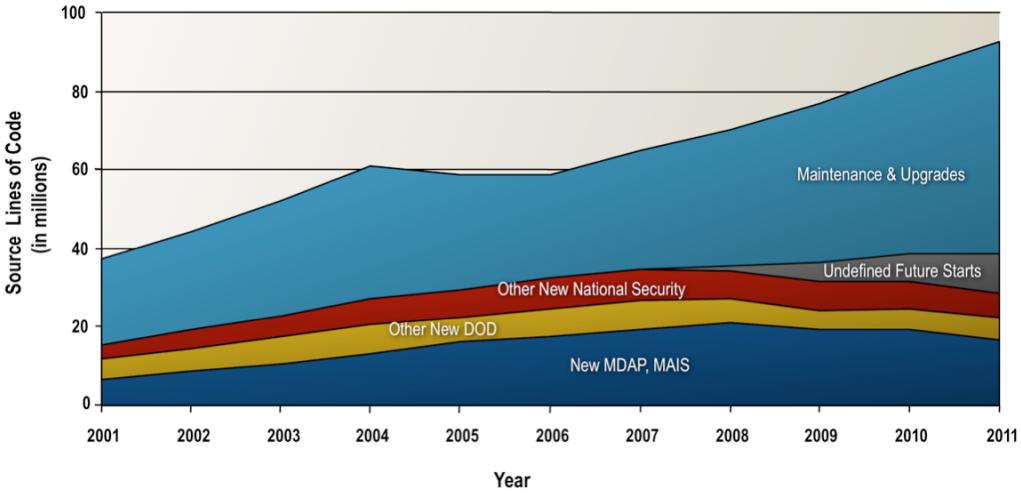
9. "Defense IT Official Says Talk on Software Quality is Cheap," *Government Computer News*, May 7, 2001 (mobile.gcn.com/articles/vol20_no10a/4167-1.html).
10. *Software Intensive Systems*, July 2006, Naval Research Advisory Committee Report, NRAC 06-03.



Sources: CARD Data, SEI, CSIS Analysis

Figure 6. Executable Source Lines of Code within Classic Weapon Systems

Because threats and capabilities change over time, it is expected that the Department's systems will require a continuing series of upgrades and technology refreshment. These costs can be substantial. The growth of SLOC of new MDAP and MAIS systems, and the SLOC for systems maintenance and upgrades are one example. Figure 7 depicts how code required for sustainment matches or exceeds those for new development. The figure also suggests that out-year budgets required to maintain and upgrade existing code will be substantial. The task force believes this to be a realistic projection for the tightly coupled code, which inhabits most existing DOD systems. However, this trend may not be inevitable. Open architectures, open standards, and service-oriented architectures, because of their mobile nature, appear to have the potential to dampen the projected rise in the cost of maintaining and upgrading software-based capabilities.



Source: CARD data, Federal Procurement Database System, QSM, CSIS Analysis

Figure 7. Estimated Source Lines of Code for the National Security Community

ESLOC is a valuable and intuitive measure that is correlated with the number of people required to build, use, and maintain software systems.[11] However, dimensions beyond size can significantly increase the complexity of IT systems. For example, Boehm and Lane (2006)[12] describe how software intensive systems of systems (SISOS) "integrate multiple, independently developed systems" and "are very large, dynamically evolving, and unprecedented with emergent requirements and behaviors, and complex socio-technical issues to address." SISOS are characterized by 10–100 million LOC; 30–300 external interfaces; 2–200 suppliers; 6–12 hierarchical levels of suppliers (primes and subs) and 20–200 coordination groups (or integrated product teams).

Boehm and Lane argue for a risk-driven spiral development model that addresses the acquisition challenges of many systems, many supplier levels, and many increments where rapid fielding, high assurance, and evolution are essential for success. They point out successful continuous independent verification and validation practices found in the continuous build practices at Microsoft[13] and in

11. Booch, G., 2008. "Measuring Architectural Complexity." *IEEE Software*.
12. Boehm, B. and Lane, J. A. May, 2006. "21st Century Processes for Acquiring 21st Century Software-Intensive Systems of Systems." *CrossTalk: The Journal of Defense Software Engineering*. www.stsc.hill.af.mil/crosstalk/2006/05/0605boehmlane.html.
13. Cusumano, M., and R. Selby. *Microsoft Secrets*. Harper Collins, 1996.

agile methods[14] as well as the use of anchor point milestones and evolutionary development in the Rational Unified Process.[15]

Vulnerability

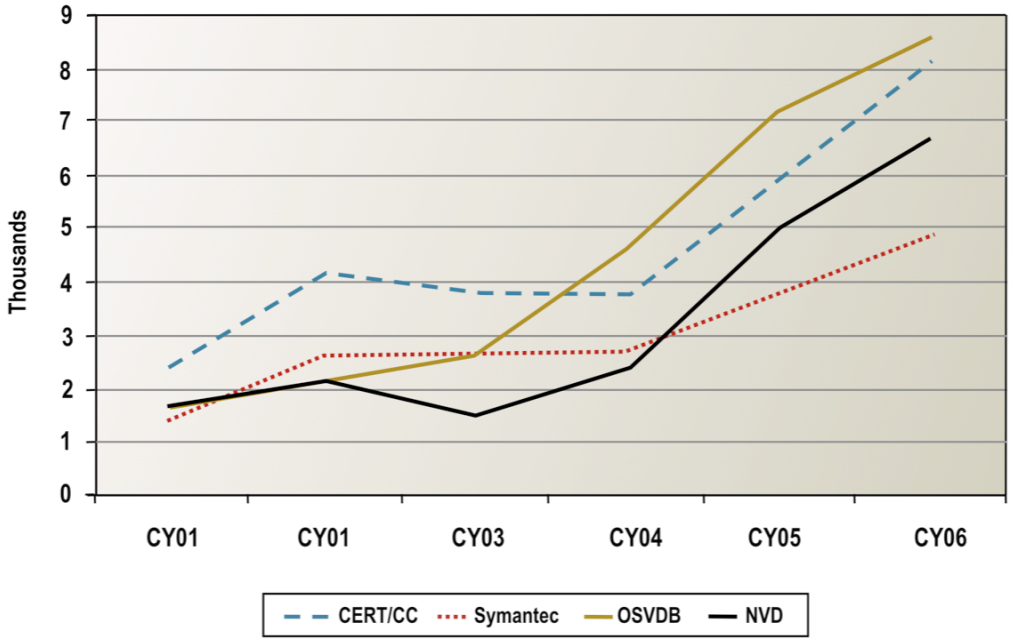
Increasing amounts of ESLOC increases the likelihood of vulnerabilities. The Common Vulnerabilities Enumeration (CVE) site (cve.mitre.org) in October of 2008 was reporting 19 new vulnerabilities each day. The number of vulnerabilities captured in the National Vulnerability Database (nvd.nist.gov), which incorporates CVE, has risen nearly four-fold from a yearly rate of 1,700 in 2001 to 6,700 in 2007. As of October 2008, there were over 33,337 CVE vulnerabilities in the data base.

The latest available data from four vulnerability sources confirms the exponential growth trend in recent years (Figure 8). In short, more software means more vulnerability. Adversaries understand this. Thus, not only are vulnerabilities increasing, the threat is increasing as well. It is also more diverse, ranging from capable state actors to small, independent, non-state rogue actors, all of which can produce enormous consequences. According to one source, attack volume has increased from 50 to 5,000 per week. Adversary attacks have also increased in sophistication (e.g., from general phishing to individualized spear phishing based on intelligence). Similarly, the number of viruses rose from approximately 20,000 in 1998, to 50,000 by 2000, to over 1 million in 2008.

This growth in vulnerabilities cannot be ignored in defense systems. In reality, vulnerabilities cannot be completely eliminated; therefore it must be assumed that some vulnerability will always exist. *DOD must develop tactics, techniques, and procedures, and concepts of operations to operate with degraded systems.* Continual tests to validate system and subsystem integrity must also be performed.

---

14. Beck, K. *Extreme Programming Explained.* Addison-Wesley, 1999.
15. Rational, Inc. *Driving Better Business With Better Software Economics.* Rational Software Corp. 2001.



Source: Computer Emergency Response Team Coordination Center (CERT/CC), Symantec Vulnerability Database, Open-Source Vulnerability Database (OSVDB), and National Vulnerability Database (NVD)

Figure 8. Correlated Upward Trends in Vulnerabilities

Cost

Another unfavorable trend is the cost of IT acquisitions. While hardware costs tend to follow a predictable trend, pricing software is challenging for many reasons. Though duplication cost is low, service life is difficult to predict. Commercial software pricing is challenging, for example, because cost can be based on upgrades, stand-alones, or suites. In a study of operating system unit costs, while the average price grew about one percent a year in the 1990s, when normalized for the functionality actually provided (which typically increases over the years), unit costs actually declined between 6 and 16 percent per year.[16] Yet commercial software has become such a large cost and valuable investment that the Financial Accounting Standards Board no longer considers it an intangible

16. National Academies Press. 2006. *Measuring and Sustaining the New Economy*, Figure 5, p. 19. www.nap.edu/catalog/11587.html.

asset but rather a fixed asset (like property, plant, and equipment). Since 1998, even the design phase of software development can be capitalized.

The Government Accountability Office (GAO) reports that 48 percent of the federal government's major IT projects have been rebaselined at least twice.[17] A 2008 RAND study of cost growth in 35 weapon programs found that development cost growth is driven equally by cost-estimating errors and requirements growth, which account for almost two-thirds the total cost growth.[18]

Acquisitions may have different cost curves during their life cycles. A complex, advanced weapon system program with a very long development cycle and few production items could anticipate the bulk of the costs to be up front. However, for a weapon system program with a short development cycle and many production items (e.g., MRAP), the bulk of the costs would occur after Milestone C. For IT acquisitions, which are not development-intensive, costs are likely to be primarily after Milestone C, whereas for complex development systems with few production items, the bulk of the costs will end up being up front.

Up-front rigorous capability (requirements) definition and systems engineering has been demonstrated to be inversely correlated with cost growth. As illustrated across a range of NASA programs, performance improves when a significant fraction (up to 12 percent) of program cost is for effective systems architecture and engineering (Figure 9).[19] Acquisition experts cite flexibility to make informed trade-off decisions at the program level, as well as concentrating on manageably sized increments that deliver capabilities in shorter time frames, as essential elements of this success. Unfortunately, the initial requirements definition and trade-off phase is rarely performed with sufficient rigor.

---

17. *OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars*. July 2008. GAO-08-1051T. Washington, D.C.: Government Accountability Office.
18. Joseph G. Bolton, Robert S. Leonard, Mark V. Arena, Obaid Younossi, and Jerry M. Sollinger. 2008. *Sources of Weapon System Cost Growth: Analysis of 35 Major Defense Acquisition Programs*, Santa Monica, Calif: RAND Corporation. www.rand.org/pubs/monographs/2008/RAND_MG670.pdf.
19. Briefing on Alternative Acquisition Model, OSD (NII)/DOD CIO, DASD for C3ISR and IT Acquisition, Irvine, Calif., August 2008.

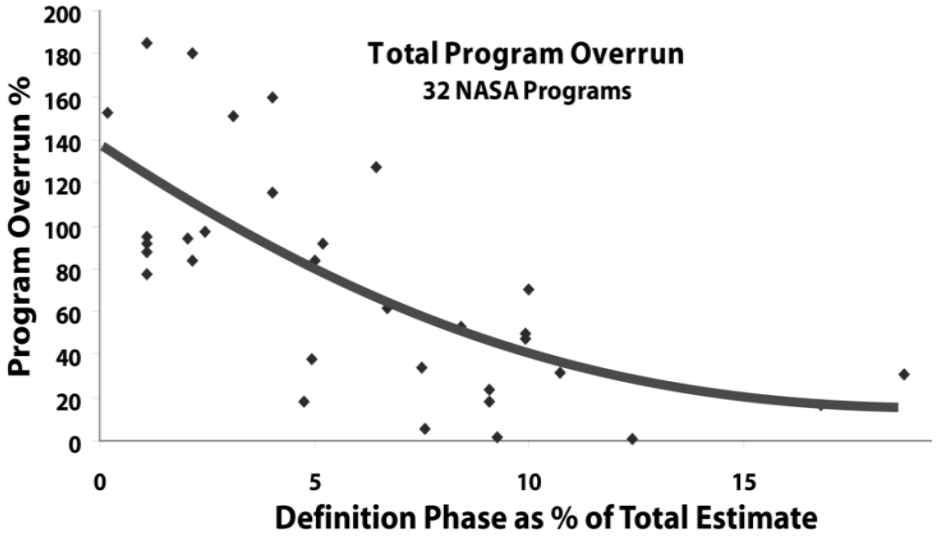


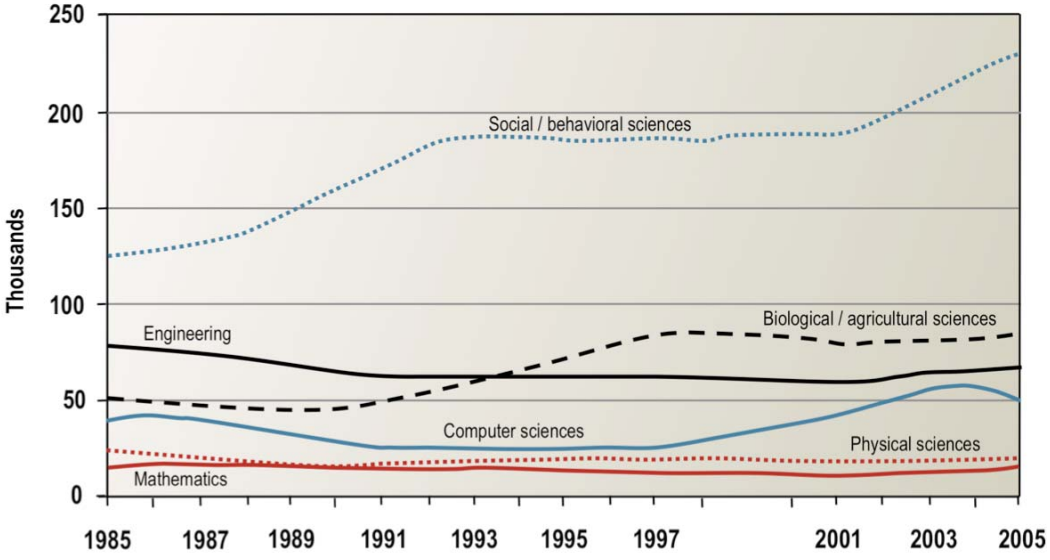
Figure 9. Rigorous Upfront Engineering Reduces Program Cost Overrun

