United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, and the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Tuesday,
March 2, 1999

YEAR 2000 COMPUTING CRISIS

Defense Has Made Progress, But Additional Management Controls Are Needed

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

Mr. Chaiman, Ms. Chairwoman, and Members of the Subcommittees:

Thank you for inviting me to participate in today's hearing on the Department of Defense's (DOD) efforts to confront the Year 2000 problem. This dilemma is particularly daunting for Defense for two reasons. First, Defense's size and scope of operations, criticality of mission, and heavy reliance on a diverse portfolio of information technology is unparalleled in either the public or private sector. Second, despite considerable progress in the last 3 months, Defense is still well behind schedule. This is largely because Defense did not have the necessary oversight and management framework for handling large-scale departmentwide information technology projects.

Defense has recently taken steps to strengthen management of its Year 2000 program by providing the controls and guidance needed to fix and test systems; it also has appropriately shifted its focus to core business readiness and operational risks through (1) planning for the performance of end-to-end tests of key functional area business processes, (2) executing a series of simulated Year 2000 operational exercises, and (3) conducting system integration tests at the military service level. Additionally, the Deputy Secretary has become actively engaged in directing and monitoring Year 2000 efforts.

We support these actions, but the key to their success rests in putting in place effective controls for Defense to have the timely and reliable information to know what is going right and what is going wrong so that corrective action can be swift and effective. These controls, which our Year 2000 guides define, require Year 2000 program management to define the appropriate performance and progress measures and reporting requirements and to ensure that these requirements are met. For Defense to minimize risks in the 305 days remaining before the Year 2000 deadline, it must act quickly and decisively to implement and enforce these controls.

Our testimony today is based on our ongoing review of Defense's efforts to solve the Year 2000 computer systems problem, which has spanned DOD headquarters; the Army, Navy, and Air Force; major components, including the Defense Logistics Agency, the Defense Finance and Accounting Service; the Defense Information Systems Agency (DISA), the Joint Chiefs of Staff; and central design activities. We also witnessed operational tests recently conducted at the North American Aerospace Defense Command (NORAD). Over the past 2 years, we have reviewed Defense's Year 2000 plans, guidance, and directives; discussed Defense's efforts with the

Deputy Secretary, many DOD executives, and members of the Defense Science Board; and attended DOD Year 2000 Steering Committee meetings. We have compared DOD's efforts to criteria detailed in our Year 2000 Assessment Guide,[1] Business Continuity and Contingency Planning Guide,[2] and Testing Guide.[3] This guidance offers a structured and disciplined approach to developing a Year 2000 program and managing the risk of potential Year 2000-induced disruptions to operations. To date, we have issued 11 products[4] and provided numerous briefings to Department officials and the Congress on this important issue.

Likewise, auditors for the Department of Defense have been assessing Year 2000 progress at the military services, Defense agencies, and other DOD organizations. Some 142 products have been issued by the Inspector General and other DOD auditors. Recently, in December 1998, the Inspector General released a report summarizing the results of combined Year 2000 audit and inspection coverage of the Department.[5]

Background

Our Year 2000 guidance defines structures and processes for effectively managing a Year 2000 program, including (1) establishing central accountability and authority for Year 2000 efforts, (2) addressing system conversion in the context of core business missions, (3) developing institutional plans and guidance governing conversion, testing, and contingency planning, and (4) defining requirements for progress reporting. These controls are needed because the risk of Year 2000 failure extends well beyond an organization's internal information systems. For example, Defense depends on information and data provided by thousands of business partners—including other federal agencies, international organizations, allies, and private sector contractors. Moreover, it depends on services provided by the public infrastructure—including power, water,

[1] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14). Published as an exposure draft in February 1997 and finalized in September 1997.

[2] Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19). Published as an exposure draft in March 1998 and finalized in August 1998.

[3] Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21). Published as an exposure draft in June 1998 and finalized in November 1998.

