Testimony

STATEMENT OF
ROBERT J. LIEBERMAN
ASSISTANT INSPECTOR GENERAL,
FOR AUDITING,
DEPARTMENT OF DEFENSE
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY
COMMITTEE ON GOVERNMENT REFORM,
AND THE SUBCOMMITTEE ON TECHNOLOGY,
COMMITTEE ON SCIENCE,
UNITED STATES HOUSE OF REPRESENTATIVES
ON THE YEAR 2000 TECHNOLOGY CHALLENGE
AT THE DEPARTMENT OF DEFENSE

Report Number 99-105 DELIVERED: March 2, 1999

Office of the Inspector General
Department of Defense

Mr. Chairman, Madam Chair and Members of the Subcommittees:

Thank you for the opportunity to discuss the challenge confronting the Department of Defense (DoD) because of the so-called Millenium Bug, which is the inability of many computers to process certain dates, especially those ending with the digits “00.” The Department’s extensive dependence on computing technology for conducting both military operations and support functions makes any potentially widespread disruption or degradation of system performance a major concern. Therefore the Secretary of Defense and Chairman, Joint Chiefs of Staff, have appropriately termed the Millenium Bug a major threat to military readiness.

Complexity of the Challenge

The task of ensuring there is no significant impairment of the Department’s ability to execute its missions and day to day functions is one of the most complex challenges ever faced by DoD managers. This is primarily because of the sheer magnitude of the problem. Consider that:

- The DoD uses about 28,000 information systems, of which approximately 2,300 are mission critical.

- About 1.5 million DoD computers exchange data with organizations as diverse as other DoD components, allies, coalition partners, defense contractors, financial institutions, the National Command Authority, other Federal agencies, and state governments;

- Hundreds of thousands of pieces of equipment, ranging from the largest weapon systems to hand held electronics, contain tens of millions of microprocessor chips, some of which are date sensitive;

- The cost of the DoD year 2000 conversion effort is estimated at $2.9 billion;

- The Department depends on hundreds of governments and firms, domestically and abroad, to provide utilities such as power, telecommunication links and water to over 500 major military bases, many of which have populations equivalent to small cities;

- When U.S. forces deploy, they depend on allies and host nations for a wide range of additional logistical

support services, as specified in thousands of agreements with dozens of governments; and

- The DoD purchases goods and services other than utilities, often electronically, from tens of thousands of contractors, 6,500 of which are considered critical suppliers.

In addition, the DoD year 2000 conversion challenge has been made considerably more difficult by a combination of factors related to management culture. Those factors included:

- A legacy of very decentralized information technology resources management, which led to a runaway proliferation of systems that was only recently addressed;

- Inadequate management visibility initially into what comprised the systems inventory, which systems were mission critical and what the interfaces were;

- Lax configuration management policies;

- An initial tendency to view the Millenium Bug as a purely technical problem that could be solved by the information technologists, without a need for much involvement by managers and commanders;

- Chronically poor documentation of systems and software modifications, so that much old, date sensitive computer code is hidden beneath newer code; and

- Resistance to reprioritizing resources to deal with the year 2000 problem early, especially if diverting resources would slow down other initiatives.

Audit and Inspection Community Role

The IG approached the Department's Chief Information Officer in early 1997 with an offer to help him achieve sufficient oversight and management control in those areas considered to have the most risk. The Chief Information Officer was very receptive to the concept of relying extensively on DoD internal audit capabilities to assure management awareness, validate reported progress and identify inadequately addressed barriers to mission continuity. Based on that informal partnership agreement, we have provided 50 "Y2K" audit reports to the

Department over the past year and a half, and are currently working on about the same number of additional audits. Coverage of Y2K conversion issues has been our top discretionary audit priority in fiscal years 1998 and 1999. In addition, we have coordinated Y2K efforts by the Military Department audit and inspection organizations, which have issued numerous reports in accordance with their own Y2K coverage agreements or taskings within their Services. We have also worked closely with the General Accounting Office and exchanged information with our counterparts in several countries.