Human Resources

The long-term supply of U.S. science and engineering students is worrisome and arguably a national security concern. Over the past decade, undergraduate engineering degrees in the United States, United Kingdom, Germany, and Japan have remained flat whereas South Korea's have risen significantly and China's have grown exponentially. While one can argue western schools are higher quality, quantity has a quality all its own. The number of doctorate degrees earned in China is growing exponentially—at a rate that could surpass the U.S. lead in annual production of doctorates in only a few years. Other countries, such as Germany, United Kingdom, Japan, and South Korea seem to be increasing the rate of their graduation of doctoral students at about the same rate as the United States. At the same time, the number of foreign students earning technical doctoral degrees in the United States has, for decades, been very high relative to U.S. citizens.

Not only is the raw amount of U.S. students at a global competitive disadvantage, but there is a growing gap between degrees earned in the social behavioral sciences as compared to engineering, computer science, and mathematics—one that favors social and behavioral science degrees (Figure 10). The Computing Research Association reports that after seven years of decline, the number of new computer science majors in 2007 was half of what it was in

2000.[20] Driven by declines in enrollment, the median graduates per computer science department dropped from 70 to 40 between 2004 and 2007.



Source: webcaspar.nsf.gov

Figure 10. Granted Bachelor Degrees in the United States

This decline in U.S. software talent is occurring in the face of increased demand. The gap between degreed professionals and job openings is growing, most notably in mathematics and computer science where only half the annual job openings can be satisfied by newly degreed students (Figure 11).[21] The latest data in the National Employment Matrix from the Bureau of Labor Statistics project 324,000 new computer software engineering jobs over the 2006 to 2016 period.[22] This 38 percent increase is much faster than the average for all occupations and one of the largest employment increases of any occupation.

20. www.cra.org/wp/index.php?p=139
21. As reported by Computer Research Association. www.cra.org/govaffairs/blog/projected_job_openings.pdf
22. www.bls.gov/oco/ocos267.htm#outlook

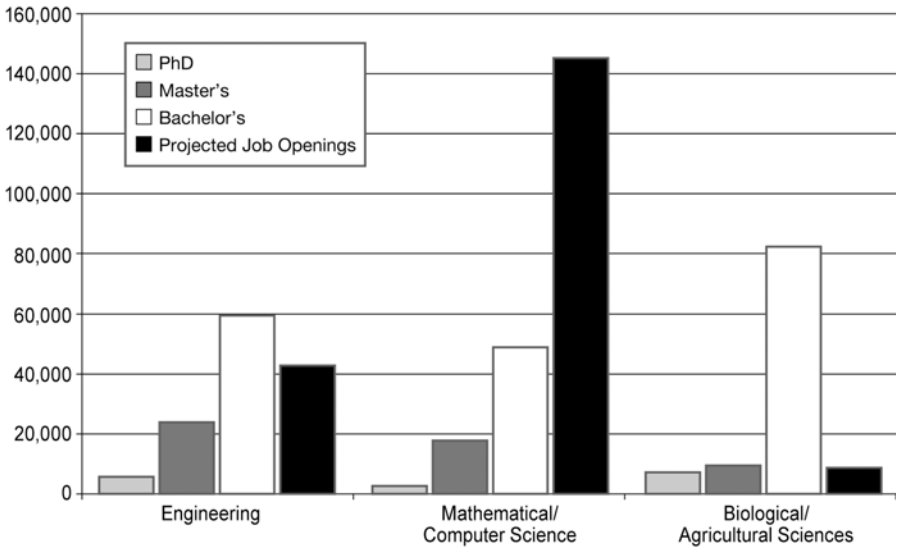


Figure 11. Annual Degrees and Job Openings, 2002–2012

To make matters worse, qualified IT systems designers, architects, and acquirers can take years to cultivate. Unfortunately, between 2002–2005, DOD experienced decreases in program managers (-5 percent), production engineers (-12 percent) and financial managers (-20 percent), whereas the test and evaluation workforce grew by 40 percent.[23] The result of the decline in experienced personnel, whether in government or industry, can be expensive rework, further increasing costs and exacerbating workforce challenges. (One GAO report cites as much as 40 percent rework in software acquisitions.)

Foreign Supply

At the same time that the supply of IT talent in the United States is declining, foreign sources of supply are rapidly growing, with notable increases in offshoring to India, Russia, and China. According to a 2007/2008 survey of 418 corporations, software and product development are the highest offshored functions, with over 70 percent of the software industry now offshoring.[24] Over the past ten years, India has

23. *Defense Acquisition Performance Assessment Report*, January 2006.
24. Lewin, A. and Heijmen, A. 2008. *Offshoring: An Intermediary Step to New Transformational Global Capabilities—Findings from the 2007-08 Offshoring Research Survey*. The Conference Board Strategic Outsourcing Webcast. Achieving the Next Evolution of Success. The survey also found that over 50 percent of companies are offshoring software development and over 30 percent new product development.

declined as the leading offshore product developer and many new specialized locations are emerging (e.g., the Middle East, Western and Eastern Europe, Latin America, Mexico, the Philippines and Russia) making supply chain analysis and risk mitigation increasingly distributed and more difficult.

Offshoring motivations are strong and include not only cost savings but growth, competitiveness, access to expertise, flexibility, and increasing speed-to-market. Service providers now aim to build capabilities to provide end-to-end business process re-engineering. Justifiably, there is increasing concern about our ability as a nation to ensure we can buy "trusted" components for our national security systems from an increasingly offshore supply chain. In 2007, a Defense Science Board task force that studied foreign influence on DOD software recommended that an intelligent risk management process is essential to ensuring a trusted supply chain, mitigate malicious attacks, enable efficient responses, and maintain trustworthiness in the software that support DOD's critical missions.[25]

Time

In addition to the challenge brought by the shortage of human expertise, the Department also faces the tyranny of time. Time scales are decreasing in two aspects. First, the pace of technology change puts pressure on acquisition time lines in order to ensure relevancy. Second, missions have evolved and are requiring increasingly more rapid response times. Conventional warfare decision cycles have shortened from days or hours to, in some cases, seconds. For example, cyber attacks on IT systems used to be lengthy, planned-out attacks, but now automated scanning, analysis, and global sharing of attack vectors enable attack cycles to occur in minutes and sometimes seconds. Unfortunately, the overall portfolio of DOD IT programs has experienced a 21-month delay in delivering initial operational capability to the war fighter, and 12 percent are more than four years late.[26]

---

25. *Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software*, 2007, Under Secretary of Defense for Acquisition, Technology, and Logistics. The task force also made recommendations in areas of procurements, intelligence, quality and security assurance, acquisition, research and development, and the national agenda. See also *Defense Science Board Task Force on High Performance Microchip Supply*, February 2005.
26. GAO-08-782, "Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment," June 3, 2008. p. 5.

Implications for Enterprise IT Acquisition

To be successful, future acquisition strategies must recognize and deal with the challenges outlined in this chapter. In particular, the growing dependence on information systems and commercial technology will mean increased

- cost whenever unique "requirements" are specified
- dependence on management of software-intensive programs
- reliance on a shared, common information infrastructure
- vulnerability with added functionality

Provisioning an information infrastructure of the scale, security, reliability, and functionality suitable for the Department of Defense is a challenge to software system design. Two principles, however, are proving effective in large-scale commercial situations:

- **Creation of a centralized governance (not program management) authority for enterprise oversight**. A successful information infrastructure—even one of the complexity of DOD's—must have a central locus for conceptual integrity. This locus should be disassociated from implementation, but have implementation visibility to identify non-compliant initiatives and problems with the conceptual framework.
- **Creation of an enterprise concept built of elements loosely coupled.** A commercial consensus is emerging regarding an approach to large-scale enterprise implementations that takes advantage of the agility afforded by incremental development approaches, economies of software reuse, and ubiquity of web-based commercial products. This approach (service-oriented architecture) is a methodology supported by an evolving set of open commercial standards. Loose data coupling, as exemplified by Cursor on Target, should also be practiced where appropriate.

  As with other large-system implementations, SOA partitions function using structured, well defined interfaces. Notably, the partitions are created in a way to support automated discovery, use, and reconfiguration over time. SOA also has special challenges for DOD. Standards, especially in the security domain, are still evolving. High-performance applications may not be well suited for the SOA approach. Nonetheless, the SOA approach, under the guidance of a centralized oversight authority, offers a way to move forward with incremental acquisitions while doing so in alignment with the Department's strategic goals.

Chapter 3. A Framework for Information Technology Acquisition

The term "information technology" covers a broad range of technologies, war fighting domains, mission applications, and "customers." For clarity we repeat the definition of IT, stated earlier, as any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing or communicating information or data. To manage this disparate set of uses and users, the task force found it useful to create an IT acquisition framework (Figure 12). The framework offered a means by which to identify substantive areas of commonality and differences between various uses and users, and to gain greater insight into policy and procedural issues affecting IT acquisition. Like any framework, it is an imperfect model of reality, but it is useful in addressing the issues at hand.

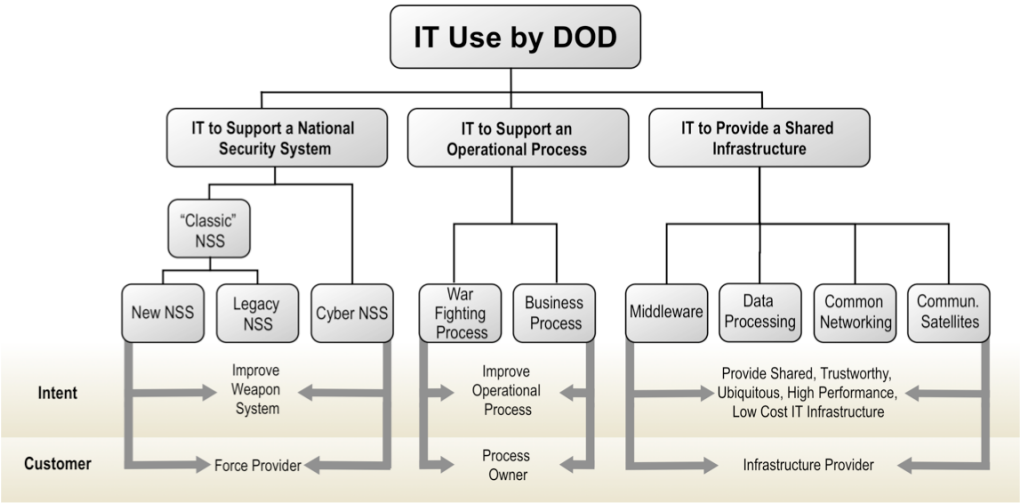


Figure 12. An Information Technology Acquisition Framework

The framework identifies three IT domains that are defined by the mission families in which the IT is used and the eventual customers:

- IT supporting national security systems
- IT supporting operational processes
- IT providing a shared infrastructure for either of the above

IT Supporting National Security Systems

National security systems (NSS) are war fighting systems, such as ships, tanks, missiles, satellites, and planes. IT is embedded within the system so that the end-product achieves its overall purpose. "Customers" of such programs are ultimately users, the war fighters, who obtain their equipment through the force providers. Examples of embedded IT applications include fire control, guidance, communications, and sensing. (For purposes of this study, we also include special networking capabilities that connect NSSs to a broader network.)

The use of embedded IT is becoming pervasive. More and more war fighting system functionality is being determined by embedded software instead of hardware, and many of the issues associated with acquiring and maintaining pure IT systems are applicable to embedded IT. In particular, the large disparity between the rapid turnover of IT and the much longer weapons systems development times is an especially important issue that must be managed.

For IT supporting national security systems, it is necessary to differentiate between new and legacy (existing) systems. IT as an embedded part of a "new" war fighting system (e.g., the radar for the proposed CGX cruiser, or fire control for the Airborne Laser), will have undergone a trade-off process to determine the best approach to meeting the program requirements. This process determines whether a requirement will be met by an approach that uses IT or an alternative that does not. In fact there are many design trade-offs in new national security systems for partitioning the functions and interoperability of embedded IT systems and subsystems, while assuring interoperability and network compatibly with the larger enterprise. At the same time there are likely to be areas of needed technology development requiring advances in science and engineering that have little or nothing to do with IT—such as 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.