[4] See attachment for a list of GAO products on Defense's Year 2000 program.

[5] Summary of DOD Year 2000 Conversion—Audit and Inspection Results (Report No. 99-059, December 24, 1998), Office of the Inspector General, Department of Defense.

transportation, and voice and data telecommunications. Defense also owns hundreds of thousands of potentially vulnerable infrastructure devices that may fall outside of the control of an individual unit. These include, for example, building and base security systems, street lights at military installations, elevators, and medical equipment.

Last April, we reported[6] that Defense operations were threatened by slow progress in fixing its mission-critical systems and mitigating Year 2000 risk. We also reported that Defense did not establish strong management mechanisms, such as a Year 2000 Program Office and a full-time Year 2000 executive and processes for validating information on component progress. In addition, it was not addressing conversion efforts within the context of business areas. Furthermore, Defense did not initially develop a detailed Year 2000 plan or guidance on developing interface agreements, testing systems, and reporting on progress. Instead, Defense delegated responsibility for addressing the problem to its components. Our reviews of individual component Year 2000 efforts showed that, in turn, the components delegated this responsibility to subcomponents and likewise neglected to implement strong management controls.

Our recommendations to Defense focused on supporting remediation efforts with adequate centralized program management and oversight. For example, we recommended that DOD establish a strong department-level program office, led by an executive whose full-time job was to effectively manage and oversee Year 2000 efforts. This office should, as a minimum, have sufficient authority to enforce good management practices, direct resources to specific problem areas, and ensure the validity of data being reported by components on such things as progress, contingency planning, and testing.

In view of the Department's status, the Office of Management and Budget (OMB) designated Defense as a "Tier One" agency in May 1998, indicating that it was making insufficient progress in remediating its systems. Defense itself designated the Year 2000 effort as one of its most significant internal management control problems for fiscal year 1998.

The lack of progress in effectively dealing with the Year 2000 problem was largely rooted in the fundamental weaknesses in managing information

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

technology that have plagued Defense for years. Since 1995, when we first designated Defense's management of information technology as a high-risk federal program,[7] we have continually reported that Defense did not have controls and processes for (1) ensuring that the costs and risks of multimillion dollar projects are justified, (2) monitoring progress and performance, and (3) stopping projects shown to be cost ineffective or technically flawed.[8] Perhaps the biggest impediment to successful IT projects has been Defense's organizational environment, which has resisted departmentwide efforts to standardize business processes and information systems and to increase oversight and visibility over information resources.

Actions Taken to Address Weaknesses Have Enhanced DOD's Year 2000 Progress

Since our April 1998 report, Defense has implemented our recommendations and taken additional actions to address the Year 2000 dilemma. Moreover, it has engaged top managers in the initiative. For example, Defense:

- Established a department-level Year 2000 Program Office headed by a full-time executive with a current staff of more than 50.
- Improved its information systems inventory to better track components' progress.
- Increased the frequency of Year 2000 Steering Committee meetings. This committee, headed by the Deputy Secretary of Defense, who is an active participant, is charged with reviewing the progress of Defense components, providing guidance, and making decisions on Year 2000 issues that have not been resolved at lower levels. When we reported on DOD's Year 2000 effort in April 1998, the committee was not meeting regularly.

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

[8] For example, in 1996 we reported that one functional area began, and later abandoned, a substantially flawed effort to develop a standard suite of information systems for materiel management after spending over $700 million without strong oversight. Our reports also found that some functional areas did not account for various categories of significant costs when making their systems decisions or adequately consider alternatives to developing systems in-house. See, Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, October 20, 1997); DOD Accounting Systems: Efforts to Improve System for Navy Need Overall Structure (GAO/AMD-96-99, September 30, 1996); Defense IRM: Critical Risks Facing New Materiel Management Strategy (GAO/AIMD-96-109, September 6, 1996); Defense Transportation: Migration Systems Selected Without Adequate Analysis (GAO/AIMD-96-81, August 29, 1996); and Defense Management: Selection of Depot Maintenance Standard System Not Based on Sufficient Analyses (GAO/AIMD-95-110, July 13, 1995).