Generally, DoD managers and commanders have been extremely cooperative and responsive to audit advice. To ensure that senior officials are aware of our audit results and so that we can effectively focus on high risk areas, we participate in Office of the Secretary of Defense and Joint Staff Y2K management conferences, workshops and planning sessions. I meet personally with senior Chief Information Officer aides at least twice a month and attend the Deputy Secretary of Defense Year 2000 Steering Group monthly briefings. Virtually all audit findings and recommendations have resulted in prompt corrective action, which is often initiated by management while the auditors are still on site and before a formal report is even issued. In addition, when Deputy Secretary Hamre was apprised

of repeated audit findings regarding inaccurate reporting of Y2K progress, he promptly convened a special session of senior DoD officials to hear our results and reemphasized the need to be responsive to audit recommendations to improve the quality of reporting. Top DoD management's encouragement of intensive auditing of Y2K progress and its responsiveness to audit results, positive or negative, have been both gratifying and challenging to the audit community.

Examples of our Y2K audit reports are summarized in the attachment to this statement.

Slow Start, But Likely a Strong Finish

As reflected in the rather low grades that Chairman Horn gave to DoD Y2K performance initially, the Department got off to a slow start. In hindsight, most managers underestimated both the complexity of the problem and the commitment of resources and executive managers' time that would be necessary. As late as last summer, audits were indicating a widespread lack of awareness; insufficient Y2K staffing at all levels of the Department; and only rudimentary Y2K planning at dozens of crucial organizations, including most combatant commands, most

functional area staffs within the Office of the Secretary of Defense, many support commands and most installations. Although many DoD organizations were working hard on the remediation of mission critical information systems, a high percentage of remediation plans provided for completion very late in calendar year 1999 and large scale “system of systems” test plans were in vague conceptual form only. There was even some resistance to the notion of modifying previously planned exercises to accommodate Y2K scenarios or to plan for other large scale testing.

A decisive turning point came in early August 1998, when the Secretary of Defense declared that the Department’s progress up to that point had been insufficient. Both the Secretary and the Deputy Secretary prescribed a number of measures during that timeframe to accelerate the Department’s effort and to move accountability for Y2K success beyond the boundaries of the information technology community to all senior managers and commanders. The strong and unambiguous message that Y2K was a genuine threat to readiness, which needed to be treated as such by the leaders of the operating forces and the acquisition, logistics, finance and other support communities, had the intended effect.

The number of mission critical systems that have been certified as Y2K compliant has grown as follows:

February 1998:	706	(24%)
May 1998 :	812	(29%)
August 1998 :	1,236	(39%)
November 1998:	1,352	(52%)
February 1999:	1,670	(72%)

Equally important, efforts have greatly accelerated over the past few months to assess the Y2K readiness of DoD-owned, infrastructure; of the private sector infrastructure on which DoD also depends; of the diverse range of data exchange partners and of host nations abroad. In addition, one of the largest testing efforts ever undertaken by the Department has now started and will continue through calendar year 1999.

Inspector General, DoD, Assessments

In the Inspector General, DoD, semiannual report to the Congress for the six month period ending September 30, 1998, and again in a December 1998 summary report on 142 audit and inspection

reports issued between August 1997 and early December 1998, we concluded that the Secretary of Defense assessment that progress had been insufficient as of August 1998 had been well founded. We also took note of the increased emphasis and progress by the Department over the last few months of 1998.

We will be issuing another summary report this month. It will reflect the results of audits and inspections conducted in late 1998 and early 1999. The results are generally much more positive than those from last year and are another indicator that the pace and effectiveness of the DoD Y2K program have improved significantly. With sustained close management attention through 1999, we are confident that the Department can achieve its goal of ensuring the continuity of critical operations and capabilities as the millenium passes. However, much work remains to be done. No assessments of overall progress can be entirely credible in the absence of significant quantities of test results, which will not be available for a few more months, and the belated start in some areas has caused a fairly high risk level to persist there.

Those areas of continuing concern include:

- Well over 600 mission-critical systems that remain Y2K non-compliant;
- infrastructure, especially overseas;
- supplier readiness;
- untested contractor off the shelf products;
- contingency planning;
- mainframe computer platforms; and
- greatly compressed testing schedules.

Testing

The continuing concern that I would like to focus on today relates to the testing challenge. The DoD Y2K conversion effort is unprecedented in many ways, one of which is the scope of the crucial Y2K testing that will continue through the end of 1999. In addition to the individual system/application testing that is performed before a system is certified as Y2K compliant, the

various DoD components are engaged in three kinds of “higher level” testing:

- Intersystem integration testing at the Military Service or lower organizational levels, either as special Y2K tests or as part of routinely performed activity such as Navy battlegroup system integration tests.

- More than 76 end-to-end system test events, covering 93 processes in functional areas such as finance or command and control, and involving over 600 mission critical systems;

- Approximately 31 operational evaluations by the unified commands around the world.