IT that is an embedded part of an existing, legacy war fighting system is usually changed in order to provide upgraded or new capabilities. Examples include a fire control upgrade for the Aegis system to address national ballistic missile defense needs, the Acoustic Rapid COTS Insertion program for submarine SONAR improvements, and Link 16 upgrades. In many such cases, key architectural trade-offs will have already been made in the original acquisition program and changes to the system and its information technology are often constrained by those original

program decisions. The task force believes that appropriate acquisition policies for legacy NSS will have more in common with policies for operational processes and much of the infrastructure than it will for policies covering new NSS—a fact that motivated the differentiation in categories.

There are, of course, gray areas. There may be next-generation systems that require such extensive changes that the original architectural trade-offs have to be revisited to allow substantive changes to underlying IT and hardware choices. In this case, the acquisition of a "legacy system" has more characteristics of a new acquisition program than a legacy one.

In Figure 12, these two cases—new and legacy national security systems—were identified as "Classic NSS." To account for the emergence of defense to cyber attacks, a cyber NSS is a system for the cyber domain, the customer of which is a force provider. In this way, it is similar to a conventional NSS such as a missile, but has many of the characteristics of a conventional IT system—workstations, servers, and networks. Therefore, "Cyber NSS" is in the eyes of an acquirer, a conventional IT system for the special purpose of defense of the cyber domain and delivered for use to force providers.

IT Supporting Operational Processes

Conventional IT systems (workstations, servers, and networks) are used to support operational processes in war fighting, much as they are used to support operational processes commercially. Two classes of such processes are of interest to DOD: war fighting processes and DOD business processes. In the first case, IT is developed as a tool set for the processes used to support war fighting operations (e.g., the Tomahawk Planning System, command and control systems, logistics systems, an intelligence analyst's workstation). In the second case, IT is developed as a tool set for processes used to support DOD business operations (e.g., payroll, purchasing, finance, TRICARE medical operations). The customer, in either case, is the "process owner" and the purpose of using IT is to make the end-process more effective.

From a war fighting perspective, these two cases are very different, but from an IT acquisition perspective, they are very similar. The acquisition program needs to balance and ensure consistency between the process being followed (tactics, techniques, and procedures), the tools being built (IT systems), and the training and capabilities of the people who will use these tools within these

processes. This need for balance holds true regardless of whether one is dealing with nuclear command and control or with staff hiring.

IT Providing a Shared Infrastructure

In a net-centric world, no deployed IT systems are islands unto themselves—they exist as part of a shared IT environment. They are usually interconnected to several others through a network, sometimes a global network that provides global interconnection. More and more, these IT systems are being constructed of common elements. Computing platforms have become commodities and are common to all applications except the most unique. A few operating systems have become ubiquitous. Commonly used middleware is more prevalent than ever before. Certain applications have become de facto standards even in the most demanding situations (e.g., the use of Power Point in command and control).

IT that provides a shared infrastructure is acting as a "utility" to various national security systems and operational processes. These utilities are at the processing, networking, and middleware levels.

- Data processing utilities are services that provide general purpose data processing capabilities (e.g., DISA data centers, servers, workstations).
- Common networking utilities are interconnection services (e.g., fiber networks, routers, long haul Internet-protocol networking services, voice-over-Internet protocol products and services).
- Middleware utilities are services that support higher level applications (e.g., directory services, security services, storage services, message services).

The intent of these services is to provide shared, trustworthy, ubiquitous, high performance, low-cost IT capabilities that allow both national security and operational process systems to fulfill their goals.

As will be observed later in this report, acquisition for shared infrastructure IT systems, with one major exception, has more in common with acquisition for operational process IT systems and legacy NSS IT systems that than it does for new NSS IT systems. The major exception deals with IT for communication satellites—that is, those satellites developed to provide long-haul communications (e.g., MUOS or MILSTAR). For this exception, acquiring these systems requires the same trade-off analysis, architectural decisions, and perhaps technology development that new national security IT systems require, and the realization process used to acquire them will have to be similar.

Chapter 4. Existing Defense Acquisition Process

While the task force was underway, the defense acquisition process was being actively reviewed, with the expectation that a new process would be approved by the time of the report's release. Thus, this chapter provides an overview of the process that existed during the task force deliberations, as well as the revised process, implemented in December 2008, and the improvements it was intended to bring forth.

Existing Acquisition Process

The defense acquisition process, prior to December 2008, was approved in 2003 (Figure 13). Its central purpose is to provide a simplified and flexible management framework for translating approved capability needs and technology opportunities into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems.

The process includes five activity phases starting with concept refinement and ending with production and deployment, and operational support. The key actors are the program manager and the milestone decision authority (MDA) who are given broad authority to exercise discretion and prudent business judgment to structure a tailored, responsive, and innovative program.

Multiple milestones and decision points throughout the process permit a program manager to report progress and the MDA to provide permission to proceed to subsequent phases. MDAs are given the flexibility to tailor procedures to achieve cost, schedule, and performance goals, and may authorize entry into the acquisition management process at any point (milestone) consistent with phase-specific entrance criteria and statutory requirements. Progress depends on obtaining sufficient knowledge to continue to the next phase of development. Evolutionary acquisition, or the division of capability into smaller, more executable increments, is DOD's preferred strategy for rapid acquisition of capability.

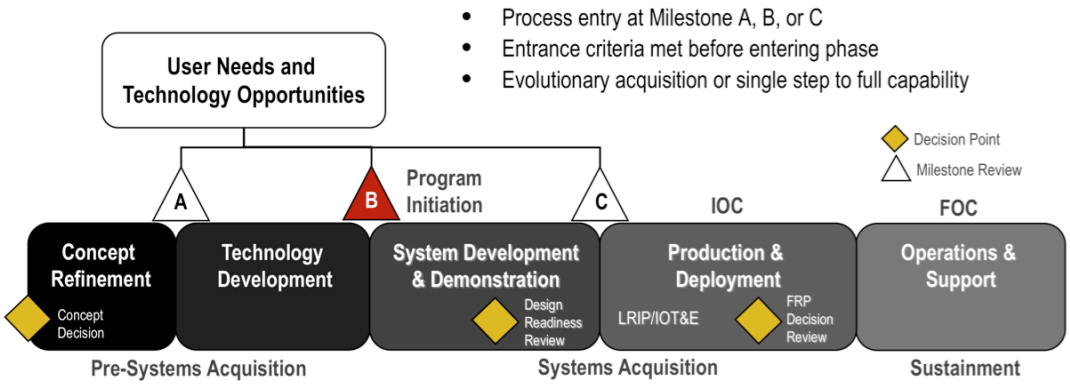


Figure 13. Prior Defense Acquisition Process

This process was designed to accommodate the needs of all programs including information technology. On most occasions, MDAs and program managers have used the inherent flexibility of the acquisition process to proceed directly to Milestone B, or enter into the System Development and Demonstration (SDD) phase, the point where programs are typically initiated. In many cases, this truncated process does not produce desirable results. In short, the deliberate and thoughtful activity of the several phases that precede SDD is either not accomplished in a substantive way or is compressed into the period immediately preceding Milestone B.

The result is that program cost, schedule, and performance may be inadequately informed by the requirements/design trade-offs that are intended to occur during earlier phases. Further, system maturity and compatibility may not have been adequately demonstrated prior to program initiation. Consequently, programs may proceed to development with additional risk and program outcomes are less predictable. Perhaps even more important, the proposed capability may not have been adequately tested against national security objectives to assure that the program supports the most pressing military missions of the Department. Given that the Services are the providers of materiel, programs sometimes reflect Service, rather than Department, priorities.

The New Defense Acquisition Process

A new defense acquisition process was approved in December 2008 (Figure 14). The new process remains generally applicable to IT programs and sustains the former emphasis on process flexibility and evolutionary acquisition. While

maintaining many of the same structural characteristics of the earlier process, it introduces some important policy changes intended to improve process discipline, program stability, and program outcomes.

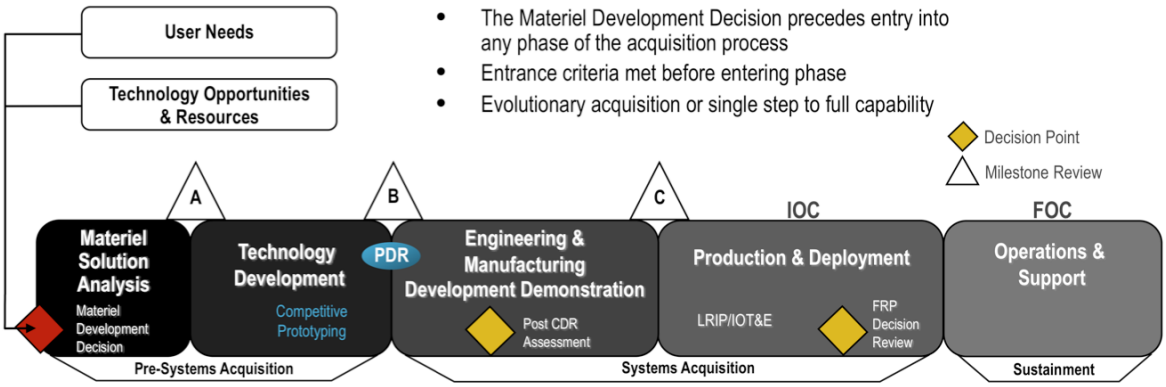


Figure 14. New Defense Acquisition Process

Policy changes embedded in the new process include the following:

- All programs will proceed through a formal acquisition process entry point, the Materiel Development Decision (MDD). Programs will no longer immediately proceed to Milestone B. Consequently, the vast majority of programs will benefit from the improved conception and technical maturity resulting from the early phases of development.
- Programs requiring technology development will conduct competitive prototyping at the system or sub-system level, when appropriate, to ensure that technologies have been demonstrated in a relevant environment and, consequently, key risks have been retired before programs are initiated.
- Where consistent with the strategy for the Technology Development Phase, preliminary designs will be prepared to ensure that requirements are well understood and cost estimates well informed.
- The Engineering and Manufacturing Phase has been redesigned to place additional emphasis on systems engineering and manufacturing readiness.
- Configuration Steering Boards have been established to ensure that requirements changes/creep, a traditional contributor to increased cost and extended schedules, are not casually approved.

While the task force agrees that these are substantive changes with potential to improve the acquisition process, more can be done to tailor the acquisition process to the unique attributes of information technology, as will be discussed in the following two chapters.

Oversight Responsibility

Oversight is a necessary and important part of the defense acquisition process, which employs a layered approach to oversight based on the level of investment (Figure 15). All programs are conceived and designed at the component level consistent with formally approved requirements. Most programs are reviewed at the same level by designated component milestone decision authorities (MDAs), typically the component acquisition executive (CAE) or a program executive officer (a flag officer or SES). The most significant investments, programs categorized as major automated information systems (MAIS) or major defense acquisition programs (MDAPs), receive additional review within the Office of the Secretary of Defense (OSD).

At the OSD level, major systems (both weapon systems and automated information systems) are initially assessed by specialized review teams called Overarching Integrated Product Teams (OIPTs) staffed with executive-level subject matter experts (Table 1). (The Investment Review Board (IRB) serves the same purpose for Business Transformation MAIS.) The ASD (NII) OIPT and the Business Transformation Agency IRB are focused on information systems, with the latter focused specifically on IT business systems. Another OIPT is principally focused on weapon systems. These groups review programs to ensure they are well planned and compliant with statute and regulation. Their findings and recommendations are reported to the milestone decision authority.

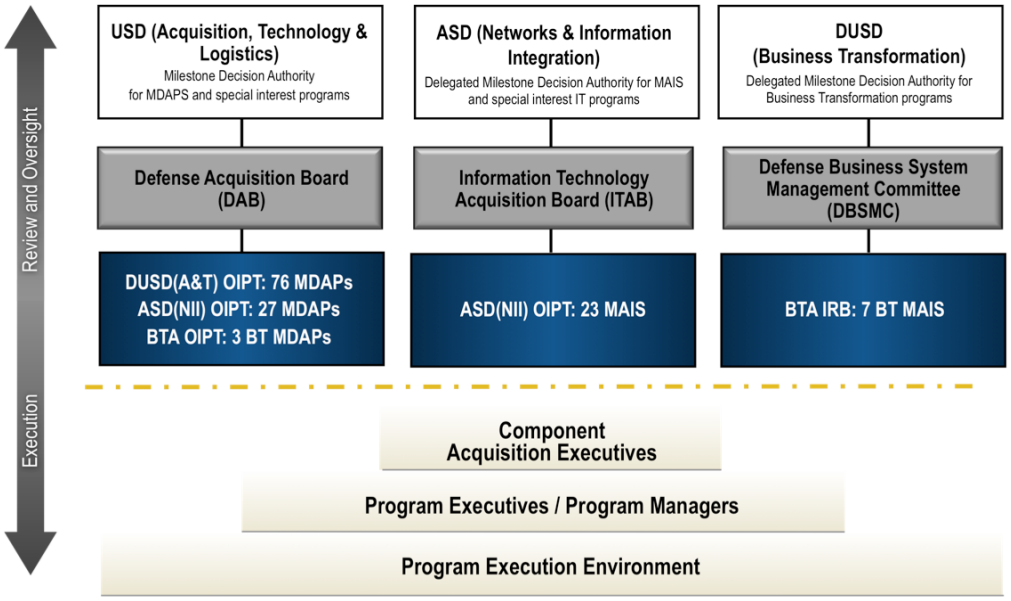


Figure 15. OSD Acquisition Oversight Responsibility

The USD (AT&L) is the milestone decision authority for major defense acquisition programs and for MAIS that achieve the same funding threshold. The ASD (NII), with authority delegated by USD (AT&L), is the milestone decision authority for a portfolio of MAIS programs and the Deputy Under Secretary of Defense for Business Transformation, also with delegated authority, is the milestone decision authority for MAIS business systems. Each of the three MDAs is advised by senior executive boards: the Defense Acquisition Board, which covers weapon systems; the Information Technology Acquisition Board, which covers major automated information systems; and the Defense Business Systems Management Committee, covering MAIS business systems. Each milestone decision authority has approval authority over assigned programs.