- Required that fiscal year 1999 information technology funding be contingent on components (1) ensuring the accuracy of the Year 2000 database, (2) completing interface agreements, (3) specifying Year 2000 requirements in contracts, and (4) developing test agreements with Defense computer centers. This was done through a series of memoranda issued by the Secretary of Defense; the Deputy Secretary of Defense; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Comptroller in August and September 1998.
- Increased its outreach efforts with state and local governments, as well as the international security sector.

While still behind in meeting governmentwide target deadlines, Defense reports that it is now making much better progress in fixing and testing its systems. In its February Year 2000 quarterly status report to OMB, Defense reported that of its 2,387 mission-critical systems

- 1,670 systems, or 70 percent, were compliant,
- 225 systems were going to be replaced or retired,
- 8 systems were being assessed,
- 96 systems were being fixed,
- 226 systems were being tested, and
- 162 systems were being implemented.

Although Defense reports that the number of compliant systems has risen from about 50 percent to 70 percent since its November 1998 quarterly status report to OMB, its remediation efforts are still at significant risk. The number of systems that have fallen behind schedule, for example, doubled from 65 to 172, and the number not expected to meet OMB's target March 31, 1999, completion date almost tripled from 54 to 156.

Furthermore, Defense is behind in terms of renovating its facilities and installations. Defense's February 1999 quarterly status report to OMB showed that only 269 of 638, or 42 percent, of Defense's installations had completed necessary Year 2000 corrections. While an additional 317 facilities are to be completed by March 31, 1999, 47 more are not expected to be done until June 30, 1999, and 5 not until September 30, 1999. According to Defense, there are another 600-plus buildings used by Defense, but controlled by the General Services Administration, that are considered at risk because the lessor has not provided Year 2000 status information. In addition, Defense does not yet have good data on the

readiness of its overseas installations, which are dependent on other nations for power, fuel, water, and other important services.

Defense's Focus Is Appropriately Shifting to Core Business Areas

While the focus of most agencies has been directed at remediating systems, the real level of Year 2000 assurance needs to be centered on business functions. That is, agencies must be able to continue to provide key services and meet agency mission objectives at an acceptable level of performance. To this end, agencies should now be focusing on end-to-end testing of business processes and developing business continuity plans for those processes. Each of our Year 2000 guides define practices and controls that are founded on first identifying core business processes, mapping mission-critical systems to these processes, and then performing assessment, renovation, testing, and contingency planning within the context of these core business areas.

Defense has appropriately shifted its focus toward ensuring the continuity of core business processes and military operations.

- First, in an August 7, 1998, memorandum, the Secretary of Defense directed the Commanders in Chief (CINC) to plan and execute a series of simulated Year 2000 operational exercises. These exercises, which were required by Defense appropriation and authorization legislation, [9] are to assess whether Defense can still perform critical military tasks with system clocks rolled forward to the year 2000, such as ensuring that Defense can continue to perform a strategic early warning mission, deploy and maneuver forces, and employ firepower. Thirty-one such evaluations are scheduled through September 1999.
- Second, Defense is requiring its principal staff assistants (PSAs) to ensure the continuity of key functional area business processes. In response, the PSAs are planning to conduct end-to-end tests to ensure that systems that collectively support core business areas can interoperate as intended in a Year 2000 environment. In an August 24, 1998, memorandum, the Deputy Secretary of Defense provided overall

[9] The Department of Defense Appropriations Act, 1999 (Public Law 105-262) and the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (Public Law No. 105-261) both required Defense to submit a plan to the Congress by December 15, 1998, for the execution of simulated Year 2000 exercises. Specifically, Defense is to conduct at least 25 simulation exercises, ensure that each of the Commanders in Chief conducts at least two of these exercises; and ensure that all mission-critical systems that are expected to be used in a major theater of war are tested in at least two exercises. Defense has not yet submitted the required plan to the Congress.

planning requirements and the expectation that all functional plans would be completed by November 1, 1999, for five functional areas: communications, health/medical, intelligence, logistics, and personnel. The Department has since added weapons and finance to those functional areas.

- Third, the military services are conducting integration testing of their systems. The testing is intended to build upon completed system's renovation, testing, and certification, and ultimately, to reduce risk and ensure the ability to execute critical combat missions in a Year 2000 environment.
- Fourth, Defense directed installation commanders to ensure that all installations will be fully functional at the year 2000. These installations are, of course, critical to housing both the military and civilian workforce as well as the weaponry and supporting activities necessary for national defense.
- Fifth, the Department has initiated regular "synchronization" meetings—chaired by the Deputy Assistant Secretary of Defense and the Joint Chiefs of Staff Year 2000 Task Force Leader–to improve and facilitate coordination of the many activities that cut across organizational boundaries.

Because of the need for close integration between the operational and functional evaluations, we are now reviewing the interaction among the various tests and evaluating the adequacy of relevant management controls. While we have not yet finished our comprehensive evaluation of these tests and controls, we can make several preliminary observations.

- The initial operational evaluations have been successful. We found the guidance provided by the Joint Chiefs of Staff for conducting the operations to be well-developed and consistent with our own published guidance. Exercises have already been conducted at the North American Aerospace Defense (NORAD) Command and the Strategic Command. We had the opportunity to observe the planning and execution phases of NORAD's missile warning operational evaluation. According to NORAD officials, the purpose of this evaluation was to confirm the correct processing of responses to airborne threats systems and not to validate every possible threat that could occur. Based on our observations, the operational evaluation was well-planned and executed. The Year 2000 date rollovers worked properly, and NORAD officials were able to recover and continue the mission when testing problems occurred. For example, a tape drive failed at one of the sensor sites, and fallout from one of the test missiles was incorrectly coded as a

missile launch. These anomalies, however, were immediately detected and resolved by NORAD officials at the time of the test.

- Since many systems and processes are outside the CINCs' control, many of the planned evaluations will require extensive support from the functional areas, such as communications and logistics. For example, the Strategic Command's five phase operational evaluation program will require extensive support from DISA to plan, schedule, and provide on-site technical support for more than 10 DISA-owned systems that make up its communications backbone. One phase of this plan has already been delayed 2 months to await DISA's installation of Year 2000 compatible components. Defense is beginning to work on these kinds of dependencies through the synchronization meetings with the PSAs and CINCs.
- Our initial reviews of the functional area readiness plans have showed mixed results. For example, while each of the functional plans discusses business functions, supporting systems, and testing requirements, the plans frequently lack important details such as test schedules, completion dates for contingency plans, or detailed mapping of systems and support activities to business functions.

DOD Management Needs Better Controls and Information on Business Operations Readiness

DOD has correctly shifted much of its emphasis on continuity of business processes rather than the status of individual systems. The Year 2000 Steering Committee, chaired by the Deputy Secretary and comprised of top management representatives from each of the services and component agencies, has been instrumental in overcoming cultural impediments that have historically limited the Department's ability to respond to information management issues.[10]

However, to effectively manage and oversee Year 2000 programs, managers and executive decisionmakers need reliable information about the nature and status of Year 2000 conversion efforts from a core business perspective. This is not available in DOD. Our Year 2000 guides recognize the importance of such information. Accordingly, the guides provide for establishing formal reporting mechanisms early in the Year 2000 program life cycle and using the information reported to oversee and control program efforts. Additionally, the guides describe the need to specify the content and format of the reports and the reporting frequency and to

[10] Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999).

establish management controls (e.g., the use of quality assurance and independent verification and validation groups) to ensure that the information being reported is reliable.

The Department's controls and reporting mechanisms are primarily still centered around individual systems. Although the functional areas and commands have been instructed to develop testing and contingency plans based on business functions, the DOD Year 2000 management plan and its supporting guidance have not been updated to reflect reporting and control mechanisms that should be in place to reinforce this evolutionary shift in focus.

It is conceivable that each component, each command, and each function is developing appropriate plans with an appropriate level of control to ensure that the right thing is being done at the right time. But there is simply no mechanism in place right now to provide this assurance, and our initial reviews of the functional plans suggest uneven levels of planning and execution across the Department.

The Department clearly needs greater visibility into the status of core business processes throughout the agency. Specifically, within the context of each core business area the Department should determine the

- status of each supporting information system critical to that process, including its schedule for remediation and testing;
- source and Year 2000 status of any suppliers or vendors critical to that process;
- outside dependencies (such as electrical power) that affect readiness;
- interfaces with other processes and outside organizations;
- scope and schedule of end-to-end testing for the process; and
- scope and schedule for business continuity planning for that process.

For any of these elements that are behind schedule, Defense needs to know what steps will be taken to get back on schedule or what steps will be taken to minimize the risks associated with their delay.

Once these assessments are complete, top management can develop an overall perspective of readiness, identify gaps or unnecessary overlaps among individual components, reallocate resources, and develop comprehensive business continuity plans that cut across organizational lines.

Additionally, the Department needs greater assurance that the information being provided is consistent both in terms of content and accuracy. To this end the Department should

- provide standard expectations for both content and reporting requirements and performance metrics for all the above elements and
- establish control mechanisms to provide assurance that reported information is complete and accurate.

Defense Has Good Opportunity to Apply Year 2000 Lessons Learned to Future Information Technology Investments

The immediate focus for Defense over the next 305 days should be on ensuring implementing and enforcing controls that focus on ensuring the continuity of operations into 2000. However, in the long term, Defense has a unique opportunity to capitalize on the valuable lessons it has learned in its Year 2000 effort and apply them to its overall management of information technology. Doing so can enable the Department to acquire and deploy high performing, cost-effective systems and to avoid repeating costly mistakes. 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, PSAs, and decisionmakers at Defense components. Best practices[11] 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. Such involvement is also critical to breaking down cultural and organizational impediments that hamper Defense-wide IT efforts.
- Defense has realized that having a complete and accurate enterprisewide information systems inventory can facilitate remediation, testing, and validation efforts. Maintaining a reliable, up-to-date 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 controls at the system level to prevent proliferation of

[11] Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994) and Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making (GAO/AIMD-10.1.13, February 1997).

Year 2000 problems between systems. This effort should help Defense to 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 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.

Conclusions

The Year 2000 program has been demanding on Defense because of the size and scope of its operations and its heavy reliance on information technology, but also because it began the effort with weak and undisciplined information technology management processes. Defense has since made strides in meeting this challenge under the leadership of the Deputy Secretary, garnering the involvement of DOD-wide managers, PSAs, CINCs, and component executives; putting controls and mechanisms in place to facilitate system renovations; and undertaking the formidable task of conducting operational exercises and end-to-end tests on functional processes.

However, DOD still faces two significant challenges and a fast approaching deadline. First, the Department must still "catch up" and complete remediation and testing of mission-critical systems. Second, it must have a reasonable level of assurance that key processes (functional areas) will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. Such assurance can only be provided if the Department takes steps to improve its visibility over the status of key business processes. This information is critical to identify those areas where it faces the greatest risk of failure and critical to providing the necessary data for preparing overall business continuity plans.

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

List of GAO Products That Address DOD's Year 2000 Problem

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999).

Defense Computers: Year 2000 Computer Problems Put Navy Operations at Risk (GAO/AIMD-98-150, June 30, 1998).

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998).

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

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997).

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997).

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997).

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997).

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00