We cannot over emphasize the need for robust in-depth testing. The sheer number of systems involved, the risk of incompatible Y2K fixes because of the number of different firms and individuals involved in remediating code, and the compression of this ambitious testing schedule into just over a year pose a formidable management challenge. In our view, it is the most daunting of the remaining Y2K challenges. A significant portion of our auditing emphasis will be directed to this area.

We will be looking for indicators of good test planning, such as detailed written test plans; management controls to ensure appropriate oversight of both the test plans and the reporting of test results; and provision for sufficient technical support before, during, and after the test. We fully anticipate that numerous previously undetected and perhaps unanticipated "glitches" will surface during each of the various types of tests. If not, the rigor of the tests-—and their credibility-—may be called into question. This is a significant mindset change for many managers and commanders, who by habit and training may tend to seek perfect scores. Identifying computer code that is still not fixed is a victory, not a defeat, for the testing process.

It is also important that managers be encouraged to seek out the most effective available Y2K diagnostic tools and not hesitate to test or retest their code, whether or not their systems are mission-critical or are included in multi-system testing. More and more powerful tools are entering the market place and can provide extra assurance.

Conclusion

In conclusion, we believe that the DoD is overcoming the increased risk posed by its belated start on several facets of the Y2K conversion effort. As the intensive effort continues, we remain committed to our partnership with the Department on this difficult matter and will continue striving to provide DoD, the President's Council on Y2K Conversion, the Office of Management and Budget, and Congress with reliable, candid and timely feedback on Y2K progress.

Attachment

Examples of Year 2000 Audit Results
Office of Inspector General, DoD

Report No. 99-086, Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility: III Marine Expeditionary Force, February 22, 1999. This was a good news report. The III Marine Expeditionary Force had taken a proactive approach to ensuring that its information systems will be compliant in the year 2000. The III Marine Expeditionary Force had made progress with actions to assess system compliance, implement corrective actions, and accurately report status issues for potential year 2000-related failures. When the III MEF year 2000 conversion effort is completed, including participation in further testing and operational evaluation, the risk of mission capability impairment because of year 2000 problems should be low.

Report No. 99-081, Tooele Chemical Agent Disposal Facility Preparation for Year 2000, February 16, 1999. The Tooele Chemical Agent Disposal Facility was considerably behind Army and DoD schedules for assessing year 2000 vulnerability and carrying out conversion measures. In addition, Tooele Chemical Agent Disposal Facility had not prepared the required year 2000 documentation, which are the assessment plan, the contingency plan, the risk management plan, and the validation plan and schedule. During the audit, reporting errors were corrected and Army management emphasis increased; however, estimated completion dates for the conversion extended well into calendar year 1999. Successful completion of all year 2000 conversion measures is necessary to avoid operational impairment and obviate any safety concerns. The Army agreed and aggressive measures are being taken to accelerate the conversion effort.

Report No. 99-079, Year 2000 Conversion Program at the Dugway Proving Ground Major Range and Test Facility, February 9, 1999. A good news report. The renovation of both business and test systems was being effectively managed. Dugway Proving Ground identified seven systems for assessment, developed contingency plans, tested all systems and maintained all the necessary documentation. The range met the Army's deadline of completing the renovation phase by September 1998. Six of the seven systems completed the implementation phase by December 31, 1998. The meteorology system completed the implementation phase in February 1999.

Report No. 99-076, Year 2000 Posture of DoD Mid-Tier Computer Systems, February 3, 1999. Good news report. Managers of the 14 mid-tier systems reviewed in the audit were actively managing each primary element to achieve year 2000 compliance, and they appropriately reported the year 2000 status of each mission-critical computer system. The major reason that mid-tier systems were appropriately managed and reported was because the primary elements of each system were the responsibility of a single manager. Additionally, Army and Air Force year 2000

reporting guidance specifically requires that Service sub-components track and report each primary element of computer systems. Further, some program managers prudently went beyond existing formal requirements to employ further risk-reduction tactics, such as testing vendor-validated products. Accordingly, for the mid-tier systems reviewed, we judged that the risk of system failure at the turn of the century because of a primary element being overlooked was low.