Programs are reviewed and approved by the milestone decision authority at key decision points in the acquisition business process to ensure they are being conceived, designed, and executed consistent with sound business practices and the approved acquisition program baseline (cost, schedule, and performance objectives). Programs are executed at the component level under the direct supervision of the component acquisition executive, program executive officers, and the program manager.

Table 1. Acquisition Category Designation

Acquisition Category	Reason for ACAT Designation	Decision Authority
ACAT I	• MDAP (section 2430 of Title 10, United States Code) • Dollar value: estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than $2.190 billion in FY 2000 constant dollars • MDA designation • MDA designation as special interest	• ACAT ID: USD(AT&L) • ACAT IC: Head of the DOD Component or, if delegated, the CAE (not further delegable)
ACAT IA	• MAIS (Chapter 144A of Title 10 of U.S.C.): A DOD acquisition program for an Automated Information System (either as a product or a service) that is either: • Designated by the MDA as a MAIS; or • Estimated to exceed:$32 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred in any single fiscal year; or • $126 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or • $378 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system. • MDA designation as special interest	• ACAT IAM: USD(AT&L) or designee • ACAT IAC: Head of the DOD Component or, if delegated, the CAE (not further delegable)
ACAT II	• Does not meet criteria for ACAT I • Major system • Dollar value: estimated by the DOD component head to require an eventual total expenditure for RDT&E of more than $140 million in FY 2000 constant dollars, or for procurement of more than $660 million in FY 2000 constant dollars (section 2302d of Title 10, United States Code) • MDA designation (paragraph (5) of section 2302 of Title 10, United States Code)	• CAE or the individual designated by the CAE
ACAT III	• Does not meet criteria for ACAT II or above • AIS that is not a MAIS	• Designated by the CAE

Chapter 5. IT Acquisition Challenges and Issues

As the previous chapter described, information technology is currently procured using the same acquisition system as is used for major hardware systems. The acquisition model most often employed is the familiar "waterfall" development model in which well-defined increments of capability or technology are designed, developed, and fielded in a pre-specified order. The "flow" of releases is sequential and deviations from the approved sequence are cause for a new baseline for the program (or in extreme cases cancellation). Since a new baseline generally triggers a complete top-to-bottom review of the program, delays are inherent and often approvals at each step up the acquisition approval chain become more difficult to obtain. The result is usually an increase in the time required to deliver the increment(s) and the program.

In his recent *Foreign Affairs* article, Secretary of Defense Robert Gates highlighted trends in today's acquisition process with platforms growing even more "baroque."[27] He questioned the necessity to go outside the normal bureaucratic process to develop technologies that will counter improvised explosive devices, build Mine Resistant Ambush Protected (MRAP) vehicles, and quickly expand U.S. ISR capabilities. In short, he questioned the efficacy of the current acquisition process, given the apparent need to bypass existing institutions and procedures to rapidly field needed capabilities to protect U.S. troops on the battlefield. The Secretary issued a call to the defense establishment to think hard about the current acquisition paradigm—a procurement process that seeks a 99 percent solution over a period of years, when today's missions require solutions over a period of months or even weeks.

Where technologies or requirements can be developed and delivered over a relatively large timeframe (years), the traditional waterfall acquisition model can deliver acceptable results—war fighters get needed capabilities in time to counter or deter the threat. However, when that timeframe is small (hours, days, or months), the deliberate, sequential nature of the waterfall model does not serve

27. Robert Gates. 2009. "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January/February.

DOD well. Information technologies reside in a domain where change occurs in small timeframes, both for technology and for the ability of adversaries to procure, adapt, and employ the technologies.

An analysis of 32 major automated information system acquisitions, conducted by the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)), calculated that the average time to deliver an initial program capability is 91 months (Figure 16). Today's "big bang" approach used in the acquisition of IT begins with an analysis phase followed by an equally long development phase that culminates in a single test and evaluation event. The average time between the start of a program's analysis phase (Analysis of Alternatives) to Milestone B (System Development and Demonstration)—is 43 months: 14 months to complete the analysis of alternatives (AoA) and 29 months to complete the economic analysis (EA). Likewise, it took an average of 48 months to deliver useful functionality from the Milestone B decision—40 months for development and an additional 5 months for operational test and evaluation

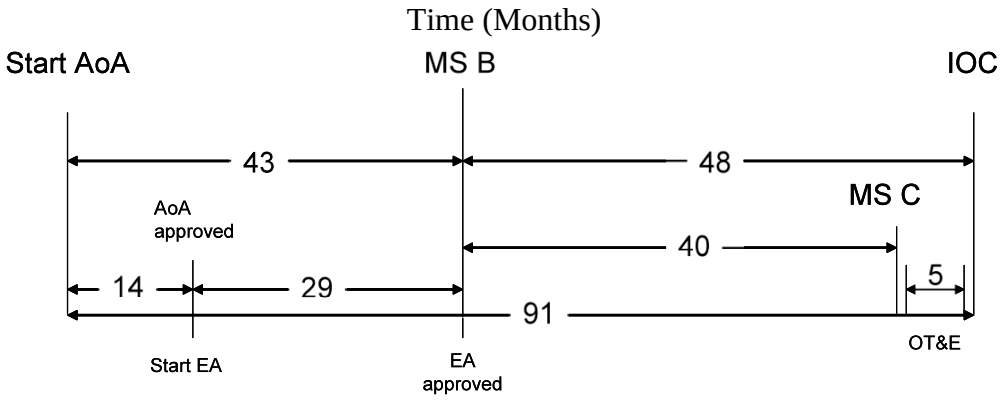


Figure 16. MAIS Acquisition Timeline

An advantage of current IT technologies (some would say a "complexity") not addressed within current DOD acquisition policies and procedures, is that the acquisition of IT does not necessarily require delivery of a "system" but instead may involve providing new services or capabilities, that may require only small investments to the supporting IT infrastructure. Given the current investments by commercial industries to invest in and deploy service-oriented

architectures, the task force expects that DOD and the Services will seek to adopt similar technologies. Without an acquisition process that accommodates, and takes advantage of, IT's rapid pace of change, future DOD acquisition officials will likely be frustrated in their efforts to equip the nation's war fighters and weapon systems with the needed information technologies.

Why the Process is "Broken"

With so many prior acquisition reform efforts to leverage, any novel approach for acquiring IT is unlikely to have meaningful impact unless it addresses the barriers that prevented prior reform efforts from taking root. Perhaps the two most important barriers to address are experienced proven leadership and incentives (or lack thereof) to alter the behavior of individuals and organizations. According to the Defense Acquisition Performance Assessment Panel, "… current governance structure does not promote program success—actually, programs advance in spite of the oversight process rather than because of it." This sentiment was echoed by a defense agency director in characterizing IT acquisition as hampered by the oversight organizations with little "skin in the game."

Many functional organizations (Comptroller, Programs Analysis and Evaluation (PA&E), Office of the Director, Defense Research and Engineering (DDR&E), and Operational Test and Evaluation (OT&E)) have assumed the responsibility to "stop" programs that are unable to fully satisfy their concerns. While these offices can bring value during program reviews, the task force believes that the nature of their involvement must be adapted in order for DOD to achieve rapid acquisition of information technologies.

Acquisition improvements can only be achieved if the program's overriding focus is performance and schedule and if decisions to proceed are made at regular intervals by the acquisition decision authority with full knowledge of the risks. This approach implies that the program manager is not obliged to obtain a "thumbs up" from each functional organization. The program manager is obliged to do all within his authority to mitigate risk but the overriding priority is to conduct the decision meeting in accordance with a desired schedule for availability of capability. Although program managers must provide the acquisition decision authority with the risks identified by the functional organizations, the milestone decision authority holds the full burden of accountability for accepting (or rejecting) program risk on behalf of the Department or Service. The intent is to set the schedule of decision points to

match the schedule for providing fielded capability, and prevent the ability of well-intentioned and necessary functional reviews to slow or inhibit the decision-making schedule. To that end these functional organizations should be involved early and continually to provide their support and insight to assure program success, rather than become a "log jam" at decision points.

The use of the Technology Readiness Assessment (TRA) illustrates this point. Instead of applying technology readiness levels (TRL) to guide fundamental advances in science and engineering underlying cyber infrastructure and leap-ahead technologies, DOD employs TRLs to assess interoperability, logistics considerations, information assurance, system engineering, and effectiveness considerations. Much of the confusion stems from the fact that TRAs were developed for a hardware model and not designed to address the maturity of IT systems for acquisitions.

In presentations to the task force, DOD officials highlighted that TRA evaluations for IT were breaking new ground and included first-ever assessments. It appeared unclear whether these efforts were focused toward evaluating maturity of salient IT criteria such as those defined by the American National Standards Institute, Institute of Electronic and Electrical Engineers, or The Open Group's Architectural Framework standards. Also, TRA evaluations are the responsibility of, and approval authority by, the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)), and TRA oversight is executed outside the typical OIPT and program office structure. Instead, oversight is conducted by DUSD (S&T) who works directly with the Science and Technology Executive in the DOD component or agency. This results in confusion and debate regarding roles and responsibilities among the other functional oversight organizations (e.g., Chief Information Officer; Director of Logistics and Material Readiness; Director of Systems and Software Engineering; or Director of Operational Test and Evaluation).

It is not uncommon for this confusion of responsibilities to lead to extended coordination cycles as witnessed by the Net Enabled Command Capability (NECC). With well over a year following the TRA's original submission to the Office of the Secretary of Defense and three separate agency attempts, the document has yet to be approved despite the program's use of standard commercial off-the-shelf (COTS) technologies. Unable to proceed forward, Congress removed $119 million from the program budget, which was subsequently followed by removal of an additional $270 million by OSD (PA&E). While we do not question that acquired software should be assessed to

assure it is ready and appropriate to insert into a DOD system, we question "stretching" the hardware rules to involve organizations and people that have little experience in IT development or acquisition.

This confusion is not limited to the TRA. The acquisition strategy for the Enhanced Polar System was in OSD coordination for over eight months before ultimately being rejected because the Air Force approval was more than three months old. These examples are two of many illustrating the lack of accountability built into the acquisition governance system, which establishes neither clear incentives for positive performance nor discipline for poor performance, with no systematic tracking of either.

Section 814 of the 2006 National Defense Authorization Act directed the Defense Acquisition University to review DOD acquisition structures and capabilities. This analysis revealed that DOD acquisition organizations are continuously evolving to address better mission focus and improved productivity; however, it did not result in improved acquisition outcomes. Today, there are four different OSD-level organizations involved in IT acquisition:

- Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, who serves as the milestone decision authority for the 23 MAIS programs
- Business Transformation Office, who serves as the MDA for seven Enterprise Resource Planning software-intensive acquisitions
- Director of Systems and Software Engineering, with responsibility focused primarily on embedded IT in major weapon systems
- Director of Space and Intelligence Capabilities Office, who leads the acquisition oversight for National Intelligence Agency programs including numerous major software-intensive acquisitions

The leadership and staff experience within these organizations vary significantly. Some leaders have recent industry or acquisition executive experience, while others have neither IT expertise nor relevant industry experience in either the leadership or staff. Likewise, it is not clear that these organizations are working together to achieve the spirit of the Clinger-Cohen Act (40 U.S.C. 11314), or serve with common focus toward achieving the five-year time-certain development imposed as part of the 2009 National Defense Authorization Act.

Recent wartime experiences highlight the importance of IT and the ability to fuse information from a broad range of sources outside DOD boundaries. Today, information derived from national intelligence is having a dramatic impact on the lethality of the nation's war fighting forces, and future operations will likely require access to even more national and international information. At the time of Goldwater-Nichols, the vast enabling capability inherent within IT was not apparent nor was the understanding of the impact of extending the edge of modern computing to effectively leverage such capabilities. Figure 17 characterizes the long-standing government weakness regarding information resource planning and decision-making where modernizations so often occur within organizations that continue to be challenged by the lack of an integrated "enterprise" philosophy.

