Testimony

Before the Subcommittee on Military Readiness,
Committee on Armed Services, House of Representatives

DEFENSE INFORMATION MANAGEMENT

Continuing Implementation Challenges Highlight the Need for Improvement

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the Department of Defense's (DOD) effort to strengthen its information technology management processes. Defense invests about $11 billion annually in technology to support a wide range of activities, including military operations and maintenance, personnel management, health services, and routine business and financial management functions--and tens of billions more on technology supporting sophisticated weaponry. This reliance will only grow as the Department moves to modernize and respond to technological advances that are changing the traditional concepts of warfighting through improved intelligence and improved command and control.

However, DOD faces a number of serious management challenges to ensure that technology-driven processes and business systems provide an adequate level of service and an appropriate rate of return on investments. Namely, it has lacked effective fundamental management and oversight controls for assessing the costs and risks of proposed information technology projects; ensuring that projects follow departmentwide technical and data standards; measuring performance; and discontinuing projects shown to be technically flawed or not cost effective. Moreover, Defense faces a major challenge in removing long-standing organizational and cultural barriers to effective investment processes. This environment has consistently resulted in expensive system failures as well as systems that have not lived up to expectations.

In view of these problems, we designated Defense's management of information technology as a high-risk federal program in 1995. The House National Security Committee (now called the Armed Services Committee) subsequently required DOD to report on its efforts to address these weaknesses and implement the Clinger-Cohen Act, which was enacted in 1996 to strengthen agency information technology (IT) investment processes. My testimony today will focus on Defense's effort to respond to this requirement and strengthen its information technology management processes. In short, DOD's planned IT management reforms represent positive first steps toward strengthening the Department's decision-making and oversight environment for information technology projects. However, for this effort to succeed where others have failed, DOD will need substantial follow through to translate these plans into concrete improvements. This will require unwavering top-level commitment to

overcome both organizational resistance and to institute meaningful controls.

DOD's Management of Information Technology Is at High Risk

In 1995,[1] we designated DOD's effort[2] to streamline its business operations and deploy more efficient and less redundant standard information systems as a high-risk area, indicating that it was especially vulnerable to waste and mismanagement. At the time, Defense was spending some $3 billion annually to develop and modernize information systems, while major business processes supported by these systems--such as personnel, payroll, inventory management, supply distribution, and contract management— were not being examined for business process reengineering opportunities. Since then, we have continually reported that Defense has lacked management and oversight controls fundamental to ensuring the success of its IT investments. These include controls and processes for ensuring that the costs and risks of multimillion dollar projects are justified; monitoring progress and performance; and stopping projects shown to be cost ineffective or technically flawed.

Not surprisingly, DOD cannot show whether it has achieved significant results from its major technology investments. For example, in July 1998, we reported[3] that, because it failed to implement basic telecommunications management policies and develop objective performance measures, DOD was unable to eliminate costly duplication of its telecommunications networks and improve the effectiveness and efficiency of its communication services. In 1997, we reported[4] that, because Defense lacked an effective decision-making framework for consolidating, modernizing, and outsourcing computer center operations, its components had developed inconsistent and contradictory computer center strategies and the Department was foregoing opportunities to further reduce computer center expenditures.

---

[1]High Risk Series: An Overview (GAO/HR-95-1, February 1995).

[2]This was previously known as the Corporate Information Management (CIM) initiative.

[3]Defense Networks: Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals (GAO/AIMD-98-202, July 30, 1998).

[4]Defense IRM: Investments at Risk for DOD Computer Centers (GAO/AIMD-97-39, April 4, 1997).

Moreover, in a comprehensive review[5] of DOD's $18 billion effort to replace functionally duplicative and inefficient automated information systems with the best existing systems (known as the migration strategy), we found that Defense consistently failed to adhere to sound IT decision-making and oversight processes. For example, at the oversight level, systems that clearly lacked key pieces of technical, programmatic, and economic justification were allowed to go forward. At the decision-making level, many functional areas did not even bother to submit their systems or analyses that supported their decisions to department-level oversight controls. For instance, one functional area spent over $700 million pursuing a substantially flawed effort to develop a standard suite of materiel management systems—which was later abandoned—without rigorous department-level oversight. Our review also found that DOD lacked key cost, performance, and scheduling data that would enable Defense to convincingly demonstrate whether this decade-long effort had been successful or not.