Report No. 99-063, Global Positioning System Receiver Compliance with Year 2000 Requirements, December 31, 1998. The Global Positioning System (GPS) is a worldwide, satellite-based radio navigation system developed by DoD. The system is able to show a user's position on or above the earth with great precision, regardless of weather conditions. Dates and times are important to GPS receivers. The receivers determine a position by comparing the time generated by an internal clock to the times received from the fleet of GPS satellites. The difference between the times is used by the receiver to compute its distance from the satellite and hence compute its location.

In February 1998, the Assistant Deputy Under Secretary of Defense (Space Systems and Architectures) issued a memorandum, "Global Positioning System Year 2000 Compliance," tasking the GPS Joint Program Office to assess the Y2K compliance status of all DoD GPS receivers. The Assistant Deputy Under Secretary also directed organizations that have procured non-validated receivers from sources other than the program office to provide the program office with the Year 2000 compliance status of those receivers by April 30, 1998.

The audit indicated that the GPS Joint Program Office had not completed the inventory and Year 2000 assessment of non-validated GPS receivers procured directly by DoD organizations, civilian Federal agencies, Defense contractors, and allied nations. The delay was primarily caused by lack of cooperation by many of those organizations. In addition, DoD had not done enough to mitigate risk by testing commercial receivers. As a result, systematic distribution of reliable information on Y2K compliance of the equipment to users has been hampered, increasing the risk of mission disruption.

After expressing some initial concern about the need for testing commercial receivers, management agreed with the report and is taking action.

Report No. 99-059, Summary of DoD Year 2000 Conversion—Audit and Inspection Results, December 24, 1998. This report summarized Y2K issues identified in 142 General Accounting Office; Inspector General, DoD; Army; Navy; and Air Force Audit reports from August 1997 to December 1998. It also included information reported by the Inspector General, Navy, and the Inspector General, Marine Corps. The Inspector General, Army, and the Inspector General, Air Force, had not yet reported on Y2K.

Year 2000 conversion problems were identified within the following areas:

- management oversight and awareness (95 reports),
- reporting (79 reports),
- assessment (97 reports),
- resource requirements estimation (48 reports),
- interface identification and agreements (74 reports),
- prioritization (14 reports),
- testing (83 reports),
- contingency and continuity-of-operations planning (104 reports),
- contracts (21 reports), and
- infrastructure (44 reports).

The results supported the DoD acknowledgements that the year 2000 conversion poses a high risk for a very wide range of DoD functions and organizations and that the conversion progress as of late FY 1998 had been insufficient. These results were briefed to the Deputy Secretary of Defense and DoD Y2K Steering Group in early December 1998.

Report No. 99-058, "Year 2000 Conversion of Defense Critical Suppliers," December 18, 1998. Until late FY 1998, outreach efforts to suppliers of National Defense goods and services were left to individual DoD components to organize, execute and monitor. As a result, the emphasis put on outreach to suppliers varied greatly among DoD acquisition and logistics organizations. Many organizations had no organized outreach effort. DoD faced an increased risk of production and delivery disruptions because of the belated outreach focus to ensure suppliers' Y2K conversion. If commercial suppliers of critical supplies experience disruptions as a result of computer failures, the logistics pipeline may be compromised.

During the audit, we worked with management to accelerate efforts in this area. The DoD established a Joint Supplier Capability Working Group. By October 1998, this team had established the methodology for identifying critical items and their suppliers, as well as a reasonable action plan for assessing critical suppliers' year 2000 compliance. A survey of 6,500 critical suppliers began in February 1999. The Defense Logistics Agency's Defense Contract Management Command will conduct most of the survey. The IG, DoD, is monitoring the effort and providing particular assistance to Defense supply centers.

Report No. 99-027, DoD Base Communications Systems Compliance with Year 2000 Requirements, October 30, 1998. The audit indicated 131 non-compliant telecommunication switches would not be replaced or made compliant by the March 31, 1999 deadline established by the Office of Management and Budget. This high risk developed because of inefficient identification of the

switch inventory, insufficiently high priority given to these critical items, and funding problems. Management agreed and additional emphasis was put on switch replacement or remediation. The IG, DoD, is tracking progress on each switch in every DoD component organization.

Report No. 99-022, Year 2000 Conversion at the Army Major Range and Test Facilities, October 29, 1998. The three Army major range and test facilities visited, the Aberdeen Proving Ground, the White Sands Missile Range, and the Yuma Proving Ground, were on schedule. All required documentation and certification forms for the compliant systems were completed as required by the Army Action Plan and the DoD Management Plan.