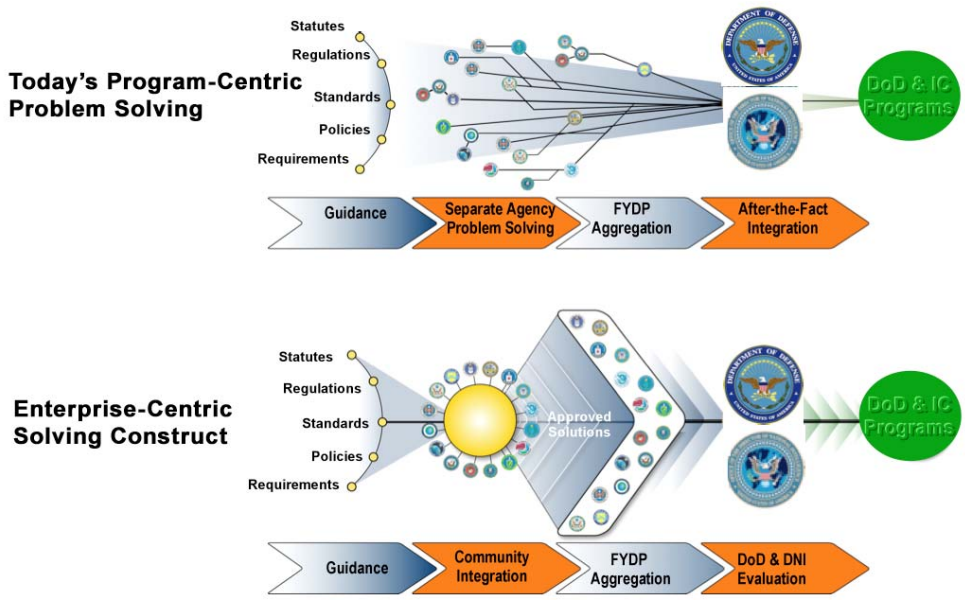


Figure 17. Effective Oversight Paradigm: Enterprise Level Decision Making

In addition to the need for more robust IT governance, DOD needs to better leverage the IT acquisition instruments and services of other federal agencies, to include better utilization of organizations such as the General Services Agency. Likewise, the Department needs to capitalize on the strides made in enhancing IT governance by better leveraging groups such as the CIO Executive Council in making investments, estimating costs, and enhancing the effective and efficient use of IT infrastructure. As the Department postures itself

for the future, the OSD acquisition oversight construct needs to be coherently linked to the larger CIO enterprise, with proper authorities to address organization-level decisions regarding information policy vision, architecture, strategy, and information assurance.

Maintaining a Knowledgeable and Experienced IT Acquisition Workforce

The number of programs having troubles associated with information technology, as reported by sources such as the GAO, suggests that the government is challenged in its ability to successfully manage the acquisition of these technologies. Anecdotal reports from industry suggest commercial companies face similar management challenges. Both government and industry have reported impending staffing difficulties due to the expected retirement of many in the current IT workforce and the small number of remaining and incoming personnel.

Given these demographics, the most often heard solutions are to streamline the processes and better train remaining and incoming personnel. The task force found these solutions to be reasonable, but perhaps insufficient.

In the years since Goldwater-Nichols, and sometimes due to "encouragement" by Congress, DOD has developed training and certification regimes for its acquisition workforce:

- The Defense Acquisition University was established to provide training and support to DOD's acquisition workforce and program managers. In addition to courses on the acquisition of hardware-based technology, the university teaches courses on the management of software-intensive programs, including the processes pioneered by the Software Engineering Institute. All acquisition workforce members are required to complete a set course of instruction, and achieve a specified level of certification, before they can be permanently assigned to designated acquisition positions. For example, program executive officers, major program managers, and program managers must complete advanced courses in program management. Given the continually evolving character of best practices for IT systems and their management, it is imperative that the DOD CIO assure that these programs are current.
- Among DOD's acquisition workforce are many individuals with degrees in disciplines such as computer science, systems engineering, electrical

engineering, engineering management, finance, and logistics. Many hold advanced degrees.

- Within the ranks of the uniformed military's core of acquisition professionals, advanced degrees and recurring tours in acquisition and/or engineering are prerequisites to advancement and selection to command.
- Within DOD and the Services, the selection (whether civilian or military) of a program executive officer, major program manager, or program manager (or the deputy to these positions) is, by directive, accomplished through a series of selection panels, committees, boards and officials—all charged with finding, recommending, and/or selecting the most qualified individual for the specific acquisition at hand.

Yet, in spite of the education requirements, certifications, and rigorous selection processes, the general impression remains that managing DOD's IT efforts should yield a better record of success. We must be clear that neither training nor education is a substitute for experience in successfully managing acquisition programs of increasing complexity. For that reason, the task force emphasizes proven experience, in addition to education and preparatory training, as the most important criteria for selecting individuals so that informed judgments based on experience can guide program decisions.

Many Other Studies Have Warned of IT Acquisition Challenges

Concerns regarding acquisition cycle time, flexibility, and efficiency have led to decades of studies and recommendations for improvement. Such acquisition reform studies have been on-going almost continuously since the original Goldwater-Nichols legislation was passed in 1986.

The Center for Strategic and International Studies sponsored several such acquisition reform studies including *Beyond Goldwater Nichols: Defense Reform Phase 1* and *Phase 2* in March 2004 and July 2005, respectively. These studies concluded that the U.S. national security apparatus requires significant reforms to meet the challenges of a new strategic era. As part of its transformational efforts, DOD must not only adapt to the post–cold war, post–9/11 security environment, but also cope with many "hidden failures" that, while not preventing operational success, stifle innovation and continue to squander critical resources in terms of time and money. It identified many organizational structures and processes initially constructed to maintain a cold war superpower

in the industrial age, but which are inappropriate for 21st century missions in an information age.

This sentiment was echoed by numerous leaders interviewed by this task force and characterized in the 2006 Quadrennial Defense Review (QDR) Report. In addition to an illustration of the gap in today's capability portfolio (Figure 18), the report noted, "as we emphasize agility, flexibility, responsiveness, and effectiveness in the operational forces, so too must the Department's organizations, processes and practices embody these characteristics if they are to support the joint war fighter and the Commander in Chief."

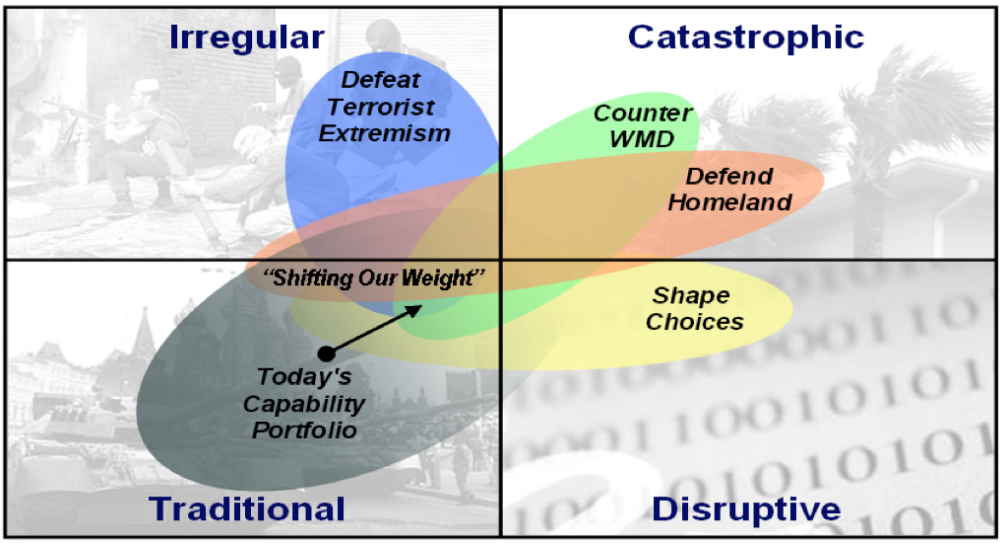


Figure 18. 2006 Quadrennial Defense Review Capabilities Portfolio

As mentioned earlier in this report, a RAND study on the cost growth of 35 weapon systems highlights that development cost growth is driven equally by cost estimating errors and requirements growth, which account for almost two-thirds of the total cost growth.[28] This conclusion also was shared by the GAO in its June 3, 2008 assessment that called for fundamental changes in the acquisition environment. It cited systemic problems at the strategic level resulting in a requirements and acquisition process that is neither agile enough to support

28. *Sources of Weapon System Cost Growth: Analysis of 35 Major Weapon Systems*, RAND Corporation, 2008. http://www.rand.org/pubs/monographs/2008/RAND_MG670.pdf

current operational needs nor able to effectively estimate the costs of such modernizations. Similar conclusions were likewise shared by several leaders interviewed by the task force who observed that the fundamental model used in the acquisition of IT capabilities is inappropriate. The 1990 Defense Science Board Task Force on Defense Software reported the need to move away from the waterfall model to an iterative model since approximately 90 percent of the time, the waterfall model results in late, over-budget, fragile and expensive-to-maintain software systems.

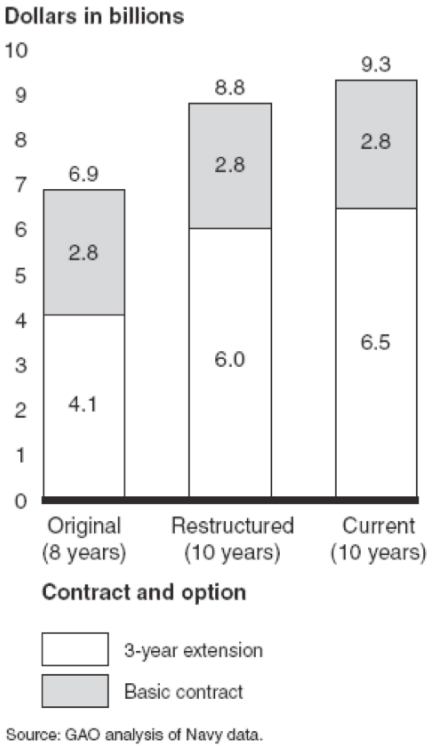


Figure 19. Cost and Schedule Overruns in IT Programs

Cost overruns and schedule delays, which result in numerous audits and evaluations by independent government and industry organizations, also point to the need for a more streamlined IT acquisition system (Figure 19). A GAO review conducted in July 2008 concluded that 48 percent of the federal government's major IT projects have been re-baselined for several reasons, including changes in both project goals and funding. Of those projects, 51 percent were re-baselined at least twice.

The Joint Tactical Radio System (JTRS) is one of many examples. Because of development and production delays, GAO reported that the military has more than doubled its spending on tactical radios from a planned $3.2 billion to about $8.3 billion over the past five years. Another example is the Navy Marine Corp Intranet (NMCI), reviewed by GAO in 2006. The NMCI program is a multiyear information technology services program. Its goals are to provide information superiority and foster innovation via interoperability and shared services. The

Navy awarded the NMCI services contract—currently valued at $9.3 billion—to Electronic Data Systems (EDS) in October 2000.

The contract calls for EDS to replace thousands of independent networks, applications, and other hardware and software with a single, internal communications network (Intranet), and associated desktop, server, and infrastructure assets and services for Navy and Marine Corps customers. GAO's 2006 review of Navy data highlighted that NMCI has met only 3 of 20 performance targets (15 percent). It cited that five shipyard/air depots continue to rely on their legacy systems rather than NMCI. Officials at two of the sites stated that NMCI is hurting workforce productivity and users "reach back" to legacy systems because NMCI is slow, sometimes taking 45 minutes to open a document. Similar to JTRS, NMCI incurred significant cost growth from its original contract award with contract extensions, revisions, and engineering changes that also delayed capability.

Legislative Changes

Congress, in its oversight role, responds to the Department's acquisition shortfalls by adding more restrictive legislative mandates. The 2007 National Defense Authorization Act contained unprecedented mandates involving the acquisition of IT via Section 816 and Section 811. Section 816 was codified as 10 U.S.C. Chapter 144A. It defined the criteria for a MAIS program and, beginning in January 1, 2008, required annual reports to Congress containing the following:

- development schedule with major milestones
- implementation schedule including estimates of milestone dates, initial operational capability (IOC) and full operational capability
- estimates of development and life-cycle costs
- summary of key performance parameters

The statute also established Nunn-McCurdy-like reporting for MAIS programs by defining the initial report as the baseline for determining significant and critical changes. Any change in cost, schedule, or performance that exceeded predefined limits will be associated with a significant or critical change, triggering a report to Congress. Likewise, the statute required program managers to submit quarterly reports disclosing program variances to the senior Department official.

Section 811 implemented new time-certain development mandates for IT business systems. The statute requires that the milestone decision authority certify that the acquisition will achieve IOC in five years or less from Milestone A before granting approval. This requirement equally applies to all IT business system acquisitions regardless of their size. The only software-intensive programs excluded from this requirement are national security systems that directly support war fighter operations. If subsequent acquisition activities are unable to achieve IOC within five years, the system would be deemed to have undergone a critical change triggering reporting in accordance with 10 U.S.C. Chapter 144A.

In the 2009 National Defense Authorization Act (Section 812), Congress extended the reporting requirements defined in 10 U.S.C. Chapter 144A to include pre-MAIS programs. However, the value of this reporting is questionable since pre-MAIS programs typically do not have development or implementation schedules, cost estimates, or key performance parameters to baseline. Another mandate contained in Section 812 was the changes associated with time-certain developments. Instead of the 5-year requirement to achieve IOC from a program's Milestone A, the law changed the date from Milestone A to start "when funds for program are first obligated."

Chapter 6. A New Acquisition Process for Information Technology

While the task force recognizes DOD's efforts to improve the defense acquisition process, the planned changes do not go far enough to address the unique characteristics of information technology programs and the rapid timeframes within which such programs evolve. Implementing IT capability is a transformational endeavor; there are continually evolving best practices, processes, and organizational considerations that must be addressed. Thus, the task force proposes that DOD develop a new acquisition management model tailored to information technology.

