Testimony

STATEMENT OF
ROBERT J. LIEBERMAN
DEPUTY INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
BEFORE THE
SENATE COMMITTEE ON BUDGET
ON
DEFENSE MANAGEMENT ISSUES

Report No. D-2001-050 DELIVERED: February 12, 2001

Office of the Inspector General
Department of Defense

Mr. Chairman and Members of the Committee:

I am pleased to be here this afternoon to discuss the management challenges facing the Department of Defense, from the standpoint of its internal auditors and investigators. My testimony will summarize and update the written analysis that we provided to you and other congressional leaders last December 1.[*] In that analysis, we identified 10 areas, each containing multiple significant challenges.

Information Technology Management

The other witnesses before you today have written eloquently on the Revolution in Military Affairs brought on by rapidly advancing technologies related to computing, communications and sensors. It is equally true that information systems are now as crucial to DoD management activities as the central nervous system is to the human body. Managers at all levels, regardless of their functions, depend on information that is compiled, analyzed, adjusted and reported with automated systems. During the Year 2000 computer conversion project, approximately 10,000 DoD computer networks were inventoried and the true extent of

[*] The letters of December 1, 2000 and the last several Inspector General Semiannual Reports to the Congress, which contain similar analyses of high risk areas, are available on-line at www.dodig.osd.mil.

the Department's dependence on those systems became well understood for the first time. The magnitude of DoD spending on information technology is less well understood, but clearly it far exceeds $20 billion annually.

Given the considerable dependence on "IT" and the high cost of large system investments, the historically poor record of the DoD for controlling the proliferation of incompatible systems with nonstandard data elements, acquiring new systems that meet user needs within reasonable timeframes, controlling cost, and ensuring the quality and security of data has been a major concern. Recognizing that such problems are common across the Federal Government, the Congress specified in the Clinger-Cohen Act of 1996 that Chief Information Officers in each agency would oversee well disciplined information technology acquisition processes. This is a daunting challenge for a department with 71 major information system acquisition projects and hundreds of "smaller" system acquisition and modification projects belonging to dozens of organizations. The DoD has been candid about the need for more effective management controls in this crucial area, but progress has been slow and the goals of the Clinger-Cohen Act have not yet been achieved.

I have mentioned the challenge of information system investments first because information problems are at the root of a very large number of DoD management problems, ranging from the inability to compile accurate financial reports to poor supply inventory management practices.

The Department has revised its basic information system acquisition procedures and been responsive to our recommendations. Nevertheless, we believe this area deserves heavy oversight emphasis as it continues to evolve. At the present time, virtually every information technology project that we audit exhibits significant management problems. The most common failing is poorly defined requirements for the system.

Information System Security

Another facet of information technology management is assuring the security of DoD systems and information. Guarding against the interception of military signals is an age-old problem and, until recently, was chiefly the province of the cryptographers. Although the DoD must always maintain tight security for its classified systems, the past few years have seen the massive expansion of networked and unclassified DoD information systems.

In turn, this expanded DoD presence on the Internet has led to a proliferation of attacks and intrusions.

Network intrusion poses a multifaceted threat to national security that cuts across society's boundaries: it potentially affects both the public and private sectors, cuts across national boundaries, and can cause problems in virtually all economic sectors and levels of government. To organizations, the threat is both internal and external, and constantly evolves. Perpetrators can include disgruntled or irresponsible employees, criminals, hobbyist hackers, agents of hostile states and terrorists.

Recent audits indicate that much more needs to be done to implement the Defense Information Assurance Program fully and to sustain a robust effort indefinitely, as 21st Century realities will demand. Although it was widely assumed that the successful management approaches and mechanisms developed to overcome the "Y2K" problem would be readily transferable to the information assurance challenge, this has occurred to a very limited extent. The strongest part of the DoD effort currently is in the areas of intrusion detection and incident response. Several Defense Criminal Investigative Service agents, from my office, are an integral component of the Joint Task Force on Computer Network

Defense, which gives DoD a powerful capability and is an excellent example of cooperation between the DoD information security and Federal law enforcement communities. Consistent policies, procedures, training and assessments in DoD computing centers and among system users remain weaker areas. In that regard, the Government Information Security Reform provisions of the National Defense Authorization Act for Fiscal Year 2001, which mandate annual information assurance assessments and IG validation audits in Federal agencies, should be very helpful in terms of focusing management attention on this problem area.

Other Security Concerns

In addition to the threat posed by unauthorized intrusion into DoD information systems, a wide range of other security issues confront the DoD. Those threats include terrorism against U.S. personnel and facilities, conducted by either conventional or non-conventional means, and the disclosure or theft of sensitive military technology. The recent terrorist attack on the USS COLE in Yemen and security breaches at the Department of Energy, the Central Intelligence Agency and DoD graphically demonstrated that security vulnerabilities need to be matters of utmost concern.