Report No. 98-207, Year 2000 Contract Language for Weapon Systems, September 22, 1998. Of 16 weapon systems reviewed, 9 weapon systems had contracts that did not contain language from Federal Acquisition Regulation 39.106, "Year 2000 Compliance." In July 1998, when the initial audit results were briefed, the Under Secretary of Defense for Acquisition and Technology had not yet issued Y2K guidance for weapon systems. On August 7, 1998, the Secretary of Defense directed the Services and Defense agencies to report on each major acquisition system under their purview. Each report was to address areas of Y2K compliance or noncompliance for each system. The Secretary of Defense also directed that funds not be obligated for any contract for information technology or national security systems that process date-related information, if that contract did not contain Y2K requirements specified in the Federal Acquisition Regulation. During the audits, the program management offices took action to ensure that the contracts and solicitations for the nine deficient weapon system programs would include Y2K compliance language.

Report No. 98-193, Evaluation of the Defense Megacenters Year 2000 Program, August 25, 1998. Although much progress had been made in converting the Defense Megacenters systems and platforms to Y2K compliance, problems remained in three areas: reporting, testing, and contingency planning.

The Defense Information Systems Agency Western Hemisphere Y2K status reports for mainframe executive operating software were incomplete and could be misinterpreted. The reports showed that the executive software product inventory was 60 percent compliant, but did not show that the domain compliance itself was zero percent. The Defense Information Systems Agency Western Hemisphere and the Central Design Activities, which are part of the Military Departments and Defense agencies, had joint responsibility for fixing segments of the domains. However, coordination needed improvement.

On July 2, 1998, the Deputy Secretary of Defense directed written agreements between the Defense Information Systems Agency and domain users. In addition, the Office of the

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) coordinated a Secretary of Defense memorandum that stated funds were not to be obligated for any domain user that failed to sign explicit test agreements with the Defense Information Systems Agency by October 1, 1998. The memorandum, dated August 7, 1998, also states that the Defense Information Systems Agency was to provide a report to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) by October 15, 1998, listing all domain users that failed to sign test agreements with the Defense Information Systems Agency by October 1, 1998. Finally, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that it would request that the Y2K compliance reports from the Defense Information Systems Agency include items that would identify domains, mission-critical systems, or national security systems that had a high risk of Y2K noncompliance.

The IG, DoD, is continuing to monitor the year 2000 conversion efforts at the Defense Megacenters.

Report No. 98-147, Year 2000 Certification of Mission-Critical DoD Information Technology Systems, June 5, 1998. The audit indicated that DoD components certified only 109 (25.3 percent) of the 430 systems reported as Y2K compliant in November 1997. Systems were not certified because DoD components did not adequately implement and enforce the guidance in the DoD Management Plan or their own Y2K guidance. Additionally, the initial DoD Management Plan was not clear as to specific Y2K certification requirements.

The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with our recommendations and instituted several measures, including the following:

- requiring that all mission-critical systems have independent tests and operational contingency plans,
- updating the DoD Management Plan in June 1998 with better guidance on certification and testing, and
- developing a new Y2K database that would include the target date to complete each phase of Y2K remediation for each mission-critical system.

Report No. 98-065, DoD Information Technology Solicitations and Contract Compliance for Year 2000 Requirements, February 6, 1998. The DoD initiated actions to address the new procurement aspects of the Year 2000 issue in mid-1996 in an Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum, “Year 2000 Computing Problem with Personal Computers and Workstations,” May 8, 1996. Federal Acquisition Regulation section 39.106, “Year 2000 Compliance,”

subsequently provided mandatory guidance to assist agencies in acquiring only those information technology products and systems that are Year 2000 compliant.

The audit indicated that initial DoD compliance with the requirements was poor. Twenty of the major 35 indefinite-delivery/indefinite-quantity and indefinite-deliver-requirement information technology contracts (for commercial off-the shelf products) that were audited did not have the required Federal Acquisition Regulation Year 2000 compliance language. None of the 35 contracts required testing of purchased products. As a result, DoD had no assurance that information technology products purchased were year 2000 compliant. Additionally, because 33 of the 35 contracts were available for use by other Federal agencies, nonconforming contract deliverables could negatively affect non-DoD systems.

Based on initial audit results, DoD issued stronger guidance on December 18, 1997, before our final report was issued. Subsequently, the DoD components reported that the 20 deficient contracts had been modified. Guidance on testing was also improved. Proper use of Y2K contract clauses is now routinely checked in most Y2K audits; some isolated instances of continued non-compliance have been reported and corrected.