The proposed model recognizes the unique aspects of information technology and provides more value-added activities, as compared to the current process. It includes enhanced stakeholder engagement and analytical rigor throughout the acquisition life cycle. Program reviews begin during the business case development phase and extend until full deployment of mission capability. In earlier phases of the acquisition, the quarterly program reviews should be calendar-based events (perhaps quarterly), while later phases should link such reviews with iterations or delivery of capability.

The success of this model is based on the following criteria:

- early and continual involvement of the user
- multiple, rapidly executed increments/releases of capability
  - well defined objectives but not over defined requirements for the initial increment
  - evolving requirements for subsequent increments/releases
  - mature technologies (often with short half-life that require periodic refresh)
- early, successive prototyping to support an evolutionary approach
- early operational release of capability from within an increment
- modular, open-systems approach—designed for ease of updates
- available full funding of initial increment(s); solid funding stream for next overlapping upgrade increment(s)

- making schedule the priority for releasing available capability and not requiring (or expecting) a "yes" vote from every functional organization prior to decision milestones
- making sure that users are trained and prepared to receive the new capability

Model Characteristics

The proposed acquisition process is divided into four phases (Figure 20). Each phase begins with either a milestone decision authority–level decision review or a milestone event to ensure adequate knowledge is available to proceed to the following phase, which is associated with increasing levels of investment.

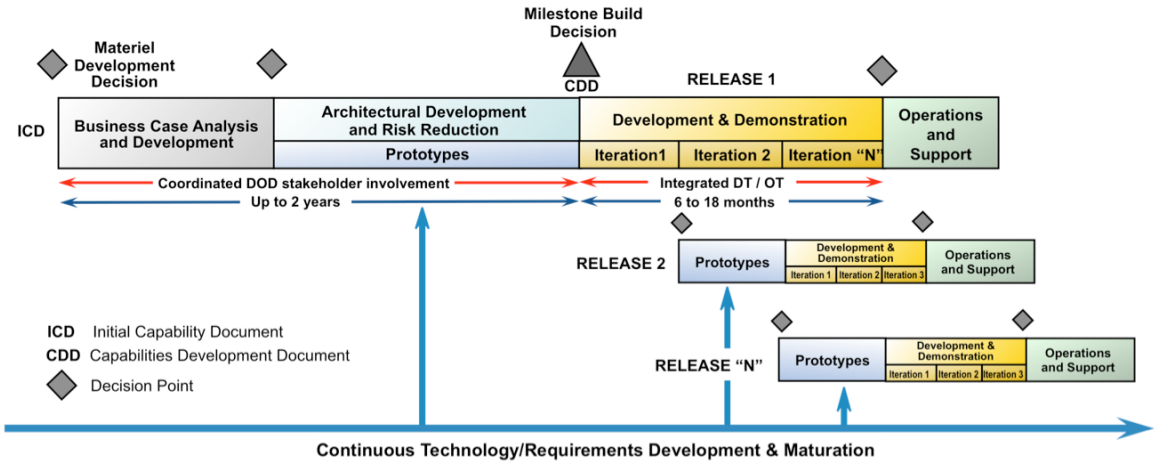


Figure 20. A New Acquisition Process for Information Technology

The new model characteristics, a number of which are consistent with DOD's new acquisition process model, are critical to success:

- **Sound structure and effective oversight**. The model is divided into four phases:
  1. **Business Case Analysis and Development**. Establish the need for the proposed capability and develop the concept for the proposed solution. The phase begins once an Initial Capability Document and draft Concept of Operations are approved, based on an identified mission need.

2. **Architectural Development and Risk Reduction**. The core architecture is built and architecturally significant features demonstrated. Prototyping begins during this phase and continues throughout the acquisition life cycle to assess the viability of technologies and minimize high-risk features, while simultaneously refining user capability expectations.
3. **Development and Demonstration**. The period when operational capability is built and delivered for a discrete number of releases. Capabilities are prioritized and parsed into groupings to establish release baselines for the sub-programs. Includes development of training programs and testing in realistic environments to ensure successful fielding of new capabilities.
4. **Operations and Support**. Provides materiel readiness, user training, and operational support over the total program life cycle.

- **Enhanced stakeholder engagement and analytical rigor at the enterprise level.** Today's practice of not extending the architecture and engineering systems analysis rigor from the enterprise level down to the program level has resulted in poor acquisition outcomes. While the proposed acquisition may well serve the individual DOD component, it is often ill equipped to foster modern "enterprise" behavior. Under the proposed process, program initiation depends on a credible business case based on analytical rigor applied and reviewed at the program and enterprise levels. The business case should demonstrate that while the solution may serve the unique needs of the individual DOD component, it must also add value when appropriate to the larger enterprise. There is a natural tension between the goals of the individual program and the goals of the enterprise. Individual programs often can quickly develop capabilities if they ignore enterprise needs. However, these capabilities are not likely to be interoperable. Activities that do not seem to need interoperability mechanisms today often will tomorrow. Further, as one looks across the enterprise at a set of mission-specific program developments, one inevitably sees redundancy and inefficiency.

  Nonetheless, processes for managing the trade-offs between local program-based decision making and enterprise coordination are themselves time-consuming. The model proposed here puts specific emphasis on this problem by calling for up-front analysis (when requirements are most flexible and costs are lowest) so that good decisions—including decisions about enterprise integration—are made

when they can have high impact. Assurance of this enterprise compliance is a critical role of the DOD CIO.

- **Acquisition processes and governance** must ensure full and effective integration of CIO roles and responsibilities for IT professionals—throughout the process.
- **Prototyping**. Each increment of development must be supported by early and continuous prototyping to ensure that the necessary technologies and functionality will be available in real time to support development. The model embraces continual technology development, prototyping, and the accompanying requirements maturation throughout the acquisition life cycle.
- **Training and testing**. To successfully field capabilities, comprehensive testing, training, and follow up user support is required. The extensive prototyping should enable user feedback and training program development to be effectively incorporated into the program early and continue throughout development.

The model also introduces some important new characteristics:

- **Multiple rapidly executed increments/releases of capability**. Each increment would be responsive to a single approved Capability Development Document (CDD) and each would be fully funded. In an important departure from current practice, each increment of capability would include multiple ("N") capability releases, each a useful stand-alone capability consistent with the approved CDD. The need for more than "N" releases would trigger a new CDD and subsequently a new increment. Each release would be developed in approximately 18 months or less. Releases, in turn, are sub-divided into multiple iterations to facilitate assessment of progress by prioritizing work scope into a smaller subset of functionality that is tested and potentially deployable. It is important to emphasize that smaller increments allow for better synchronization with enterprise capabilities now evolving at the same rapid rate as the program capabilities. More frequent releases allow opportunities to continually address integration and interoperability issues rather than having to get them all "right" in the requirements phase.

  All releases would be accommodated by the baseline for the increment or, consistent with recent changes to statute, could be treated as sub-programs with unique cost, schedule, and performance parameters.

Prototyping will typically be employed in each release, but whether it is necessary will depend on the capability goals of the particular release. Deployment would be based on the results of testing and approved by the acquisition decision authority. In short, this approach replaces the current "big bang" model with a responsive alternative that provides incremental mission capability much sooner.

- **Thoughtful satisfaction of requirements**. The objective of this new model is to develop and deploy the highest priority mission capability first. Therefore, capabilities defined in the CDD should be prioritized, and, where appropriate, grouped into a limited number of time-phased releases that correspond to mission priority. While each increment will be supported by an approved CDD, an agile approach would, with the active engagement of the requirements community, allow for (and encourage) reprioritization of requirements for each iteration and release (and for the increment as a whole) based on subsets of functionality to prevent delay and facilitate rapid development/deployment. While rapid introduction of smaller releases of capability is attractive, it must be moderated by potential confusion in the field and the training required in support of each release. Therefore, tight coordination between user operators and developers is required to schedule each release.
- **Better informed cost estimates**. By decomposing and managing an acquisition in well understood and thoughtfully described smaller units, the Department's process for creating realistic initial cost and schedule baselines has the potential for significant improvement. As noted by the earlier references to RAND, GAO, and Defense Science Board reports, the acquisition and resourcing processes do not always produce realistic cost and schedule estimates; hence program buy-in with very optimistic estimates is common while resulting cost and schedule performance is poor. To enhance the fidelity of cost and schedule estimates, the new model departs from the current practice of requiring a cost estimate only at program initiation. Instead, each release is treated as a sub-program for purposes of cost and schedule estimating and reporting. Following the initial cost estimate at the "build decision" (program initiation), estimates are refined after each release to reflect program results based upon realized performance and forward-looking priorities. The Department should also embark upon an effort to improve analytical rigor by expanding the analysis beyond previous DOD cost information; estimates should leverage all relevant cost databases. The task force

recognizes that experienced analysts necessary to achieve this fidelity are not currently available in the Department or the Services.

- **Contracting and funding**. We envision a lean, commercially based acquisition model that emphasizes extensive analysis prior to development, a flexible requirements process, better cost estimates, and modular and incremental development and fielding over shorter cycles. This model implies that each development increment will result in less than the ultimate capability—a change that the Department and Services should be prepared to accept. In addition, and important to the success of this new model, the contract vehicles used to acquire these increments must be flexible enough to allow for changes in delivered capability within a particular increment or allow capabilities to be deferred to subsequent increments if the capability realization must be delayed without onerous cost consequences to the government.

  This contracting approach will require careful definition of the expected increments of capability as well as flexibility within the contracting vehicle to allow the program manager to defer based on his or her own authority. When the requirements for subsequent increments of capability are not sufficiently refined to support detailed cost estimating, DOD should embrace the concept of "level-of-effort" funding. This approach will ensure that adequate funding is continuously available to support multi-increment developments and, as important, to upgrade and sustain fielded capability. It will also require significant training and culture change for DOD contracting officers and program officials. This model, in effect, "fixes" budget and program timelines. The burden, then, is on the program to define capabilities that can be fit into those constraints. Finally, just as there is no substitute for acquisition leadership experience, the same is true for contactors. 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.

- **More frequent but less formal progress reviews**. As defined earlier, progress in today's acquisition oversight process is accomplished through overlapping and protracted coordination, which tends to make change at the margin rather than enable substantial trade-offs. Instead, the IT acquisition process requires continuous "hands-on" oversight beginning at the Material Development Decision via quarterly program reviews to get first-hand progress as reported by the program manager. Program

reviews, tied when possible to release "iterations," will expose flawed programs or poor design early while the program is small and, by forcing early integration, it avoids the downstream issues resulting in more robust and maintainable designs. Multiple decision points can be interspersed throughout the program based upon the inherent risk and program life cycle.

- **Tailored testing practice**. Test planning, test execution, and post-deployment support cannot be based upon traditional thinking that scope and content is fixed at the beginning. Instead of a single test event, acquisition activities rely on development test events after each iteration and operational testing to support decisions to field the release. An especially important planning consideration is the use of automated testing to allow effective iterative testing of previous functionality.
- **Modular, open-systems approach**. In an operational setting, the IT acquisition process requires movement to an open architecture structured for ease of upgrades. A fundamental step is to partition the design into a hierarchy of individual modules (both hardware and software) with well defined interfaces based on open standards, such that the inputs and outputs of a module are effectively isolated from the specific design utilized inside that module. Thus, so long as interface requirements are satisfied, changes can be made within a module without impacting higher level system functionality and reuse of modules is enabled.

  The use of standards-based reference models, well-defined and published interfaces, and test and acceptance criteria ensures transparency and the widest range of options in vendor selection. A standards-based, open system serves to mitigate the specification of a system for a vendor's proprietary product, but also helps to prevent restrictive intellectual property rights issues and vendor lock-in. This practice clearly follows commercial best practices; however, in rare instances a more deliberate government specific policy may be needed to increase the information assurance position of critical systems.

The growing importance of information demands focused management of the information technology enterprise. The policy revisions proposed here are consistent with current best commercial practice, have been employed successfully by industry (and to a far lesser degree in DOD), and reflect principles that are both effective and applicable to the DOD IT acquisition environment. The employment of an agile approach will increase IT capability,

program predictability, reduce cost, and decrease cycle time—all business imperatives, especially in a potentially austere budget environment.

Model Phases

Each phase of the new acquisition process for information technology is described in more detail below.

Business Case Analysis and Development

The Business Case Analysis and Development phase establishes the need for the proposed capability and develops the concept for the proposed solution. During this phase designers will develop an understanding of the operational objectives, the operator's perspective of the criteria for success, and the implications for architectural imperatives and complexity issues. This activity includes understanding the goals, rules, data flows and interdependencies of the proposed system with existing systems in the mission context. It also includes cost/benefit trade-off analysis (the analysis of alternatives and business case analysis) to not only identify the preferred solution but also to quantify benefits of the proposed solution. The sponsoring component can accomplish this via business/system context diagrams, modeling, and data transaction diagrams to illustrate key attributes in context of the larger enterprise.

The phase begins with a Materiel Development Decision review led by the milestone decision authority. The purpose of the review is to gain approval for the Initial Capability Document and draft Concept of Operations resulting from the analysis of current mission performance and potential concepts across the DOD components, international systems from allies, and cooperative opportunities. Guidance for the analysis to be conducted during the phase is also approved. Approval of these documents is required for entrance into the phase.