Recent audits have indicated that the DoD needs to improve security measures to guard against both internal and external threats. We have not audited force protection issues, but we have extensively reviewed a number of other areas where unacceptable vulnerability exists. These include the Defense Personnel Security Program, which by 1998 had allowed hundreds of thousands of overdue security clearance requests to accumulate. The Department took aggressive measures during 2000 to address productivity and resource problems at the Defense Security Service (DSS), with mixed success to date. In April 2000, the DSS estimated that it would reduce the number of pending cases to about 260,000 by now. As of January 31, 2001, however, there were 442,643 cases pending in DSS and 45,128 more pending at the Office of Personnel Management. It likely will take at least two years to achieve reasonable average turnaround times for security clearance investigations and further attention to the clearance adjudication process also is warranted.

Similarly, there is a consensus in the Executive Branch and Congress that the export license regime of the 1990's was inefficient and probably ineffective in controlling the unintended loss of U.S. military technology. During 2000, the DoD worked with other Federal agencies to streamline the

licensing processes and approved additional resources to improve the speed and value of license application reviews. The task of determining to what extent the fundamental national export control policies need to change, however, remains unfinished business for the new Administration and Congress.

It is important to view security as a paramount consideration for virtually all DoD programs and operations. Issues such as properly demilitarizing military equipment before disposal and controlling the access of contractors and visitors to technical information at military engineering organizations and laboratories need more attention. We are monitoring DoD implementation of numerous agreed-upon audit recommendations on these matters.

Financial Management

The DoD remains unable to comply with the requirements in the Chief Financial Officers Act of 1990 and related legislation for auditable annual financial statements. The results of audits of the DoD-wide and other major financial statements for FY 1999 were essentially the same as in previous years. The Military Retirement Fund statements received a clean audit opinion, but all other DoD financial statements were unauditable. We have not yet issued the audit opinions on the financial statements

for FY 2000, but there will be no significant change in those bleak outcomes. Previous DoD goals for obtaining clean opinions on all or most annual statements during the FY 2000 timeframe were unrealistic and it is unclear what a realistic goal would be at this point. A few relatively small DoD organizations and funds may achieve favorable opinions in the near future, but the major funds still pose a formidable challenge. The root problem is that DOD lacks modern, integrated information systems that can compile auditable financial statements. The Department also has major concerns that the Federal Accounting Standards Advisory Board could issue additional guidance that would further complicate this challenge.

During the past year, the DoD made hopeful progress in addressing major impediments to favorable audit opinions. These problems cannot be solved quickly and some could not be addressed until new Federal accounting standards were issued and interpreted, which is still an incomplete process and is not controlled by DoD. Policies were issued to implement several new accounting standards and more contractors were engaged to provide their expertise on a variety of issues, such as determining the value of different categories of property.

Most importantly, the Department took steps to apply the lessons learned from the successful DoD Y2K conversion program to the financial system compliance effort. The DoD Senior Financial Management Council, which had not met for several years, was reconstituted to ensure senior management control. A comprehensive program management plan was issued on January 5, 2001.

We strongly recommended this initiative. Indeed, I believe it is the most heartening development in this area in several years. I urge the new Administration and Congress to support this adaptation of the successful Y2K management approach to the somewhat similar information systems challenge involved in attaining CFO Act compliance.

One of the benefits of using the Y2K management approach for financial systems compliance is that it provides good metrics for the most important aspect of the DoD financial management improvement effort. As welcome as those metrics will be for measuring system compliance status, however, even they will not measure the usefulness of the data to managers, appropriators or budget committees. Numerous recent statements and testimony to Congress by the Office of Management and Budget, GAO and DoD officials have stressed that the ultimate goal of financial

management reform legislation is ensuring useful financial information for sound decision-making by managers throughout the year, not merely clean audit opinions on annual financial statements. We agree. Audit opinions are a simple and readily understandable metric, but judging the usefulness of financial information is far more difficult. Likewise, audit opinions on financial statements provide little insight into the efficiency of functions such as paying contractors or capturing the cost of operations of individual bases and work units. The DoD has long-standing deficiencies in both of those areas.

Acquisition

The DoD is working toward the goal of becoming a world-class buyer of best value goods and services from a globally competitive industrial base. The Department hopes to achieve this transformation through rapid insertion of commercial practices and technology, business process improvement, creating a workforce that is continuously retrained to operate in new environments, and heavily emphasizing faster delivery of material and services to users. In order to fulfill these objectives, the DoD has initiated an unprecedented number of major improvement efforts, including at least 40 significant acquisition reform initiatives.