This review, as well as many others, showed that perhaps the biggest impediment to successful IT projects is DOD's organizational environment, which has resisted departmentwide efforts to standardize business processes and information systems and to increase oversight and visibility over information resources. For example, the Department's Corporate Information Management initiative largely failed in meeting its original goals of bringing widespread efficiencies to its business processes because the Department could not overcome initial resistance to new ways of doing business. More recently, Defense civilian personnel management officials reported to us[6] that they did not consider several options that would radically change personnel management operations because the military services had a vested interest in maintaining the status quo even if those options offered opportunities for cost savings and increased operating efficiencies.

Many of Defense's fundamental IT management weaknesses were manifested in early efforts to solve the Year 2000 computing problem. When first confronted with the problem, Defense did not establish strong centralized oversight and management mechanisms, such as a Year 2000

---

[5]Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, October 20, 1997).

[6]Defense IRM: Alternatives Should Be Considered in Developing the New Civilian Personnel System (GAO/AIMD-99-20, January 27, 1999).

Program Office and a full-time Year 2000 executive and processes for validating information on component progress. And, initially, it did not develop a much needed detailed Year 2000 plan or guidance for developing interface agreements, conducting testing, remediating systems, and reporting on progress. Instead, Defense delegated responsibility for addressing the problem to its components. In turn, the components delegated this responsibility to subcomponents and likewise neglected to implement strong management and oversight controls. As a result we reported[7] that Defense was making inadequate progress in fixing its mission-critical systems and in mitigating Year 2000 risks, thus threatening its ability to carry out critical operations.

DOD has since implemented better controls and processes to strengthen its management over the Year 2000 problem and improved its progress in renovating systems. This has, however, taken extraordinary effort and serious Year 2000 risks remain. While major challenges still face the Department in addressing the problem, some of the hard lessons learned with respect to the Year 2000 project now offer avenues for longer term benefits to IT management.

Legislative Reforms Aimed at Addressing IT Management Weaknesses

Several recent management reforms, including revisions to the Paperwork Reduction Act, the Clinger-Cohen Act of 1996, the Government Performance and Results Act of 1993, the Federal Acquisition Streamlining Act of 1994, and the Chief Financial Officers Act of 1990, have introduced requirements emphasizing the need for federal agencies to significantly improve their management processes, including how they select and manage IT resources. For instance, a key goal of the Clinger-Cohen Act is that agencies should have processes and information in place to help ensure that IT projects are being implemented at acceptable costs, within reasonable and expected time frames, and are contributing to tangible, observable improvements in mission performance. Moreover, these agency processes should be institutionalized throughout the organization, and should be used for all IT-related decisions. The ultimate goal of these various legislative reforms is for DOD and other agencies to make better decisions that will measurably increase the performance of the organization.

---

[7] Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

DOD's Required Report Shows Progress, But Concerns Remain

In view of Defense's long-standing information technology management weaknesses and reforms called for by Clinger-Cohen and related legislation, the Committee required DOD, by December 1, 1998, to review and report on its efforts to improve IT management. The Committee specifically asked that DOD's report include a review of the following.

1. DOD's overall information technology management strategic plan, including any service and agency subsets.

2. Performance measures and plans for implementing them.

3. Barriers to achieving the goals of the information management strategic plan and performance measures.

4. Policies and directives for implementing IT management reforms required by the Clinger-Cohen Act.

5. Actions taken to integrate the Clinger-Cohen Act reforms into DOD's existing Planning, Programming, and Budgeting System (PPBS).

6. Actions taken on the GAO recommendations contained in its report on DOD's system migration strategy for improving DOD's management controls over investments in national security systems and combat support (administrative) systems.

7. DOD's plans to perform vulnerability assessment and operational testing for Year 2000 compliance or contingency plans.

DOD's subsequent report to the Committee responded to the first six areas of concern and outlined the Department's plans to improve IT management in most of these areas. According to Defense, plans for testing of Year 2000 compliance and contingency plans will be discussed in a separate report to the Committee.[8]

Our analysis of these plans and initial actions taken by the Department shows that, for the most part, they represent good first steps toward strengthening decision-making and oversight processes for IT. However, it

---

[8]See <u>Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises</u> (GAO/AIMD-99-52R, January 29, 1999) for more information about the Committee's requirement with respect to Year 2000 vulnerability assessments and operational testing.

is still very premature to determine whether Defense can overcome its cultural inertia and go beyond these first steps. Also, important management areas have not been adequately addressed, particularly with respect to performance measurement and capital planning and investment control.

DOD's IT Management Strategic Plan

Almost every organization has mission and information planning processes and plans. But the most effective strategic business and information management planning processes are both tightly linked and anchored, not to bureaucratic requirements, but to explicit goals that meet external needs. For this reason, the Paperwork Reduction Act requires each agency to develop and maintain a strategic information management plan on how information management activities help accomplish agency missions.

DOD's report states that the Department (1) developed an information management strategic plan in March 1997 to ensure that IT investments maintain a strategic business and mission focus and (2) completed its first information management strategic planning cycle. Among other things, DOD indicates that the strategic plan represents the DOD Chief Information Officer's (CIO) "high-level vision and direction for the Department as a whole, with cross-cutting [CIO] goals, objectives, strategies, and performance measures that support all missions, functions, and organizations." The new DOD-wide information management strategic planning process and the issuance of the DOD CIO strategic plan should facilitate coordination and integration of IT-related efforts among the military services and Defense agencies.

DOD's report stated that a revised draft of the strategic plan, which is due to be approved for issuance around the end of this month, is better linked to the strategies of, among other things, DOD's overall strategic plan—the May 1997 Report of the Quadrennial Defense Review. CIO office officials also stated that their IT strategic planning has been broadly inclusive of other DOD organizations and components. These are positive developments addressing concerns we have raised in the past.

Nevertheless, DOD CIO officials deleted from the revised draft of the strategic plan the "outcome" and "outcome performance indicators" subsections that were included under each of the four goals in the March 1997 strategic plan. The specific and trackable information previously provided has been replaced by an appendix discussing IT performance

measures in much more general, and less useful, terms. DOD CIO officials were unresponsive to our inquiries about their reasons for this change.

Moreover, the plan does not identify the DOD resources needed to achieve DOD's goals and objectives. Rather, it makes clear that it is up to the DOD components and the PPBS process to provide for the resources needed to achieve the DOD-wide plan's goals and objectives. Our review of four components' information management strategic or implementation plans-- those of the three military departments and the Defense Information Systems Agency (DISA)—also showed that none of these plans identified the resources needed to carry out the DOD-wide plans. The Army's plan predates the DOD-wide strategic plan and, therefore, did not make any specific reference to it. Based on our best practices research in this area, we know that successful IT planning depends on keeping a mission and strategic business focus and integrating needs across functional areas and missions. Thus, it is critical that DOD's component strategic plans link to the overall plan and that components provide adequate resources to fund IT efforts.

DOD's IT Investment and Performance Measurement Approach

Many of the problems we identified in our earlier reviews of DOD's IT efforts are rooted in the fact that DOD's management and oversight processes over IT projects are not effectively integrated to enable the Department to manage from a portfolio perspective. Considering investments as a total package of possible projects is important because it forces an agency to decide which projects are the most critical to meeting mission needs and thus should receive the most resources and attention. Moreover, we have found that because DOD lacked IT performance measures, senior managers could not begin to compare results being achieved against projected costs, benefits, and risks.

DOD's December 1, 1998, report recognizes these problems and, toward this end, states that the department has been "significantly reorganized to more effectively measure DOD information technology performance within the context of functional mission outcomes." A single Directorate, under the DOD Deputy CIO, for example, has been established to (1) promulgate performance measurement guidance and (2) incorporate performance measurement as the cornerstone for IT investment portfolio oversight and outcome-based programming and budget assessments for the CIO and the Chief Financial Officer.

The Office of the DOD CIO is also developing an IT investment portfolio (ITIP) oversight approach that is intended to (1) provide the DOD CIO with better information to support management and investment decisions and fully implement IT performance measurement in the Department, (2) assist functional managers in building and managing IT portfolios consistent with strategic visions, goals, and measures of performance, and (3) assist program managers in effectively managing performance, cost, and schedule risks in the acquisition of IT that supports functional mission needs and strategic plans.

According to DOD, a DOD team has developed a draft ITIP template, which will be validated during 1999 through pilot programs, with the eventual goal of adopting it for departmental use. According to DOD CIO officials, the Department is about to establish a DOD-wide working-level integrated process team to implement the ITIP oversight approach.

We believe that these efforts have the potential to improve the allocation of IT resources and visibility over IT investments. They can also put DOD in a better position to effectively implement requirements of the reform legislation. Nevertheless, Defense has been slow to implement these changes-- it has been almost 3 years since the Clinger-Cohen Act was enacted and the approach is still being designed and pilot tested. Moreover, because effective portfolio management will require DOD to overcome cultural barriers to change, it remains uncertain whether DOD can achieve the support needed to institute this new program.

Barriers to Achieving the Goals of the IT Strategic Plan

DOD's December report contained only a single paragraph addressing cultural barriers to change and did not provide any specifics on how these impediments will be overcome. Although they cited "many" DOD reform initiatives which should help address this problem, DOD officials offered little more in the way of specifics of how these barriers will be removed or how DOD's progress with respect to doing so will be measured.

As noted in our previous reports, the biggest challenge to effective IT management in DOD is the prevailing organizational structure and embedded culture found throughout the Department. Specifically, the three military services have clearly defined roles and responsibilities and separate budget authority, program execution, and functional authority for the enforcement of national defense policy and objectives. This environment has promoted stovepipe systems solutions in each component and made it difficult to implement departmentwide oversight or visibility

over information resources. Until DOD can specifically address how these barriers will be overcome, successful implementation of its IT management reforms will remain in doubt.

Department Directives and Policies Issued to Implement IT Reforms

Policies and procedures are essential to executing management reform. They provide essential clarity, purpose, direction, and instill authority and accountability for managing an organization in an effective manner. The DOD report calls attention to a June 2, 1997, memorandum, in which the Secretary of Defense clarified the DOD CIO's responsibilities for implementing the IT-related requirements of the Clinger-Cohen Act. It directed that the CIO promote improvements to work processes and supporting information resources.

The DOD report states that (1) its recent reorganization created an Information Policy Directorate within the Office of the Deputy CIO/Deputy Assistant Secretary of Defense (Implementation and Policy), which, since its creation in mid-1998, has focused on ways to quickly issue new policies and purge old ones, (2) the CIO has developed a common framework for updating IT management policies around the achievement of information superiority (a Joint Vision 2010 goal), more directly linking IT with the mission, and (3) policies are being reviewed and updated or eliminated and directive-type memoranda are being used to issue policy guidance more quickly, working with those who must apply these reformed policies.

DOD CIO officials emphasized that DOD's new approach is to more quickly coordinate and issue shorter guidance and policy memorandum (that is, within 6 to 8 weeks, 3 months at most). A memoranda describing the general approach to issuing timely guidance over the next several months was issued by the DOD CIO on November 9, 1998. And, Defense is in the process of developing guidance for electronic commerce, the Defense Messaging System and Information Interoperability and Integration. It also expects to issue a memorandum to replace the "capstone" IT management directive (Directive 8000.1) by August 1, 1999. CIO officials told us that various offices and study groups are planning to develop numerous other directives including ones that address IT investment portfolio implementation, architectures, and enterprise software. However, they could not estimate how many of these would be issued this year.

Defense's plans do not yet call for guidance in some key areas. For example, it does not plan to issue guidance on preparing economic analyses even though DOD itself has acknowledged the need for consistent

and standard techniques in preparing economic analyses to support a portfolio management approach to IT.

Our analysis indicates that, within the past year, the DOD CIO has initiated a major collaborative effort with various military services and defense agencies to improve written IT management policies. These policy improvement steps, and their collaborative nature, are encouraging. However, few results have accrued from this collaborative effort. This opinion is buttressed by a statement made last November by the CIO that many of DOD's IT management policies "have not kept pace" with legislative and technological changes or DOD's priorities and needlessly complicate DOD's achievement of its goals.

Integrating IT Capital Planning and Investment Control Processes into PPBS

Our best practices research,[9] which helped form the basis for many of the Clinger-Cohen IT management reforms, emphasized the need for integrated planning, budgeting, and performance measurement. This helps organizations to never lose sight of critical information systems projects and to treat them consistently throughout sometimes disparate management processes.

At DOD, the Planning, Programming, and Budgeting System (PPBS), along with DOD requirements and acquisition processes, is intended to integrate, among other things, budgeting and IT investment management. Over the past year, DOD and its component processes have been reviewed and changes have been made in PPBS to ensure full participation of the DOD CIO in the Department's decision-making process. For example, the DOD CIO now participates as a full member on two important DOD management bodies--the Defense Resources Board (DRB) and the Defense Planning Advisory Group (DPAG). The DRB, chaired by the Deputy Secretary of Defense, is the senior DOD group that advises the Secretary and Deputy Secretary on major programming decisions which provide the basis for the military services' and defense agencies' budget estimates. The DPAG is responsible for the developing the guidance that supports and facilitates budget preparation. DOD's report stated that the DOD CIO's membership on the DRB should ensure that the CIO's position is heard in all budget deliberations.

---

[9]Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994).

These changes should help to elevate top management visibility into IT management in the Department. However, DOD CIO officials we spoke with indicated that the PPBS processes do not fully meet the Clinger-Cohen Act requirements. For example, PPBS decision-making processes are not based on consideration of defined selection criteria nor do they provide the quantifiable measurements of progress, timeliness, and results to senior executives required by the Clinger-Cohen Act.

Actions Taken to Improve Management Controls Over IT Investments

In our report on DOD's migration strategy, we made a number of recommendations aimed at ensuring that DOD's continued investment in migration systems provided measurable improvements in mission-related and administrative processes. For example, we recommended that Defense require its components to rank development/modernization systems justifications and complete them on an expedited basis. We also recommended that the CIO certify that these justifications include (1) an analysis of operational alternatives that clearly demonstrates that continuing with migration is the best solution for improving performance and reducing costs in the functional area, (2) an economic analysis showing a return on investment or other mission benefits that justify further investment, and (3) documentation showing that the system currently complies with applicable Defense technical standards and uses standard data. Additionally, we made recommendations aimed at correcting weaknesses within the current life-cycle management environment and ensuring the successful reengineering of processes and implementing of corporate information systems for functional areas. Defense generally concurred with these recommendations and agreed to implement corrective actions.

However, Defense has made little progress in addressing our recommendations. While Defense's plans to reform IT management have potential for addressing some of the weaknesses we identified in our report, nothing has actually been fully implemented to address our concerns. Furthermore, in December 1998, DOD indicated that it no longer concurred with the recommendations aimed at improving the quality of data in the Defense Integration Support Tools (DIST)--a system which served as the department's inventory for information systems--because it stopped using this system and undertook other efforts to improve inventory-related data. The lack of complete and accurate system inventory data was a major problem impeding Defense's early Year 2000 efforts to complete assessments and estimate costs.

Our recommendations were aimed not only at bringing meaningful change to the current decision-making and oversight environment for migration, but to facilitate DOD's implementation of the Clinger-Cohen Act and to rectify the weaknesses that pervade a broad spectrum of DOD's IT efforts, including management of telecommunications networks, computer systems, and the Year 2000 program. The Department's failure to implement our recommendations serves to limit its ability to comply with basic tenets of good information management practices and the specific requirements of the Clinger-Cohen Act.

Year 2000 Offers Another Avenue for Making Long-Term Improvements

As mentioned earlier, when first confronted with the Year 2000 problem, Defense's long-standing IT management weaknesses made it difficult for the Department to lay the groundwork for effective planning and oversight. Nevertheless, out of necessity, the Department has learned that a business-as-usual approach will not work for a problem as pervasive as Year 2000. In turn, Defense has had to implement new mechanisms and management approaches that could well be applied to longer term technology management efforts. For example:

- Defense has learned that Year 2000 efforts cannot succeed without the involvement of top-level managers, including the Deputy Secretary, senior information management officials, the Comptroller, the principal staff assistants, and decisionmakers at Defense components. Best practices have shown that top executives need to be similarly engaged in periodic assessments of major information technology investments in order to prioritize projects and make sound funding decisions.
- Defense has realized that having a complete and accurate enterprisewide information systems inventory can facilitate remediation, testing, and validation efforts. Having a reliable system inventory is also fundamental to well-managed information technology programs since it can provide senior managers with timely and accurate information on system costs, schedule, and performance.
- Defense has spent 3 years identifying system interfaces and implementing interface controls at the system level to prevent proliferation of Year 2000 problems between systems. This effort should help Defense prevent future data exchange problems in its systems and resolve conflicts between interface partners.
- Defense has made some progress in identifying and prioritizing its mission-critical systems and is expected to further prioritize as operational and functional evaluations highlight the "thin line" systems that are truly critical to Defense operations. Once the Year 2000 effort is

completed, Defense can use this information to further identify and retire duplicative or unproductive systems.

In short, it is clear that DOD has a significant opportunity to institutionalize some valuable lessons learned from its Year 2000 experience—namely, involving top managers in IT decisions and establishing good visibility over systems. By applying these lessons learned to its overall IT efforts, DOD will be better positioned to acquire and deploy high performing, cost-effective systems; avoid repeating costly mistakes; and ensure an adequate return from its multibillion dollar IT investments.

Conclusions

DOD is making progress in its attempts to improve its IT management processes in concert with recent governmentwide IT management reforms. However, it is unlikely that these initial steps will develop into meaningful, tangible reform of DOD's information management processes and achieve real impact over the selection and control of its technology investments without confronting fundamental management issues that continue to plague the Department. These issues center around the very real cultural barriers that limit effective management initiatives within the Department and the lack of well-defined processes, disciplined management, and sustained top management attention required to overcome those barriers. The Department's recent experiences with its Year 2000 efforts should serve as an example that consistent—and persistent—attention by top management can make a significant difference. If these lessons can be applied to other aspects of IT management and backed by good processes and reasonable controls, then the Department will be poised to harvest significant returns from its investment dollars.

Mr. Chairman, this concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.