The DOD component(s) accomplish cost/benefit analysis by balancing incremental investments with returned value (qualitative and quantitative results) that can offer accountability with stakeholders by tracking results over time. Analyses consider the probability and confidence levels of performance, scalability, cost growth, changes in commercial performance and standards, enterprise benefits, and range of uncertainty.

The Business Case Analysis and Development Phase exit criteria are met when the business case has been completed, materiel solution options for the

capability need identified, and the approved Initial Capability Document recommended.

Architecture Development and Risk Reduction

The purpose of the Architecture Development and Risk Reduction phase is to build the core architecture, demonstrate the architecturally significant features, and gain user support for the proposed conceptual technical solution. While the concept of prototyping begins during this phase, continuous prototyping activity is needed throughout the acquisition life cycle to assess the viability of technologies and minimize high-risk features while simultaneously refining user requirements. Therefore, it is expected that technology development and prototyping activity continues in support of follow-on releases and/or increments of capability. Completion of this phase of activity does not mean that a program has been initiated.

Entrance into this phase depends upon an approved business case including a proposed materiel solution(s), economic analysis, draft CDD, full funding for architecture development and risk reduction activities, and enterprise engineering artifacts highlighted in the earlier phase.

Activities in this phase begin with a decision review marking the formal entry point into architecture development and risk reduction. At this review, the milestone decision authority assures that the exit criteria of the Business Case Analysis and Development phase have been met and approves the proposed materiel solution and the technology development strategy, which describes the phase activities, funding, and objectives.

A System Requirements Document is developed based on capabilities outlined in the draft CDD. These prioritized requirements are subsequently time-boxed and decomposed into lower level requirements. A time-phased workload assessment is needed to identify the manpower and functional competency requirements for successful program execution and the associated staffing plan, including the roles of government and non-government personnel.

A list of known or probable Critical Program Information and potential countermeasures in the preferred system concept is also initiated during this phase. This activity is extended throughout the acquisition life-cycle to identify critical technologies and prototypes that may inform program protection and integration in subsequent acquisition activities.

Multiple risk reduction demonstrations focused on small subsets of functionality may be necessary before the user and developer agree that a proposed technology solution is affordable, militarily useful, enterprise aligned, and based on mature, demonstrated technology. (Enterprise alignment refers to synchronization and prioritization in terms of contribution of the larger environment.) Leveraging draft operational requirements, the program manager defines the system architecture, system-of-systems functionality and interfaces, and complete hardware and software detailed design for the system and increment.

The DOD component's CIO conducts IT maturity assessments against standards set by the American National Standards Institute, Institute of Electronic and Electrical Engineers, or The Open Group's Architectural Framework to assess the proposed solution and its ability to support an open architecture framework while addressing information security concerns. While the objective is to develop IT systems based on mature technologies, in rare instances where this may not be the case, the milestone decision authority, in consultation with the DOD CIO, determines whether TRAs and TRLs are necessary for acquisitions involved in fundamental advances in science and engineering underlying the cyber infrastructure and leap-ahead technologies (i.e., acquisitions truly involved in technology-push).

The Technology Development Strategy includes a description of how the materiel solution is divided into increments, releases, and capability iterations. It also includes strategies needed to rapidly incorporate technology solutions and establish the number of prototype units or engineering development models that may be produced in support of development and demonstration activities. The initial capability increment, including the sub-division of capability into releases, is to be defined by the Capability Development Document. Each release should not exceed approximately 18 months and should be further sub-divided into iterations (nominally three in number). Each iteration represents a subset of useful functionality that is tested and potentially deployable. Because of operational considerations, iterations are typically bundled together, operationally tested, and deployed via a release.

During Architecture Development and Risk Reduction, the user prepares the Capability Development Document to support the acquisition program. The CDD builds on the Initial Capability Document and provides the detailed operational performance parameters necessary to complete the proposed system design. These requirements are prioritized and parsed into groupings to establish

baselines for initial and subsequent releases. The program manager decomposes these operational requirements by translating the requirements into features of functionality. These features are further decomposed and prioritized into smaller units of functionality and incorporated into the Technology Development Strategy planning.

The project exits Architecture Development and Risk Reduction when an affordable program increment of militarily useful capability has been identified and approved by the proposed user; the technology approach for that program has been assessed; architectural and design risks have been identified and assessed; cost estimates are complete; and a system or increment can be developed within a short timeframe to achieve the time-certain mandates imposed by Congress.

Development and Demonstration

The purpose of the Development and Demonstration phase is to build and deliver operational capability for a discrete number of releases. Releases beyond that planned number restart the entire process and would typically be associated with a follow-on increment.

Entrance into this phase depends upon an approved CDD and proposed acquisition strategy and acquisition program baseline for "N" releases established at the Milestone Build Decision. As noted earlier, the requirements are prioritized and parsed into groupings to establish release baselines for the sub-programs. Likewise, appropriate planning documentation similar to those required for the current Milestone B decision is approved by the DOD component. In contrast to today's acquisition paradigm, these documents are considered "living documents" requiring updates at the end of a release. Finally, the program is fully funded; therefore, all releases for a given capability increment are fully funded at the Milestone Build Decision.

The Development and Demonstration Phase activities begin with a milestone decision review marking the successful completion of architecture development and risk reduction and commitment to develop and operationally field mission capability. At the Milestone Build Decision, the milestone decision authority approves the acquisition strategy and the acquisition program baseline, which is documented in a decision memorandum.

Leveraging the requirement priority set forth in the validation process, the program manager updates the architecture as necessary and completes design of the initial release with increasing level of detailed design associated with the first iteration. This includes system and system-of-systems functionality and interfaces, and complete hardware and software detailed design for the release. Also, the development of user training and implementation plans coordinated with the proposed releases are completed and verified through testing.

Following design activity, the development effort is focused at the iteration-level to produce system capability needed to satisfy approved requirements. Developmental test and evaluation is conducted to assess technical progress against critical technical parameters and, where appropriate, the use of modeling and simulation to demonstrate system and system-of-systems integration.

Following the nominal completion of three iterations, an Initial Operational Test and Evaluation (IOT&E) is accomplished prior to operationally fielding a release. An operational release is preceded by a decision from the milestone decision authority approving each release and follows successful IOT&E. IOT&E and fielding decisions are conducted for each release until the program satisfies the requirements for the increment.

Operations and Support

The Operations and Support phase provides materiel readiness and operational and user support over the total program life cycle. Training users in the new capability and providing support for initial use is critical to successfully fielding the capability. Training programs should be tested and evaluated to assure that they are comprehensive and effective. Life cycle sustainment planning and execution seamlessly span a system's entire life cycle. It translates force provider capability and performance requirements into tailored product support to achieve specified and evolving life cycle product support availability, reliability, and affordability parameters. Entrance into this phase depends on meeting the following criteria: an approved Life Cycle Support Plan and a successful Deployment Production Decision.

Subsequent Increments

Consistent with an evolutionary approach, multiple increments may be required to satisfy the capability need. In that case, each follow-on increment typically begins at the Milestone Development Decision and capitalizes on

continuous technology development and prototyping activity. Additional increments start the decision process again and must have approved requirements, be based upon mature technologies, have an acquisition strategy and baseline approved by the milestone decision authority, and be fully funded.

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 trade-offs for both hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in a 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 IT 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 IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the IT technology could otherwise be a few generations old at IOC.

While one could argue that this required new decision could add confusion to the process, 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.

Chapter 7. Summary and Recommendations

As stated at the outset of this report, IT acquisitions continue to grow in size, cost, and complexity, and the percentage of embedded IT in weapon systems is growing. Yet at the same time many IT acquisition programs have not met expectations and attempts to streamline the acquisition progress have not met with success. Cycle times continue to lengthen and costs increase. In the view of the task force, there are two chief causes for these circumstances: (1) there is not sufficient leadership with proven experience to structure executable programs and (2) the DOD IT acquisition process is inconsistent with the rapid pace of commercial IT technology cycles. DOD must take action to remedy these problems. Toward this end, this chapter summarizes the key findings and recommendations of the task force.

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 5000.2) are principally designed for programs where technology development for hardware and software is a critical component. The recent release of DOD Instruction 5000.02, implemented December 2008, offers 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 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 systems, embedded IT in weapon systems, and IT upgrades to fielded systems.
- Direct that **all** personnel within the Office of the Secretary of Defense, 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 USD (AT&L) should lead an effort, in conjunction with the Vice Chairman, Joint Chiefs of Staff, to develop new, streamlined agile capability (requirements) development and acquisition processes and associated policies for information technology programs.

The task force proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. The process is agile, 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 user (requirements) community throughout the acquisition process, with "capability needs" (vice requirements) constructed in an enterprise-wide context. It is envisioned that

requirements will evolve to "desired capabilities" that can be traded off against cost and IOC to get the best capability to the field in a timely manner. Systems analysis should be used to determine capability needs trade-offs rather than the typical functionality, cost, and IOC dates. 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 CIO, PA&E, DDR&E, OT&E, Comptroller, operational users, and others—need to be involved early and constructively in the process, prior to the milestone build decision.

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational testing 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—that will 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 this new process is continuity of funding, to maintain a solid funding stream for following, sometimes overlapping, capability releases. Along with the flexibility built into the process, relevant metrics need to be developed 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, the same is true for contactors. 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.

Implementation training for users is integral to the process. Training packages need to be designed and tested before each release. After fielding, testing of system effectiveness and the supporting training needs to be performed to provide feed-back to system developers.

The task force believes that 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 21). IT is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

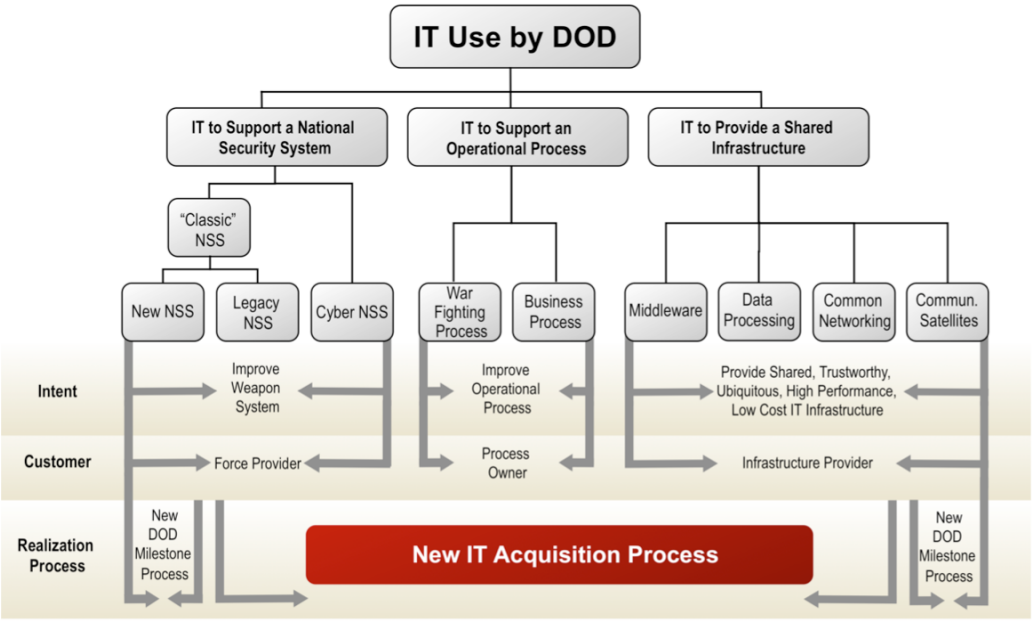


Figure 21. An Information Technology Acquisition Framework

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

The DOD CIO function is currently housed in the Office of the Assistant Secretary of Defense for Networks and Information Integration (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 ASD (NII)/DOD CIO reports directly to the Secretary of Defense—a reporting chain that the task force believes 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 authorities and responsibility for information policy vision, architecture, infrastructure, metadata and other 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 programs. However, the task force believes that some of the functions delineated here need to be strengthened in order to ensure that the full responsibilities of the office can be effectively executed.

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 must have strong authorities and responsibilities for enterprise-wide information policy vision, architecture, infrastructure, metadata 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 at 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.

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.

While not the centerpiece of this report, the task force believes that information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. IT 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 not only undermine 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 operate with degraded systems.

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 milestone decision authority consistent with program risk.

Furthermore, acquisition authority and expertise within OSD is currently spread across several organizations—under the USD (AT&L), the ASD (NII), and in the Business Transformation Agency—resulting in diffusion of capability and a competition among scarce resources. At the Service level, similar disaggregation of responsibility also exists. This disaggregated approach seems inefficient to the task force, 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 (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 acquisition programs is better understood. In addition to the matter of milestone decision authority responsibilities and organization, the Defense Acquisition Executive advisory staff (DDR&E, PA&E, OT&E, Comptroller, and others) 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 MDAP, MAIS, and special interest programs. The USD (AT&L) should:

- aggressively delegate milestone decision authority commensurate with program risk
- implement 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.[29]

29. We note that there was not a consensus view within the task force concerning this recommendation; a dissenting view is included in Appendix A.

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 report, but among these problems, lack of experience dominated. The Department has mechanisms to acquire experienced talent including the Intergovernmental Personnel Act and other special hiring authorities. In general the DSB has found that these programs are underutilized.