Despite some successes and continued promises from ongoing reforms, the business of creating and sustaining the world's most powerful military force remains expensive and vulnerable to fraud, waste and mismanagement. In FY 2000, the DoD bought about $156 billion in goods and services, with 15 million purchasing actions. The Department currently is attempting to stretch its acquisition budgets across 71 major programs, estimated to cost $782 billion, and 1,223 smaller programs worth $632 billion.

The scope, complexity, variety and frequent instability of Defense acquisition programs pose particularly daunting management challenges. Aggressive acquisition cost reduction goals have been established, but it is too soon to tell if they are achievable. Many specific initiatives have not yet been fully implemented and are in a developmental or pilot demonstration phase.

In the push to streamline procedures and incorporate commercial practices and products, the Department cannot compromise its insistence on quality products and services at fair and reasonable prices. An inherent challenge throughout the Department's acquisition reform effort is ensuring that critically needed controls remain in place and there is proper

oversight and feedback on new processes. Recent audits continued to indicate a lack of effective means for identifying best commercial practices and adapting them to the public sector; overpricing of spare parts; inattention to good business practices and regulations when purchasing services; poor oversight of the several hundred medium and small acquisition programs; and adverse consequences from cutting the acquisition workforce in half without a proportional decrease in workload.

Although the DoD must continue to address the challenges of how to control the cost of purchased goods and services, the most fundamental acquisition issues confronting the Department relate to requirements and funding. The expanding national dialogue on military missions, the Quadrennial Defense Review and actions by the new Administration and Congress will probably alter DoD missions, military force structure and acquisition requirements. Whether changes in requirements and the topline budget are major or minor, there needs to be a far-reaching rebalancing of acquisition programs to match available funding.

Finally, we believe that the Department needs to put more acquisition reform emphasis on ensuring the quality, serviceability and safety of purchased equipment, parts and supplies. Concentrating on prices and timely delivery is vital,

but quality should be the most important attribute for DoD purchases, especially for materiel used by the warfighters. Minimizing vulnerability to fraud, especially false statements regarding product testing and product substitution, remains imperative. We currently have nearly 700 open procurement fraud investigations and we achieved 134 convictions, with recoveries of $170 million, in this area during FY 2000.

Health Care

The Military Health System (MHS) costs over $20 billion annually and serves approximately 8.2 million eligible beneficiaries through its health care delivery program TRICARE. TRICARE provides health care through a combination of direct care at Military Department hospitals and clinics and purchased care through managed care support contracts. The MHS has dual missions to support wartime deployments (readiness) and provide health care during peacetime.

The MHS faces three major challenges: cost containment, transitioning to managed care, and data integrity. These challenges are complicated by the inadequate information systems available to support the MHS.

Cost containment within the MHS is challenged by the continued lack of good cost information and significant levels of health care fraud. Lack of comprehensive patient-level cost data has made decisions on whether to purchase health care or provide the care at the military treatment facility more difficult. Recent legislation, which expands medical benefits for eligible beneficiaries, will entail considerable program growth in an area where cost control has been difficult.

To combat health care fraud, the Defense Criminal Investigative Service has developed an active partnership with the TRICARE Management Activity to give high priority to health care fraud cases, which comprise a growing portion of the overall investigative workload. We have about 500 open criminal cases in this area. In FY 2000, our investigations led to 94 convictions and $529 million in recoveries.

Supply Inventory Management

Supply management to support U.S. military forces, which are located around the world and use several million different types of weapon systems, other equipment, spare parts, fuel, apparel, food items, pharmaceuticals and other supplies, may be the most difficult logistics challenge in the world. Despite the clear need to modernize DoD supply operations, it should be noted that

U.S. military logistics performance has been excellent in demanding situations such as recent deployments to comparatively remote areas of the world.

Every facet of supply management involves challenges and it is critically important to recognize that weapon systems and other equipment must be designed, selected and procured with logistics support as a paramount concern. The use of standardized parts, commercial items, non-hazardous materials and easy to maintain components will considerably ease the supply support problem for each system or piece of equipment. Conversely, inattention to such factors during acquisition will increase the risk of higher costs and logistics failures.

The logistics community relies heavily on program managers and operators to help forecast supply requirements, and historically this has been very difficult. The Department has been justifiably criticized for accumulating excessive supply inventories, but supply shortfalls are at least as great a concern due to the impact on readiness. Current logistics reform initiatives are principally focused on introducing private sector logistics support practices, which in turn are based on applied web-based technology. The DoD has initiated a myriad of logistics improvement initiatives, most of which are

still in early stages. We anticipate continuing valid concerns about all phases of supply support, including requirements determination, procurement, distribution, and disposal.

Other Infrastructure Issues

Despite numerous management initiatives to reduce support costs so that more funds could be applied to recapitalizing and ensuring the readiness of military forces, more can and should be done. Organizations throughout the Department need to continue reengineering their business processes and striving for greater administrative efficiency.

Unfortunately, cutting support costs can easily become counterproductive if the quality of support services and facilities is degraded. In addition, there are numerous bona fide requirements in the support area that will be expensive to address. For example, the average age of structures on military installations is 41 years and wholesale recapitalization is needed. In the category of family housing alone, a third of the 285,000 units require replacement in the next several years. The backlog of real property maintenance is $27.2 billion.

Three areas hold the most promise for reducing installation level costs: base closures, public/private competition for

activities like base maintenance, and measures to avoid hazardous material handling and cleanup costs through better up-front planning. Unfortunately, progress in all three areas is difficult because of controversy about the validity of data used by decision-makers or their objectivity.

Readiness

Concern about the readiness of U.S. military forces was a principal issue last year in congressional hearings and was addressed during the Presidential election campaign. There is a fairly broad consensus that readiness shortfalls exist, although the extent of impairment to mission capability is more contentious. Clearly, there are spare parts shortages; significant backlogs for depot maintenance ($1.2 billion); concerns related to recruiting, retention and morale; disproportionately numerous deployments for some units; unanticipatedly high operating tempo; and equipment availability problems. In response, the DoD and Congress have made major budget adjustments and military entitlements have been expanded. The Department's readiness posture ultimately depends, however, on the effectiveness of hundreds of support programs, which range from training to supply management.

The DoD audit community supported the successful program to overcome the Year 2000 computer challenge, which the Department considered to be a major readiness issue, with the largest audit effort in DoD history. The IG, DoD, issued 185 "Y2K" reports. Due to that massive commitment, resource constraints and other workload, our recent coverage of other readiness issues was severely limited. We plan to restore at least some of the necessary coverage during FY 2001, continuing our particular concentration on chemical and biological defense matters. On January 31, for example, we issued a report on the establishment of National Guard Weapons of Mass Destruction-Civil Support Teams. The audit indicated they were not yet ready for certification as mission-ready. We are working with the involved DoD organizations to ensure that the concerns related to those certifications are expeditiously and fully addressed.

Human Capital

Like most government organizations, DoD faces a range of serious personnel management issues. The deep cuts in both the military force structure and the civilian workforce after the end of the Cold War were not accompanied by proportionate reductions in military force deployments or in civilian workload. On the contrary, military operations tempo has been very high and there have been indications of morale problems among both military and

civilian personnel. Among the negative effects of downsizing are increased retention problems because of slow promotions and overworked staffs, recruiting problems and skills imbalances.

Human capital concerns apply in virtually all segments of the workforce. Our February 2000 report on the impact of cutting the DoD acquisition workforce in half was received with considerable interest by both the DoD and Congress. The Federal Chief Information Officers Council has been pushing vigorously for attention to problems in the information technology workforce. The Secretary of Defense Annual Report to the President and the Congress for 2001 includes the following analysis of the DoD Test and Evaluation (T&E) community:

"Since 1990, the T&E business area has reduced government personnel by more than 40 percent, and T&E institutional budgets by 30 percent. Over this same period, developmental test and evaluation workload has remained essentially stable, and operational test and evaluation workload has significantly increased. As a result, T&E is not sufficiently funded or manned to effectively and efficiently address the test and evaluation challenges of the next decade. To be responsive to the philosophy of early use of T&E for discovery of military effectiveness and suitability issues, T&E personnel will be

overextended. While the principles of the faster, better, cheaper acquisition reform philosophy are sound, the implementation which has stretched the resources of T&E has also resulted in a rush-to-failure mode for some acquisition programs."

In addition to rethinking what size workforce is needed to meet mission requirements, as opposed to cutting mission capability to meet personnel reduction goals, the DoD needs to develop more effective training methods to enable continuous learning to keep abreast of emerging technology and changing management practices. It also must find ways to compensate for the pending retirement of a large portion of the experienced workforce, improve competitiveness with private industry, and develop better incentives for productivity improvement.

The recent initiatives on improving military pay and benefits, the development of a pilot personnel management reform program for acquisition personnel, and other new initiatives indicate that human capital issues are now in the forefront of management concerns.

Summary

This has been a broad brush treatment of a large and complicated picture. In closing, I would like to emphasize that, on the whole, DoD managers react positively and do their best to take responsive action on the many problems identified for them by my office, the GAO and other oversight organizations. I am proud of the Department's record of agreeing to take responsive action on 96 percent of the over 3,000 recommendations made in Inspector General, DoD, reports during the past three years. The fact that serious problems persist generally is attributable to their inherent difficulty or to conflicting priorities, rather than indifference toward the best interest of the Department and the taxpayer.

This concludes my written statement.