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 Executive (USD (AT&L)) and the component 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, in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

Conclusion

The task force believes that actions in these four areas will improve the acquisition of information technology in DOD: (1) acquisition policies and process, (2) roles and responsibilities of the CIO, (3) milestone decision authority roles and responsibilities, and (4) acquisition leadership expertise. But caution is offered that emphasis and focus only on the acquisition process is not enough. While the task force feels that a new process is needed that better takes into consideration the unique aspects of information technology, it 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.

Appendix A. Dissent to Report

I am gratified to see the changes to the original report which remove the recommendation to move NII under AT&L. However, having removed that recommendation, the report is not particularly consistent in other recommendations. Since NII will remain as a direct report to the Secretary of Defense, the lack of any discussion of using the Clinger-Cohen procedures to acquire IT systems is disturbing. I disagree that the DOD would be better served by not allowing the use of the alternative acquisition procedures available through Clinger-Cohen. The DOD could acquire IT systems in the context of Process Improvement where a business case is developed which combines Process Changes with IT acquisition. This would be particularly useful for the Business Transformation Agency programs. Today, Clinger-Cohen allows the Secretary of Defense to declare any IT program as a National Security System and leave only Clinger-Cohen requirements for meeting standards from that acquisition, so anything the report contemplates as an improvement by eliminating the Clinger-Cohen acquisition process can be done today, but the department will lose an alternative process to use when it is advantageous.

With only IT acquisition oversight of IT programs moving from NII to AT&L, the number of NII personnel who would transfer would be less than six. NII would have to have people reviewing the related programs in order to form advice on possible changes which would lead to a better integrated result. Budget reviews would still be required, Congressional interface would still be required, and there would be increased overlap in those functions between AT&L and the CIO. If so few people would move, then why move anybody? Such a recommendation is inconsistent with the dialog in the report suggesting that concentration of the few IT professionals in OSD is desirable. Perhaps a better recommendation would be for AT&L to reorganize within its resources to have a focal point for IT as it applies to embedded systems and those IT systems which are determined to be National Security Systems. That office could be the major coordination vehicle with NII to maximize the utility of the Clinger-Cohen process to areas where it might be more effective than use of the 5000 processes.

John Stenbit

Terms of Reference and Legislative Directive

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAY 01 2008

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on the Department of Defense Policies and Procedures for the Acquisition of Information Technology

In accordance with section 887 of the National Defense Authorization Act for FY 2008 (PL 106-65), you are requested to carry out a review of Department of Defense policies and procedures for the acquisition of information technology.

The purpose of the Task Force will be to determine whether existing acquisition policies and processes provide the foundation necessary for an effective acquisition model and to identify recommended improvements to enhance the Department's approach to information technology acquisition.

The matters addressed by the review shall include the following:

(1) Department of Defense policies and procedures for acquiring information technology, to include national security systems, major automated information systems and business information systems, and other information technology.

(2) The roles and responsibilities in implementing such policies and procedures of:

(a) The Under Secretary of Defense for Acquisition, Technology, and Logistics;
(b) Chief Information Officer of the Department of Defense;
(c) The Director of the Business Transformation Agency;
(d) The Service Acquisition Executives;
(e) The Chief Information Officers of the Military Departments;
(f) Defense Agency acquisition officials;
(g) The Information Officers of the Defense Agencies, and;
(h) The Director of Operational Test and Evaluation and the heads of the operational test organizations of the military departments and the Defense Agencies.

(3) The application of such policies and procedures to information technologies that are an integral part of critical weapons or weapons systems.

(4) The requirements of subtitle III of title 40, United States Code, and chapter 35 of title 44, United States Code, regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.

(5) Department of Defense policies and procedures for maximizing the usage of commercial information technology while ensuring the security of the microelectronics, software, and networks of the Department.

(6) The suitability of Department of Defense acquisition regulations, including Department of Defense Directive 5000.1, Department of Defense Instruction 5000.2, and the accompanying milestones, to the acquisition of information technology systems.

(7) The adequacy and transparency of metrics used by the Department of Defense for the acquisition of information technology systems.

(8) The effectiveness of existing statutory and regulatory reporting requirements for the acquisition of information technology systems.

(9) The adequacy of operational and development test resources (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of information technology systems both during development and before operational use.

(10) The appropriate policies and procedures for technology assessment, development, and operational testing for purposes of the adoption of commercial technologies into information technology systems.

A report will be submitted to the Secretary of Defense and Congress not later than January 28, 2009.

Where relevant, the Task Force should draw upon previous DSB reports to include the 2006 Summer Study on Information Management for Net Centric Operations, the Task Force reports of Mission Impact of Foreign Influence on DoD Software, and High Performance Microchip Supply.

The study will be sponsored by me as the USD(AT&L) and the ASD(NII). Dr. Ron Kerber and Mr. Vince Vitto will serve as the Task Force Chairpersons. Mr. Skip Hawthorne, OUSD(AT&L) will serve as the co- Executive Secretary and LTC Karen Walters, USA, will serve as the DSB representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

John J. Young, Jr.

110TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPORT
110–477

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2008

CONFERENCE REPORT

TO ACCOMPANY

H.R. 1585

DECEMBER 6, 2007.—Ordered to be printed

SEC. 887. DEFENSE SCIENCE BOARD REVIEW OF DEPARTMENT OF DEFENSE POLICIES AND PROCEDURES FOR THE ACQUISITION OF INFORMATION TECHNOLOGY.

(a) REVIEW REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall direct the Defense Science Board to carry out a review of Department of Defense policies and procedures for the acquisition of information technology.

(b) MATTERS TO BE ADDRESSED.—The matters addressed by the review required by subsection (a) shall include the following:

(1) Department of Defense policies and procedures for acquiring national security systems, business information systems, and other information technology.

(2) The roles and responsibilities in implementing such policies and procedures of—

(A) the Under Secretary of Defense for Acquisition, Technology, and Logistics;

(B) the Chief Information Officer of the Department of Defense;

(C) the Director of the Business Transformation Agency;

(D) the service acquisition executives;

(E) the chief information officers of the military departments;

(F) Defense Agency acquisition officials;

(G) the information officers of the Defense Agencies; and

(H) the Director of Operational Test and Evaluation and the heads of the operational test organizations of the military departments and the Defense Agencies.

(3) The application of such policies and procedures to information technologies that are an integral part of weapons or weapon systems.

(4) The requirements of subtitle III of title 40, United States Code, and chapter 35 of title 44, United States Code, regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.

(5) Department of Defense policies and procedures for maximizing the usage of commercial information technology while ensuring the security of the microelectronics, software, and networks of the Department.

(6) The suitability of Department of Defense acquisition regulations, including Department of Defense Directive 5000.1 and the accompanying milestones, to the acquisition of information technology systems.

(7) The adequacy and transparency of metrics used by the Department of Defense for the acquisition of information technology systems.

(8) The effectiveness of existing statutory and regulatory reporting requirements for the acquisition of information technology systems.

(9) The adequacy of operational and development test resources (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of information technology systems both during development and before operational use.

(10) The appropriate policies and procedures for technology assessment, development, and operational testing for purposes of the adoption of commercial technologies into information technology systems.

(c) REPORT REQUIRED.—Not later than one year after the date of enactment of this Act, the Secretary shall submit to the congressional defense committees a report on the results of the review required by subsection (a). The report shall include the findings and recommendations of the Defense Science Board pursuant to the review, including such recommendations for legislative or administrative action as the Board considers appropriate, together with any comments the Secretary considers appropriate.

Task Force Membership

CHAIRS

Name	Affiliation
Vincent Vitto*	Private Consultant
Ronald Kerber*	Private Consultant

MEMBERS

Priscilla Guthrie	Institute for Defense Analyses
Paul Hoeper	Private Consultant
Paul Kaminski*	Technovation
Tony Lengerich	Oracle
Noel Longuemare	Private Consultant
Mark Maybury	MITRE Corporation
Richard Roca	John Hopkins University–Applied Physics Lab
John Stenbit	Private Consultant
Alan Wade	Private Consultant

GOVERNMENT ADVISORS

Don Johnson	Office of the Assistant Secretary of Defense for Networks and Information Integration

EXECUTIVE SECRETARY

Skip Hawthorne	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

DSB REPRESENTATIVE

LTC Karen Walters, USA	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

STAFF

Barbara Bicksler	Strategic Analysis, Inc.
Teresa Kidwell	Strategic Analysis, Inc.

*Defense Science Board member

Presentations to the Task Force

Name	Topic
MAY 19-20, 2008	
Mr. Tim Harp DASD (C3ISR and IT Acquisition)	IT Acquisition/NII
Mr. Josh Hartman OUSD (AT&L)	IT Acquisition/AT&L
Mr. Dave Tillotson Deputy Chief of Warfighting Integration and Deputy Chief Information Officer, U.S. Air Force	IT Acquisition/Air Force
Robert S. Gorman General Counsel, DISA	IT Acquisition Policy and Procedures
LTG Jeff Sorenson Chief Information Officer, Army G-6	Supporting an Expeditionary Army at War
Honorable John Grimes Assistant Secretary of Defense for Networks and Information Integration and DOD Chief Information Officer	Discussion with DOD Chief Information Officer
Mr. Paul Ketrick Business Transformation Agency	Business Capability Lifecycle
Robert J. Carey Chief Information Officer in the Department of the Navy	IT Acquisition/Navy

JUNE 19-20, 2008

Lt Gen Charles Croom Director, Defense Information Systems Agency	IT Acquisition/ Defense Information Systems Agency
Mr. Dave Pratt SAIC	Service-Oriented Architecture Acquisition Working Group
RADM Hilarides Navy Program Executive Officer for Submarines	Rapid Capability Insertion Model
Mr. Don Johnson Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer	Alternative Model in Acquiring Information Technology
Mr. Richard Honneywell Electronic Systems Center, Wright Patterson Air Force Base	Information Technology Acquisition
Mr. Gary Winkler Army Program Executive Officer for Enterprise Information Systems	An Army Perspective on Information Technology Acquisition
Dr. Gary Federici and Mr. Carl Siel Department of the Navy	Law and Policy Implementation Challenges

AUGUST 6-7, 2008

Mr. Roy Evans MITRE Corporation	Rapidly Fielding Information Technology
Dr. Jacques Gansler	Integrating Commercial Systems

SEPTEMBER 16-17, 2008

Dr. Andre van Tilborg Deputy, Office of the Deputy Under Secretary of Defense for Science and Technology	Technology Readiness Assessments as Part of the DOD Acquisition Process
BGen Glenn M. Walters, USMC J8, Deputy Director for Resources and Acquisition Mr. William J. Cooper J8, Capabilities and Acquisition Division	JCIDS and Information Technology Requirements
Ms Regina Begliutti and Dr. Scott Comes Office of the Secretary of Defense, Program Analysis and Evaluation	Analysis of Alternatives Process for IT Systems
Col Ralph W. Harris Operational Test and Evaluation, DOT&E Dr. David Carlson Institute for Defense Analyses	Acquisition of Information Technology – Operational Test Considerations
Clark Reddick Director, C4ISR Technologies David Chaffee Director, Air Force and Agency Programs, Northrop Grumman	Transition to Open Systems
Mr. Gary Pennett Associate Director for Investment Office of the Under Secretary of Defense (Comptroller)	Planning, Programming, Budgeting and Execution Process
Jennifer S. Walsmith National Security Agency Central Security Service Senior Acquisition Executive	Agile Acquisition Process

Glossary

ACAT	acquisition category
AIS	automated information system
AoA	analysis of alternatives
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
CAE	component acquisition executive
CDD	Capabilities Development Document
CERT/CC	Computer Emergency Response Team Coordination Center
CIO	Chief Information Officer
COTS	commercial off-the-shelf
CVE	Common Vulnerabilities Enumeration
DAB	Defense Acquisition Board
DBSMC	Defense Business Systems Management Committee
DDR&E	Director of Defense Research and Engineering
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DSB	Defense Science Board
DT/OT	developmental test/operational test
DUSD (S&T)	Deputy Under Secretary of Defense for Science and Technology
EA	economic analysis
EDS	Electronic Data Systems
ESLOC	executable source lines of code
FY	fiscal year
GAO	General Accountability Office
GIG	Global Information Grid
ICD	Initial Capability Document
IOC	initial operational capability

IOT&E	Initial Operational Test and Evaluation
IRB	Investment Review Board
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITAB	Information Technology Acquisition Board
JCIDS	Joint Capability Integration and Development Systems
JCS	Joint Chiefs of Staff
JTRS	Joint Tactical Radio System
LOC	lines of code
MAIS	major automated information system
MBD	Milestone Build Decision
MDA	milestone decision authority
MDAP	major defense acquisition program
MDD	Materiel Development Decision
MRAP	Mine Resistant Ambush Protected
MUOS	Mobile User Objective System
NASA	National Aeronautics and Space Administration
NECC	Net-Enabled Command Capability
NII	Network and Information Integration
NMCI	Navy Marine Corp Intranet
NSS	national security systems
NVD	National Vulnerability Database
OASD (NII)	Office of the Assistant Secretary of Defense for Networks and Information Integration
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense
OSVDB	Open-Source Vulnerability Database
OT&E	Operational Test and Evaluation
PA&E	Program Analysis and Evaluation
QDR	Quadrennial Defense Review
RDT&E	research, development, test, and evaluation
SDD	System Development and Demonstration

SISOS	software intensive systems of systems
SLOC	source lines of code
SOA	service-oriented architecture
S&T	science and technology
TRA	Technology Readiness Assessment
TRL	technology readiness level
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics