OVERSIGHT OF THE YEAR 2000 PROBLEM AT THE DEPARTMENT OF DEFENSE: HOW PREPARED IS OUR NATION'S DEFENSE?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

AND THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

MARCH 2, 1999

Committee on Government Reform

Serial No. 106–41

Committee on Science

Serial No. 106–47

Printed for the use of the Committee on Government Reform and the Committee on Science

Available via the World Wide Web: http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

60–621 CC WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
JOHN T. DOOLITTLE, California
HELEN CHENOWETH, Idaho

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
GARY A. CONDIT, California
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
CARLA J. MARTIN, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
MATT RYAN, *Senior Policy Director*
MASON ALINGER, *Clerk*
FAITH WEISS, *Minority Counsel*

COMMITTEE ON SCIENCE

HON. F. JAMES SENSENBRENNER, JR., (R–Wisconsin), *Chairman*

SHERWOOD L. BOEHLERT, New York
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan*
DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California
JUDY BIGGERT, Illinois
MARSHALL "MARK" SANFORD, South Carolina
JACK METCALF, Washington

GEORGE E. BROWN, JR., California, RMM**
RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
TIM ROEMER, Indiana
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
ALCEE L. HASTINGS, Florida
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON-LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
VACANCY
VACANCY

SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, Maryland, *Chairwoman*

CURT WELDON, Pennsylvania
ROSCOE G. BARTLETT, Maryland
GIL GUTKNECHT, Minnesota*
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California

JAMES A. BARCIA, Michigan**
LYNN N. RIVERS, Michigan
DEBBIE STABENOW, Michigan
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
BART GORDON, Tennessee
TIM ROEMER, Indiana

EX OFFICIO

F. JAMES SENSENBRENNER, JR., Wisconsin+

GEORGE E. BROWN, JR., California+

CONTENTS

OVERSIGHT OF THE YEAR 2000 PROBLEM AT THE DEPARTMENT OF DEFENSE: HOW PREPARED IS OUR NATION'S DEFENSE?

TUESDAY, MARCH 2, 1999

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY OF THE COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON TECHNOLOGY OF THE COMMITTEE ON SCIENCE,

Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the Subcommittee on Government Management, Information, and Technology) presiding.

Present: Representatives Horn, Morella, Ehlers, Gutknecht, Biggert, Walden, Ose, Bartlett, Miller, Turner, Maloney, Mink, Jackson Lee, Udall, Rivers, Stabenow, and Wu.

Staff present from the Subcommittee on Government Management, Information, and Technology: Russell George, staff director and chief counsel; Matt Ryan, senior policy director; Bonnie Heald, director of information/professional staff member; Mason Alinger, clerk; Faith Weiss, minority counsel, Committee on Government Reform; and Jean Gosa, minority clerk, Committee on Government Reform.

Staff present from the Subcommittee on Technology: Richard Russell, staff director; Benjamin Wu, professional staff member; Richard Lukas, intern; and Joe Sullivan, clerk.

Mr. HORN. A quorum being present, the joint hearing of the House Subcommittee on Government Management, Information, and Technology of the House Government Reform Committee and the Subcommittee on Technology from the House Science Committee will come to order.

Only 304 days remain to reassure American citizens that the Federal Government's computer systems, those that are most critical to our lives, are year 2000 compliant. Unfortunately, even today many governmental entities, as well as private organizations, are only now recognizing the potential severity of this problem. Some have just begun to fix their systems, leaving little, if any, time for one of the most important aspects of this effort, adequate testing. The problem is real. The deadline is unmovable. The House Subcommittee on Government Management, Information, and Technology has focused on the potential problem since April 1996.

The year 2000 computer glitch, often called the "millennium bug," or simply "Y2K," dates back to the 1960's and 1970's when computers were bulky in size but small in memory. To conserve limited space or memory, programmers began designating the year by using two digits rather than four. The year 1967, for example, appears as "67." The first two digits are assumed to be "19." Unless corrected, these date-sensitive computer systems and microchips embedded in countless mechanical devices may misinterpret the two zeros in 2000 as 1900, or just have sheer confusion with the "00." This confusion could cause the systems to generate erroneous information, corrupt other systems or possibly shut down.

Last week the subcommittee issued its seventh report card which showed considerable improvement throughout the Federal Government. Still, much work still remains. We will continue to steadfastly monitor the Federal Government's year 2000 readiness, prodding those departments and agencies that seem to be lagging behind.

I view our Department of Defense as the Nation's supreme national insurance policy. I sleep soundly every night, Mr. Secretary, secure in the belief that our national defense is the best in the world. However, the Department's biggest battle currently resides with its own computer systems that are paramount to its mission. The year 2000 technology challenge confronts many organizations, but Defense is especially critical to the Nation.

Given the Department's size and vital mission, today we will hear the testimony from Department officials about the status of the Department of Defense's year 2000 readiness. Since November, and as shown in our most recent report card, the Defense Department has reported modest improvement in making its mission-critical systems year 2000 compliant.

In December, the Department reported that 81 percent of its mission-critical systems were compliant. In February, the report of the Office of Management and Budget in the Defense Department reported only that 72 percent of its mission-critical systems are compliant. This discrepancy shows that either the Department has taken a huge step backward in its year 2000 readiness, or the Department is inconsistent in what systems are critical to its mission.

Either way, I am concerned about this inconsistency. I hope that we can clear it up this morning, as to what steps the Department of Defense is taking to solve its year 2000 issues. The Department of Defense also recently reported that it has more than 2,300 mission-critical systems. That awesome figure represents more than one-third of all mission-critical systems in the Federal Government.

In addition, at last report the Department of Defense still had to repair, test, and implement an additional 636 mission-critical systems. My concern is that while the Department has made good progress, there remains much work to be accomplished and the timeframe to do so is relatively compressed. January 1, 2000 will not wait for anyone, not even the U.S. Department of Defense.

This morning we will hear from the Defense Department's Office of Inspector General, which has gone over 140 reports on the DOD progress. We will also hear from the General Accounting Office, which has been doing outstanding work for this subcommittee on numerous Federal departments. Finally, we will hear from Dr.

John Hamre, distinguished Deputy Secretary of Defense, who has proved the importance of solid management leadership in solving the year 2000 challenge. I look forward to delving into all of these views and these issues this morning, and I welcome today's witnesses.

This is a joint committee hearing as I said earlier, with the Science Technology Subcommittee. I will now yield for an opening statement to the distinguished chairman of that committee, Mrs. Morella of Maryland.

Mrs. MORELLA. Thank you. Thank you, Mr. Chairman. I am pleased to participate with our subcommittee jointly with you in the latest installment of our ongoing series of joint hearings on the impact of the year 2000 computer problem on our Nation's public and private sectors.

This morning we turn our attention to a topic of very critical importance to the country, our national security. The very same doomsayers that initially told us that as the clock strikes midnight on January 1, 2000, planes will fall out of the sky, would also have us believe that missiles will be launched across the globe. We know that is not true.

Just as we have been assured by the Federal Aviation Administration that the safety of air transportation will not be compromised, we have already heard from the Department of Defense that Y2K will not cause our nuclear arsenal to inadvertently be deployed. What the millennium bug can do however, is potentially render our defense systems inoperable so that we would not be able to respond effectively to any challenges to our country's security.

In this age of weapons of mass destruction delivered by missiles and by terrorists, to be unprepared is to potentially jeopardize the safety of our Nation, and by extension, the world. The United States is a world leader, and we as a Nation are expected to lead the world. There is no alternative. For there is no other country capable of organizing against an Iraqi dictator who wants to get weapons of mass destruction. We are the one. There is no other country capable of sustaining freedom against a North Korean dictatorship actively seeking to get nuclear weapons. We are the one.

We cannot allow Y2K to compromise our Nation's military preparedness and readiness. We have American men and women who across the globe are protecting our Nation and the principles for which this Nation has been founded. For over 200 years, we have placed these men and women in harm's way to secure the peace with a covenant that if they provide their courage and skill, we will provide them with the effective equipment and support to do their job. We must not let the Y2K bug sever that covenant.

We must do all the we can to ensure that military hardware and the three "C's," command, control and communication, are not endangered as a result of this computer glitch. I am concerned about the IG and GAO reports that reveal the depths of the problems at DOD, especially the Inspector General's recent report about the haphazard Y2K certification of our nuclear weapons stockpile. Defense is not a sector that can be taken lightly.

Last year, Congress appropriated $1.1 billion specifically for the Department's Y2K efforts because we understand the importance of DOD's mission to our Nation. We will not allow for our national se-

curity to be jeopardized. We in Congress stand ready to help in any way that we can. It is up to Secretary Cohen and the President now to work with us to ensure that we can effectively maintain the peace throughout the world as we ring in the new millennium.

I look forward to hearing our very distinguished witnesses today. Thank you, Mr. Chairman.

Mr. HORN. Thank you very much. I now turn to the ranking minority member on the committee, Mr. Turner of Texas.

Mr. TURNER. Thank you, Mr. Chairman. I want to commend you and Chairwoman Morella for your leadership in trying to be sure that all of our Federal agencies are ready for the Y2K conversion process. It is a very difficult task for both the public and the private sector and certainly a great challenge for the Department of Defense.

As we know, the Department of Defense is heavily automated. It relies on more than 2,000 mission-critical systems. These systems span diverse operational areas ranging from the Department of Defense command and control systems, satellite systems, the global positioning system, all the way to detail systems relating to inventory, transportation management, medical equipment and payment and personnel records. Its weapons, equipment and facilities all contain embedded microprocessor chips, some of which may have the Y2K date problems.

As of February 1999, the Department of Defense reports that it has repaired, validated and implemented 72 percent of its mission-critical systems. However, that means that 632 mission-critical systems have not yet been fixed and implemented. As many as 220 mission-critical systems may miss the federally imposed deadline of March 31 of this year. The Department of Defense also has over 2,000 non-mission-critical systems that still need to be repaired. Clearly, there is much work to be done.

Last year, the Department of Defense Inspector General identified serious problems with the accuracy of some of the Department's reports on the number of Y2K-compliant systems. Today we will hear that the Department of Defense has improved its ability to track its Y2K work. But it will be difficult to know whether the Department has properly classified its systems as mission-critical or non-mission-critical until it completes its simulated year 2000 exercises and other planned testing. The Department of Defense faces a huge challenge in its Y2K conversion efforts due to a late start, the size of its systems, and their complexity. Although the pace of repairs and testing has been improved, the Inspector General cautions that the number and severity of Y2K problems at the Department of Defense cannot be quantified until, at least, June of this year, when additional test results will be available.

What is more, the Inspector General expresses the concern that the Department's Y2K testing may be rigorous enough to catch serious problems, given the compressed testing schedule. Each of us looks forward to your testimony today. We hope to hear more about the testing process, the operational evaluations that you have conducted to date and the Department's assessment of its own condition. I hope the Deputy Secretary of Defense will also address whether our weapon systems will be repaired in time.

The good news is that at the highest levels of the Department there is an increased focus on Y2K. The Department has seen great improvements in recent months. We appreciate each of our witnesses being hear today. Again, Mr. Chairman and Mrs. Morella, thank you for your leadership in this area.

Mr. HORN. Thank you very much. We will now yield for an opening statement to the vice chairman of the Subcommittee on Government Management, Information, and Technology and that is Mrs. Biggert of Illinois.

Mrs. BIGGERT. Thank you, Mr. Chairman. Thank you for your excellent work in putting together such a fine schedule of hearings to highlight our Nation's readiness for the year 2000. I too am committed to the oversight of our Federal departments and agencies. I am pleased that so many of our agencies are making progress in their efforts to become Y2K compliant. I am also concerned that some of our departments, especially those with critical missions such as our Nation's defense, have much work to do before they are ready for the year 2000 date change.

The Department of Defense operates about one-third of our Federal computer inventory. It has identified some 2,500 mission-critical systems. Yet, only 72 percent of these systems were Y2K compliant as of February this year. Admittedly, the Department of Defense faces a heavy burden to ready itself for the year 2000. Our Nation though is known for its military strength. Much of this military advantage comes from the United States' investment in information technology. However, it is this same technology that must be now updated, tested and readied for the year 2000 date change.

The Department of Defense, I believe, has made much progress in its efforts to ensure continued computer capacity in the new millennium. I am interested to hear today's testimony discussing the Department's progress on its command and control systems, satellite technology, global positioning systems and highly specialized management systems.

I, too, thank today's witnesses for coming to our hearing today. I look forward to the testimony and the opportunity for questions.

Mr. HORN. Thank you very much. I now yield to the gentlewoman from the Subcommittee on Technology, distinguished Member from Hawaii, Mrs. Mink.

Mrs. MINK. Thank you, Mr. Chairman. I have no prepared statement. I do want to say that this series of hearings that you have called, Mr. Chairman, on this very important issue is certainly keyed into the entire country's concern about whether this Nation is prepared for the looming coming of the year 2000. Nothing is more important, in my opinion, than hearing from the Department of Defense and all other agencies and entities related to our defense, to see where the status of readiness is with reference to this very important issue. So, I look forward to the testimony of all our witnesses who are here and hope that we have made considerable progress on the questions that have been raised last year and currently by the GAO. Thank you very much.

Mr. HORN. Now, the gentleman from California, Mr. Ose.

Mr. OSE. I do not have a statement, Mr. Chairman.

Mr. HORN. OK. Now we have the gentlewoman from Texas, Sheila Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, thank you for your kindness. I will only offer my appreciation to all of the chairmen and ranking members for holding this very vital hearing. Let me say, Mr. Chairman, I have found out by being in the District that Y2K now is the topic of discussion. This could not be a more vital area of oversight for the American people. They are looking to this Congress for guidance. They certainly are concerned about issues, not only of national security, which is the topic of this hearing, but our readiness overall. We have a responsibility I think, Mr. Chairman, not only to our citizens, but to the world. I will continue to work with you in oversight of this issue for our commitment to ensure the safety and quality of life that Americans have come to understand.

I would ask, Mr. Chairman, that I can submit my entire statement into the record. I thank you for the time.

Mr. HORN. Thank you very much. Our next opener is Mr. Miller of California.

Mr. MILLER. Thank you, Mr. Chairman. I really appreciate your conducting this hearing today on the status of the Department of Defense's preparedness for facing the technical challenges associated with the year 2000. Of all the agencies, DOD's Y2K compliance, to me, is of most great concern. If the dooms-dayers are right, and I am really praying that they are wrong about the seriousness of the year 2000 problem, failure of the DOD to inoculate their systems against the Y2K bug could pose many major domestic and foreign safety issues.

I am particularly interested in hearing from the witnesses on whether the DOD will be Y2K compliant and what the agency is doing to prepare our forces here and overseas against those individuals or governments who may try to take advantage of weak times. The questions are: are we prepared to defend ourselves, our deployed troops and our embassies? Moreover, are we prepared to assist our allies if they are attacked in the year 2000? These are important questions whose answers need to be addressed. Once again, Mr. Chairman, I thank you very much.

Mr. HORN. I thank you very much. Now I yield some time to the gentlewoman from Michigan, Ms. Stabenow of the Subcommittee on Technology.

Ms. STABENOW. Thank you, Mr. Chairman. I would just also echo the thanks to both you and our Chairwoman Morella for holding one more hearing on this critical issue. I have held two series of meetings in my district in Michigan, one last year and one this year. I find that the concerns certainly of my constituents have risen. It is important that we have accurate information so that people know how to prepare without overreacting and yet being prudent.

One issue that comes up over and over again is the Department of Defense, and grave concern about the progress that we have been making and where we will be. I am very anxious to hear today, and I know that my constituents are anxious to hear as well. I appreciate all of you being here.

Mr. HORN. I thank the gentlewoman.

The gentleman from Oregon on our side, Mr. Walden, waives his opening statement. We now turn to the other gentleman from Oregon, Mr. Wu.

Mr. WU. I have no opening statement, Mr. Chairman. Thank you.

Mr. HORN. All right. Both of you go to the top of the line in the chairman's view. [Laughter.]

Good freshmen, they are. They are excellent Members.

Now, we finally get down to business. You all know where we are coming from after our opening statements. So let me note to you that the tradition of the Government Management, Information, and Technology Subcommittee is to swear in all witnesses. So, ladies and gentlemen, if you will stand and raise your right hands. Yes, and by the way, all the people behind you will take a microphone so that I don't do this 10 times this morning.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all have taken the oath. We are delighted to have all of you here. Everybody knows this is the department about which we have the major concern, both for the good of the world as well as the good of the United States. So, we are going to start with the first individual from the Office of Inspector General in the Department of Defense, Mr. Robert J. Lieberman, who is the Assistant Inspector General for Auditing for the Department of Defense. Mr. Lieberman will make the opening statement.

Obviously, we would like you to summarize it. But, take your time if you don't want to summarize it. Give us the important things. A number of Members probably just flew in to vote today and have not had the chance to see the testimony. So, lay it all out there.

STATEMENTS OF ROBERT J. LIEBERMAN, ASSISTANT INSPECTOR GENERAL FOR AUDITING, DEPARTMENT OF DEFENSE; JACK L. BROCK, DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE; JOHN J. HAMRE, DEPUTY SECRETARY OF DEFENSE, DEPARTMENT OF DEFENSE, ACCOMPANIED BY GARY A. AMBROSE, DIRECTOR, AIR FORCE YEAR 2000; KEVIN MCHALE, DIRECTOR, YEAR 2000 PROJECT OFFICE, MARINE CORPS; STEPHEN I. JOHNSON, PROJECT MANAGER, YEAR 2000 PROJECT OFFICE, NAVY; MIRIAM F. BROWNING, DIRECTOR FOR INFORMATION MANAGEMENT, OFFICE OF THE DIRECTOR FOR INFORMATION SYSTEMS, ARMY; ROBERT F. WILLARD, DEPUTY DIRECTOR FOR OPERATIONS FOR CURRENT READINESS AND CAPABILITIES AND DIRECTOR, YEAR 2000 OFFICE, JOINT CHIEFS OF STAFF; AND R.F. SMITH, VICE DIRECTOR, NORAD COMBAT OPERATIONS

Mr. LIEBERMAN. Good morning, Mr. Chairman, Madam Chair, members of the subcommittees. Thank you for the opportunity to discuss the challenge confronting the Department of Defense because of the so-called "millennium bug." I would like to save time by verbally highlighting some of the significant parts of my statement and ask that the remainder be entered into the record.

Mr. HORN. I might say that every statement that anybody makes in any hearing is automatically put into the record the minute we introduce you. It is a unanimous consent motion, forever.

Mr. LIEBERMAN. Thank you. The task of ensuring that there is no significant impairment of the Department's ability to execute its missions is one of the most complex challenges ever faced by DOD managers. This is primarily because of the sheer magnitude of the DOD problem. In terms of size, complexity and diversity, no other public or private sector organization faces a Y2K problem of such scale.

In addition, with the benefit of hindsight, it is clear that the DOD Y2K conversion challenge has been made more difficult by a combination of half-a-dozen or so factors related to DOD management culture. The two most important of these factors, in my opinion, are first the legacy of very decentralized information technology resources management, which led to the runaway proliferation of systems. It has made it doubly hard to establish a well-synchronized and controlled DOD-wide Y2K conversion program.

Second, there was an initial tendency, particularly middle-management level of the Department, to view the millennium bug as a purely technical problem that could be solved by information technologists without a need for much involvement by managers and commanders.

The IG approached the Department's Chief Information Officer in early 1997 with an offer to help in him achieving sufficient oversight and management control in those areas considered to have the most risk. Based on the resulting informal partnership agreement, we have provided 50 Y2K audit reports to the Department over the past year-and-a-half. We are currently working on about the same number of additional audits. Summaries of a few of these reports are attached to my written statement.

In addition, we have coordinated Y2K efforts by the Military Department Audit and Inspection Organizations, which have issued over 90 reports in accordance with their own Y2K coverage agreements or tasking within their services. We have also worked closely with the GAO and exchanged information with our counterparts in several countries.

I want to stress this morning that generally DOD managers and commanders have been extremely cooperative and responsive to audit advice. This includes taking measures to ensure better accuracy in reporting. Top DOD management's encouragement of intensive independent auditing of Y2K progress and its responsiveness to audit results, positive or negative, deserve note.

Turning to the question of what these audits have shown. The DOD clearly 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 still 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 notions of modifying previously planned exercises to accommodate Y2K scenarios or of planning for other large scale testing.

The decisive turning point came in early August 1998, when the Secretary of Defense declared that progress up to that point had been insufficient. His strong and unambiguous message that Y2K was a genuine threat to readiness had the intended effect. The number of mission-critical systems that have been certified as Y2K compliant now stands at about 72 percent, as has been mentioned. Somewhat behind plan, but considerably better than the 24 percent figure from this time last year.

Equally important, efforts have finally accelerated over the past few months to assess the Y2K readiness of DOD-owned infrastructure, of the private infrastructure on which the 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.

With sustained close management attention through 1999, we in the IG's office are confident that the Department can achieve its goal of ensuring the continuity of critical operations and capabilities as the millennium passes. However, I want to stress that 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 still not be available for a few more months. It must also be recognized that the belated start in some areas has caused a fairly high risk level to persist there.

In our opinion, those areas of continuing concern include, first, the well over 600 mission-critical systems that remain Y2K noncompliant. Second, the infrastructure, especially overseas. Third, supplier readiness. Fourth, untested contractor off-the-shelf products. Fifth, contingency planning, particularly at the mission or functional level. Sixth, mainframe computer platforms and seventh, the greatly compressed testing schedules.

I would like to close with a few extra words on the testing challenge. The DOD Y2K conversion effort is unprecedented in many ways. One is the scope of the critical Y2K testing that will continue through the end of 1999. We cannot over-emphasize the need for robust, in-depth testing. The huge number of systems involved, the risk of incompatible Y2K fixes because of the number of different firms and individuals involved in remediating code, the late fielding of many remediated systems, and the compression of this ambitious testing schedule into just over a year, pose a formidable testing management challenge. In our view, effective testing is the most daunting of the remaining Y2K challenges.

In conclusion, we believe that the DOD is overcoming the increased risk posed by its belated start in 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.

Thank you, and I would be happy to answer any questions.

[The prepared statement of Mr. Lieberman follows:]

Hold for Release

Until Delivery

Expected 10:00 a.m.

March 2, 1999

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,

U.S. House of Representatives

on

The Year 2000 Technology Challenge at the 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.

Mr. HORN. Thank you very much. We are going to withhold all the questions until all the witnesses have testified. Our next presenter is Mr. Jack L. Brock, the Director of the Governmentwide and Defense Information Systems for the U.S. General Accounting Office, the auditing on both finance and program arm of the Congress and the legislative branch. Thank you.

Mr. Brock.

Mr. BROCK. Thank you, Mr. Horn. Thank you, Mrs. Morella and members of the two subcommittees. I am pleased to be here today.

Before I start, I would like to say that we have worked very closely with the DOD IG during the course of our audits and they have done commendable work and I think have added an immense amount of credibility to what the Department is trying to do to be Y2K ready. I would also like to say that if we had testified last year, our message would have been far more grim than it is today. I would like to congratulate the Department on an incredible amount of progress that has been made over the past year. A lot of that progress has to do with the very much increased level in presence of top management within the Department assuming ownership and control over the problem.

It still faces major issues in being year 2000 ready. I think this is a situation where the risks are so great and the need for insurance is so great, it is like going to a party and you don't want to risk your pants falling. Not only do you want to wear a belt, but you want to have suspenders on as well. What we would like to see here are the presence of additional controls that will allow increased assurance that risk will be minimized and that business processes and war fighting processes will work. We are no longer talking about systems, because the systems have to operate in an environment of business operations. These operations depend on a variety of factors, not just a system. I think the Department is moving into that realm, but we have a few items of advice.

Mr. Lieberman I think correctly described the complex organization that the Department is. It clearly, of all the Government agencies and possibly of any entity in the world, has the most complex set of operations to carry out. Many of the other hearings that you have had on Y2K have dealt with agencies that are primarily engaged in transaction processing, very complex operations that pale in light of the complex command and control, weapon systems, and other types of systems that the Department has to field and make sure is ready.

In that backdrop, I would also like to say that the Department has a history of very poor management over information technology. In fact, we would argue that some of its success has been the ability to tap vast sums of money to overcome problems in development. In fact, these poor controls in management process have limited the effectiveness of their Y2K program. I think there are lessons to be learned from this that we will address later, but this was an initial barrier to the Department in getting on top of its program.

I also agree with Mr. Lieberman that the program really began to turn around last summer when both Deputy Secretary Hamre and Secretary Cohen issued very strong letters to the Department saying, "We are running behind. We need to make fixes. We need

to start focusing on our key functional and operational capabilities to make sure that these functional and operational capabilities will be able to continue after the year 2000."

I would like to highlight a couple of things that the Department has done in that regard. First of all, it has had a very high level of involvement in ownership of the problem by senior management. Second, in turn the Department has now shifted its focus toward ensuring the continuity of core business processes and military operations. More specifically, I would like to identify five areas that the Department has done.-

First, last summer the Secretary of Defense directed the commanders-in-chief to plan and execute a series of simulated year 2000 operational exercises. These exercises are essentially to determine whether the Department can carry out critical military tasks with the systems' clocks rolled forward to the year 2000. These are such things as providing strategic early warning, deploying and maneuvering forces, and employing fire power. Thirty-one such evaluations are now scheduled through the fall of 1999. Second, the Department is requiring its principal staff assistants, these are the Under Secretaries and Assistant Secretaries that own the functional areas of the Department or have responsibility for those, to conduct end-to-end tests to ensure that the systems that they have collectively support core business areas and can inter-operate in a year 2000 environment.-

The Department originally designated five functional areas: communications, health and medical, intelligence, logistics and personnel, and has since added weapons and finance to those functional areas. Third, the military services commanders are conducting integration testing of their systems. This testing is intended to build upon completed systems renovation testing and certification, and ultimately is designed 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 the 600-plus installations scattered all over the world will be ready to house both the military and civilian work force, as well as the weaponry and supporting activities that are necessary for national defense.-

As you can gather from these four things, they are pretty complex and diverse. Last, the Department has initiated what they call "synchronization meetings" that are chaired by the Deputy Assistant Secretary of Defense and the Joint Chiefs-of-Staff Year 2000 Task Force leader. These are designed to improve and facilitate coordination of the activities that cut across organizational boundaries.-

Because of the complex interrelationships between these activities, we have recently begun additional audit work, Mr. Chairman, to look at those relationships and to see how well they are being carried out. While we don't have a complete answer on their success or on their progress, we do have a number of observations that we are prepared to make on those.-

First of all, I would like to say that the initial operational evaluations carried out by the CINCs have been successful. The guidance that was provided by the Joint Chiefs-of-Staff was excellent. It was very much in line with our own criteria and we found it very

useful in conducting our audits. The exercises that have already been conducted at NORAD and the Strategic Command have gone pretty well. Last week I had staff at NORAD and they were looking at NORAD's test of the missile warning operational evaluation. My team there said that the test worked. It was primarily to look at processing responses to airborne threats.

The operational evaluation was very carefully planned. They followed the test script. The results showed no Y2K failure. There were a number of relatively minimal system failures that were not related to Y2K. The staff and personnel at NORAD were able to take care of these and to successfully move the test on. As the course of these operational evaluations continue, we will continue to follow their progress as well.

However, because of the interrelationships of systems all across the various commands and all across the functional areas of DOD, many of these planned evaluations will require extensive support from the functional areas, such as communications and logistics. For example, when we were talking to officials at the Strategic Command, who were doing a five-phase operational evaluation program, they indicated that they required extensive support from DISA. DISA is the agency within the Department of Defense that supplies communication and computing support. They provide support to the Strategic Command on its communications backbone. The initial phase of this plan had to be delayed because of one of DISA's programs not being ready for testing. There are all sorts of dependencies that exist among these tests that have to be carefully monitored to make sure that the tests can be completed.

Finally in this regard, our initial reviews of the plans for functional areas, these are the health, personnel, finance, logistics, et cetera, show these plans have mixed results. Our review has shown mixed results. For example, while each of the functional plans discusses business functions supporting systems and testing requirements, many of the plans lack important details such as a test schedule, complete data for contingency plans or detailed mapping of systems and support activities to business functions.

While DOD has correctly shifted its emphasis to continuity of business processes rather than the status of individual systems, its controls and reporting mechanisms are still centered around individual systems. To effectively manage the program in the future, we believe that managers and executive decisionmakers need reliable information about the nature and status of year 2000 conversion efforts from a core business process. This isn't readily available in DOD.

For example, although the functional areas and commands have been instructed to develop testing and contingency plans based on business functions, the overall DOD Y2K management plan and supporting guidance have not been updated to reflect reporting and control mechanisms that need to be in place to reinforce this shift in focus. It is entirely conceivable that every component, every command and every function is developing appropriate plans with an appropriate level of control to ensure that the right thing is being done at the right time. There is simply not a mechanism to provide assurance. Our reviews, for example, of the functional plans, sug-

gest an uneven level of planning and execution across the Department.

We believe that the Department needs greater visibility into the core business processes throughout the agency. Specifically, for each core business process identified, the Department should determine the following. First, the status of each supporting information system critical to that process, including its schedule for remediation and testing—this information is largely being gathered now. Second, the source and year 2000 status of any suppliers or vendors that are critical to that process. Third, the status of outside dependencies that affect readiness. Fourth, interfaces with other processes and outside organizations. Fifth, the scope and schedule of end-to-end testing for the process. And sixth, the scope and schedule for business continuity planning for that process to continue.

For any of these elements that are behind schedule, Defense needs to know what steps will be taken to get the schedule back in line, and what steps will be taken to minimize the risks that might be associated with delay. Once the assessments are complete, the Department is going to be in a better position to take an overall look at their prospective readiness; to identify gaps or unnecessary overlaps; to reallocate resources, if necessary, and to 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 needs to provide standard expectations for both content and reporting requirements and performance metrics for all of the above elements, and to establish control mechanisms that ensure reported information is both complete and accurate.

Finally, just to make a few remarks. I mentioned earlier that GAO has long had a concern with the Department's information management. In fact, since 1995, this area has been on our high risk list. One of the major barriers to effective information that we have observed within the Department is their inability to cut across stovepipes and overcome cultural inertia to change. They have plenty of processes, but no action.

I think now we are seeing a shift. In the Y2K program, we have seen a lot of shift in management attention, willingness to cut across program lines—maybe not as many processes as we would like—but a real shift. The lessons learned from Y2K can be transferred to their overall management of information technology. While this might be an expensive lesson, it will be an important one, and hopefully worthwhile for the Department.

That concludes my statement, Mr. Horn.

[The prepared statement of Mr. Brock follows:]

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

GAO/T-AIMD-99-101

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the Department of Defense's 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 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

[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.

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 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

[4] See attachment for a listing 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.

power, water, transportation, 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 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.

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

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 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

[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

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 personnel.
- 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.

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 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

[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 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 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 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.

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

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 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.

[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).

- 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.

Attachment

Attachment

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).

(511657)

Mr. HORN. Thank you very much, Mr. Brock. The GAO always gives us a lot of helpful comments. We appreciate it.

We now are going to the Deputy Secretary of Defense, Dr. John Hamre, who is accompanied by a number of the program directors. Now I am going to sort of have to juggle things here to let the Deputy Secretary of Defense get back to work, because he is going to be back up here this afternoon.

Mr. HAMRE. I have another hearing.

Mr. HORN. So, I think I am going to ask one question here, and then give the statement. Then every Member will have a shot at you here, so to speak. I would just ask this. You have heard the IG and you have heard GAO. Do you have any reaction to their testimony at this point?

Mr. HAMRE. Sir, I have a couple of reactions that I think will come out in the context of the statement that I am going to give.

Mr. HORN. OK, fine.

Mr. HAMRE. By and large, we have had a very open process. We meet on a monthly basis, and Jack Brock sits through these endless sessions with me and has been at every single one of them. I have been grateful to have him there, as has Bob Lieberman.

Mr. HORN. And he hasn't won the Scowcroft Award by going to sleep or anything? [Laughter.]

Mr. HAMRE. No. He has woken me up a few times, I must say. I really thought this was going to be a hostile hearing, at first. You started with an accusation that over at the Department we had too much bulk and too little memory. I thought you were talking about me.

Mr. HORN. I was talking about the 1960's computers.

Mr. HAMRE. OK. Yes, our computers. I'm afraid I might qualify as well. [Laughter.]

May I say at the outset, that the most important people—the Secretary, you are right, was the catalyst that got the Department focused. But we have four kinds of catalytic converters here. It is Art Money, who is going to replace me when I have to get up and leave, and he is our Assistant Secretary of Command Control Intelligence; Marv Langston, who is his Deputy, has really been riding shotgun over this, and his trusty agent, Bill Curtis, has been doing absolutely all of the legwork for the Secretary. Bob Willard here has been for the Joint Staff, really pulling the test environment together. These are the four individuals that I needed to highlight to you. They have been absolutely instrumental and have done a terrific job. I will ask Art to step in, very briefly, after I leave.

Sir, it is rare that any military organization knows exactly the time and the place when the enemy will attack. Indeed, we are largely preparing ourselves, in the strategic sense, for opponents that we will confront. Rarely do we know exactly when the enemy will attack and exactly where the enemy will attack. This is an exception. We know exactly where it is going to be and we know exactly when it will happen. It isn't a matter of just computer geeks not keeping our computers running. It is warriors, like Bob Willard and others, who are not going to be able to do their job if we are not ready. So, this is not about management. This is about being able to protect and defend the United States of America.

I would like to put the bottom line right up front. We will be able to protect and defend the United States of America on January 1, 2000, and on the second and on the third and every day after that. That is not just our computer systems that run personnel records or accounting. That is our war machines, those things which will go out if we have to ask them, to take to combat the enemy. We will be ready. I will go through that today.

With your permission, sir, I would like to go through a series of charts just to try to illustrate what it is we are going to do. Can I get the first chart please?

[Chart shown.]

Mr. HAMRE. This is where we stand right now and this is the progress. If it is red, it is what we have reported. If it is the dash line, it is where we are against our totals. We have 2,300 systems that we need to have fixed if we are going to be able to carry out our missions. This is across the board. This is everything from an aircraft carrier and all the systems on the aircraft carrier, to intelligence systems, to accounting systems, to finance for payroll, the whole works.

At the end of December we had 1,673 systems. Today, I think it is 1,730, something like that; 1,722 systems are fixed as of today, and validated as being fixed.

Mr. HORN. On that point, "fixed" and "validated," is there room for testing here?

Mr. HAMRE. Yes, sir. That is all going through with the systems testing, not the end-to-end operational functional tests that Jack was talking about. But it is systems testing. So before they can ever get permission to be put on that column as being "filled," they have to be fixed, and an independent source has to validate that it has been fixed.

As you can see, we are stretching out. You will see by the next chart we will be in 90 percent, 93–94 percent here by the end of March. We will make 100 percent of our goal by the end of the year.

Let's go to the next chart, if we could.

[Chart shown.]

Mr. HAMRE. Seventy-three percent of the systems were totally fixed and fielded. You see these bars here that have that little shaded area at the top? That is meant to represent that the system is fixed, but is not completely fielded. So, Brother Johnson is here with all of the ships out in the Navy. Not all of the ships may be completely fitted with a fix. But those that are going to war will be fitted. What you are seeing here of that differential is the difference between: we know the software works. We know it works when it is installed, but it isn't in every single ship, for example. Or it is not every piece of equipment. As you can see, it narrows down and gets smaller.

By the end of the year, we will have six systems that are not going to be year 2000 compliant out of the 2,300. In those six, the fix is done. It is just a fielding issue. The ship may not go to sea for another 14 months. So this is just an example of it's fixed, not fielded. But it doesn't matter. OK?

As you can see, we will by March have 93 percent of the systems fixed. What I would like to do is to show three followup charts that illustrate how we are tracking individually.

Let us go first to the Army.

[Chart shown.]

Mr. HAMRE. First of all, the bar when it is red, it is still being fixed. When it is green, it is fixed but is still being fielded. So as you see, the top three systems will all be fixed. They will be fixed by the summer. It just takes virtually a day to get it installed. It does not take any time.

For the systems below that, as you can see, there tends be a longer implementation period. But in each case, we have got the fix largely in hand and it is just being fielded.

Now these are the 10 most important systems out of the Army. There are 24 all together that are not fixed right now. These are the 10 most important. We are tracking every one of them. We have got witnesses here that know every single fix, down to where the electrons go. So if you want to ask any questions about them, we can.

Mr. HORN. I understand from staff that we don't have these charts.

Mr. HAMRE. Be glad to give them to you.

Mr. HORN. I would like them put in the record at each part of your presentation. I realize your color charts are way ahead of the congressional and GPO charts. We have a little problem distinguishing green and red. It is always in versions of black.

Mr. HAMRE. I understand. We will annotate them. Could we go back to the previous chart? I just wanted to make a point on something.

Mr. Chairman, in your opening statement you said that we were reporting 81 percent fixed, but the report that you got from OMB said that we were only 62 percent fixed, or something like that. I will tell you what the problem is. It is a useless reporting requirement that is not doing anyone any good. We submit these reports. They are a couple of months late by the time it goes through all the building and writing a thick, darn report. Our preference would be to have your staff come over and sit in on our monthly sessions. You can see the data the day we do it.

Mr. HORN. I think some of them have.

Mr. HAMRE. Instead of us generating a report that is 2 months late and does not give you information and just confuses you, thinking that we are slipping back, I would rather have you there looking at the stuff we are looking at. It would make a lot more sense.

Mr. HORN. I will take your invitation up. We have had staff in your meetings.

Mr. HAMRE. Yes, on several of them. We would be glad to have them attend our monthly meetings. It would be great.

That is where we are today, 81 percent. We will be at 93 percent. We will make 100 percent.

OK, let's go two down to the Navy charts, if we could.

[Chart shown.]

Mr. HAMRE. Same situation, where we are showing you the 10 most important. In this case, as you see, largely it is a fielding

issue. If it is a long, green bar, it is largely a fielding issue. In very few cases, for example the backup mission planning system for Navy SpaceCom, is one that is late. It is a backup system. It is not our primary control system for our satellites.

OK, next chart. Let's go to the Marine Corps.

[Chart shown.]

Mr. HAMRE. Only three systems. The thin red line. You know they don't have much, but they are getting it fixed. It is going to be just fine.

OK, next chart, Air Force.

[Chart shown.]

Mr. HAMRE. Air Force is doing very well. As you can see, it is largely fielding questions and will easily be done. Mrs. Morella mentioned GPS, or Mrs. Biggert mentioned GPS. GPS will be fixed. We have a somewhat additional, different problem. There is a thing called the "end of week" problem that occurs this fall which we have fixed. The satellites are fixed. The ground stations are fixed. The Government-licensed receivers are fixed. But if people have made a non-licensed receiver, they may have problems. We have been trying to advertise this because it is an important technical detail associated just with the GPS system. But we will be ready. Any war machine will be ready for it. Again, we would be glad to go into any of the details behind any of these.

Here is where we are with nuclear command and control systems. As you can see, the green bar is where it is completed and totally fixed. The yellow is where it is completed and not completely fielded. As you can see here, by the end of March we are going to have all but 12 systems completed, some in some various phase of fielding. This is absolutely everything. This is from the early warning satellites, to the radars, to the command and control displays at NORAD here in town, down to the mission planning systems for the nuclear systems, down to the stewardship custodial systems that we have for individual warheads. Everything is being tracked. We will be done and fully tested by the last quarter of the fiscal year. There is no risk that the Department of Defense cannot manage and control its nuclear weapons.

OK, next chart.

[Chart shown.]

Mr. HAMRE. I just would like to take a moment to explain. There is a proposal that we have made to our counterparts in Russia. We are not worried about their control over their nuclear weapons. This is a country and a government that has emphasized control over everything else. We are absolutely convinced that there will be positive control over nuclear assets. We are less optimistic that their early warning systems will function. We don't think the early warning systems are all of a sudden going to show satellite tracks of attacking warheads or anything like that. We don't know how you would go from a computer glitch to trajectories of an attack profile. We don't think that will happen.

But it is possible that computer screens could go blank or could be interrupted. In this world, we are not interested in having a lot of confusion and doubt. So we have approached our counterparts in Russia and have invited them to join us in a center for Y2K strategic stability. We will have an early warning center. We modeled

this after the air traffic control center that we operated in Berlin for 25 years.

For 25 years, when Berlin was still a divided city, the United States, Russia, France and the United Kingdom jointly operated an air traffic control center so that there would not be any confusion in people's minds about aircraft coming in. Every airplane had to be logged in advance. There were coordination procedures. We felt that the best thing to do was to do that together in one room. That is our model for this. We will be ready this fall. We will be ready in the last quarter. We have invited our counterparts from Russia to come over and join us at the center. They will have their own communication links so they can get back home secure, on their own. They can look at our machines just in case there is any disruption that they might have. We think that this is an important contribution to stability. This is something that we are pursuing quite aggressively.

Mr. HORN. I would agree with you. Have you had a reception of this that is positive?

Mr. HAMRE. Sir, yes, we have. There has obviously been a bit of concern by both parties. You know, we are anxious to have them join us. We have to do it in a way where they cannot look back up our system and determine what the configuration of our system is like and any vulnerabilities it might have. Similarly, they are always apprehensive that this is somehow a plot, you know. We are going to spy on them or something. So there is a natural reticence that always comes when we approach things like this.

We just had a team over, I think it was a week ago. They had very good discussions. There are going to be followup discussions, I think, next month. We have been talking with them more widely about year 2000. Mr. Money can describe that to you because of our efforts with them. But I think that we have received a good response. I rather think this is going to happen. I think it is a confidence-building measure that both parties understand and think would be important. I might say that I think we are prepared to offer this to other countries too, if we feel that we need to provide a reassuring environment.

Mr. HORN. Well, that was going to be my next question. What about some of the nuclear countries that are not too cooperative with us?

Mr. HAMRE. I think our view is that this is a stabilizing contribution that would be useful to others. We of course have to work this out collaboratively. We are open to discussing that with people. There are no impediments on our side to wanting to talk to people about that.

OK, let's go to the next chart.

[Chart shown.]

Mr. HAMRE. I'll break this down. This is just general timelines. There is no real precision to it. The axis at the bottom shows you the dates. We started the remediation some time back. It will continue right up until probably November. I think some of the last systems do not field until probably November. There has been contingency planning going on along at the same time. Every one of these systems has to have a contingency plan if there is failure. These are the gents at the table here that are the individuals re-

sponsible for developing those contingency plans, if we have problems.

Operational testing has begun. As a matter of fact, I will ask Admiral Willard to describe a test that he just observed out at our Southern Command. I would ask your permission, Mr. Chairman, for Colonel Smith to give a brief report on the test we just did at NORAD, both in December and just last week, to give you a sense of what the operational testing environment is like.

We have designated the Y2K operations period from I think it is September 1st through March 31st. There will be a special command and control, as it were, over our systems for that period. I will describe the significance of that by going to the next chart.

[Chart shown.]

Mr. HAMRE. What you see here are test periods. Again, the axis on the top shows you the months of the year. On the vertical axis is our various military war fighting command. So, USACOM is the Atlantic command. There is a Central Command, the European Command, the Pacific Command, Forces Korea, all of our CINCs. What the Secretary did was he said, "This is a war fighting issue. Are we going to be able to defend the country or not? I am going to put the CINCs in charge of testing, because they are going to have to live with the results." The first sense of discipline in the system was to say that we were not going to take anybody's word except for the guys that are going to live or die if it does not work.

We put the CINCs in charge of testing. These are the test windows. We are going to just discuss one of them when I ask Colonel Smith to do it, down where you see where it says "NORAD," the third up from the bottom. There were some tests that were done back in December. He has just done some tests in February and I will ask him to give a brief description. We are doing literally hundreds of tests. This is the most sophisticated testing environment that has been established, I think, in the Department to prove out that this stuff works.

Let me go to the next chart.

[Chart shown.]

Mr. HAMRE. This shows you the testing that is being done in functional areas, not just the war fighting systems. Now let me go down in, for example, Finance. I used to be the Comptroller, so I was concerned about this. An example of what we are doing in Finance is that we are doing an end-to-end test where the payroll clerk will leave an earning statement for an individual and will see that those electrons get over to the Defense Finance and Accounting Service to authorize payment. That will go to the Federal Reserve, which will take the electrons and pass them to the banking system. The banking system will route them to a correspondent bank, the correspondent bank into the service member bank. Then we will see if all of the accounts clear.

That is the kind of end-to-end testing that we are doing, for example, in the finance world. We are doing that kind of end-to-end testing in each one of these areas. It is very extensive testing going on here for the next 4 to 6 months. Now, generally, you will see blocks. Some of them are designated as backup blocks in case we uncover some problems. So far, what you will see is that the testing has gone fairly well. In other words, the test fixes that we iden-

tified when we did the systems tests and proved in the systems tests have carried over to the end-to-end tests. That has largely been our experience.

We have also found that in the systems tests that some of the commercial products that we have been given that were told were fixed, really were not fixed. We were able to quickly identify what the problems were. This kind of a rigorous test environment is letting us get on top of the problem and be able to get things turned around very quickly.

Before we go to the next thing, I wonder if I could just ask Admiral Willard to talk briefly about his experiences he just had watching the SOUTHCOM test.

Admiral WILLARD. Good morning, sir. I would like to talk about a test that was conducted by the Commander in Chief (CINC) of Southern Command (Southcom) and it had to do with their mission in performing counternarcotics operations. Specifically in support of that mission, they were examining their ability to detect, track, and monitor both aircraft and vessels on the sea, as well as source-zone targets in the countries of South America. They examined their abilities to hand off to their joint counterparts, as well. It was a collaborative effort between headquarters of SOUTHCOM and the interagency task forces that exist to support counternarcotics operations radar site, as well as aircraft and ships at sea that were participating in the exercise.

In all, they tested over 30 systems, of which 24 in the architecture included clocks or date functions. They encountered no hard failures in any of their systems. They encountered one, what they termed a "soft failure," that was year 2000 related, having to do with a message handling system and specifically, an archive function of the message handling system. Though it did not impact their operations, it was nonetheless considered a Y2K minor failure. They also uncovered a couple of other systems failures that were not associated with the year 2000 but, interestingly, were date functions within all of the systems, whether they had Y2K related clocks or not. So they were uncovering a good deal about themselves.

They published some very good lessons learned that we are sharing with the other commanders in chief, the unified commanders, who are readying for their own operations evaluations. Also, in their preliminary report, they reported a number of ancillary benefits that they have derived from this entire process: a better understanding of their own architectures; a better understanding of how they interact with their supporting agencies; in fact, a better understanding of their entire mission area. We are finding that we not only derive benefits in terms of our confidence level and our ability to deal with the year 2000 issue, but we are deriving a number of other departmental benefits, as well.

Mr. HORN. Well, I am delighted to hear that because I have visited the Southern Command about 2 or 3 years ago, and watched what they have been doing on narcotics. I was very impressed with the coordination that has finally been occurring over the last few years among all relevant agencies.

Have we still got so many flights ending up over the waters of Puerto Rico that we had 3 years ago? It is really unbelievable.

Admiral WILLARD. The answer to that is, yes, sir. We are continuing to be successful.

Mr. HORN. I am impressed by that end-to-end testing. I think that has been our worry from day one. I agree with you completely. This ought to be an exercise which cleans up the management flow-through of decisionmaking and other things. Get rid of some and keep the others. I hope that exercise has been just what you say it is in other commands.

Mr. HAMRE. Sir, we will give you an example of that just shortly. If I might go to, I think this is the last chart.

[Chart shown.]

Mr. HAMRE. I would like to explain something. We are shifting over our focus. By the way, I agree with what Jack Brock said to you. We do need to shift our focus from systems now to functional agencies. I think we are doing that. I will be glad to sit down with Jack to figure out if there are some things we need to improve in our process. I think that is the right focus.

I would like to shift and conclude here by saying if there are going to be problems, the Department of Defense is going to get asked to try to help remediate them here in the United States.

FEMA doesn't have its own helicopters. We have helicopters. When there is flooding, they ask us to show up and do the relief activity. If there are hurricanes that come ashore, we are the ones that set up the tent cities and pump the clean water and deliver food. So we know we are going to be called to respond if there are problems in the United States.

We also know that we have to have a process where we do not respond and put at risk our ability to fight a war if we have to. So we have developed a system of priorities. The Secretary has approved this. We can allocate our resources, at least think about them in a rational manner, when we are responding to the consequences. Our first priority is to fight and win a war, if we have to.

First of all, any unit, right now, its day-to-day mission is to carry out an on-going military operation, to carry out on-going intelligence operations, to protect and support the national command authorities, to do those kind of "survival of the Nation" functions. Any unit that is assigned to do that may not divert its resources to anybody for anything, without getting the permission of the Secretary of Defense. That is priority No. 1.

Priority No. 2 is any organization that is an early deployer for a war, if we have to get involved, and by this we mean within the first 60 days, we will let that unit commander help out locally. But they may not consume material, resources, and supplies that cannot be recovered within 60 days, without getting the permission of the chairman of the Joint Chiefs. We are not going to compromise or sacrifice our ability to get ready to deploy for a major war if we have to.

After that, all commanders are authorized to make resources available to help out locally. There is going to have to be some rationalization process. We think that the next most important thing is, priority No. 3, supporting our sister agencies in the Federal Government. We don't want to have a problem with the Federal penitentiaries. I am not forecasting there will be, but that is clearly

an area where we are going to be helpful if we are asked to be helpful. We want to help our brethren in the Customs Service if something comes up in the FAA.

Let me give an example. We have the ability in the Department of Defense, of course, to set up our own air traffic control. When we send a deployment, for example, to Bosnia, we don't necessarily trust the local air traffic control system. So we set up our own, complete with air traffic control towers and radars, approach radars, et cetera. We can do that for several dozen locations at once. If we have problems here in the United States, we are prepared to help set up air traffic control. But we need to know that we are not going to do that and put at risk our ability to support a war plan. It is that sort of rationalizing of scarce resources so that we can make sure we can do it without jeopardizing our primary mission. That is the purpose of this process.

Mr. HORN. Has the FAA Administrator or the Secretary of Transportation asked for help?

Mr. HAMRE. Sir, no, they haven't. Everything we hear, and again I am taking my knowledge from talking in detail with John Koskinen, and John sits in with our monthly sessions, that we think they are going to be OK. There could be some problems with regional airports, more at the local level. We don't know that yet. I know that that is very much what they are turning their focus to.

Again, we are saying that we have assets. We will support. We will provide the supporting activity for the rest of the Government. We are first going to have a process to make sure that we can afford to do that from our primary war fighting mission.

Mr. HORN. Well after this hearing is over, I am going to phone up and see why they aren't calling you, because they should.

Mr. HAMRE. Well, sir, I think our preference would be is that we do this together through the process John Koskinen has set up for the Federal Government, rather than them just call us directly. Of course they can call and we would be glad to respond. We would like to have it in a coordinated manner through John. John is doing a terrific job. We think that mechanism could work and could work fairly well.

OK, I think that here is where we are. We will be ready on January 1st. As I said, there are only six systems, and they are not crucial for going to war because the systems are not going to be going to war. Our war fighters are responsible for testing. So if there is a problem with the guys that are going into combat, they have a responsibility for telling us we have a problem. There are contingency plans in place for every one of these systems.

Infidelity. This was one of those issues we worked earlier in the year. I know the fidelity was less than it should have been earlier. I think it has improved. I will have to rely on some continuing input from the IG and GAO to help us identify that. We are very open to doing it. The nuclear command and control system is fixed, or is going to be fixed. It is going to be very scrupulously and rigorously tested. We are prepared to support domestic activity and overseas activity, if necessary. We are going to have to do that in a very disciplined way. We have got lots of assets, but we don't

have anything close enough to cover it if it is a very, very widespread problem.

Now, sir, with your permission I would like to ask Colonel Smith to give you a summary of the testing that we did, one of those little boxes. This was the little box that we did out at NORAD. It was really the first, lead sophisticated testing. If I could indulge the committee to take this briefing right now.

[The prepared statement of Mr. Hamre follows:]

Statement of

JOHN J. HAMRE
Deputy Secretary of Defense

Before the

Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
United States House of Representatives

On

PROGRESS TOWARD YEAR 2000 COMPLIANCE

March 2, 1999

Table of Contents

List of Figures

Introduction

Thank you Mr. Chairman and members of the Committee. I am honored to be here. I am pleased to have the opportunity to discuss the potential impact of the Year 2000 problem on the Department of Defense again this year. I am also pleased to report that DoD will continue operations and maintain military readiness before, during, and after 1 January 2000. Today I would like to review briefly how the Y2K problem affects the Department of Defense, summarize our efforts in 1998, highlight our plans for 1999, and finally, outline how our work on Y2K will affect future DoD information technology operations.

The Y2K Problem

I think by now everyone is familiar with the origin of the Year 2000 problem. In the 1950's and 1960's, computer programmers, in order to reduce the need for expensive computer memory, developed the convention of storing dates using only two digits for the year, assuming that the software would be replaced long before the Year 2000. However, the silicon chip and our dependence on computer software have become so pervasive that legacy systems rarely were replaced; they just grew. The Year 2000 problem affects four aspects of computer systems: software, hardware, firmware, and embedded chips.

The Year 2000 problem is an especially large, complex, and insidious threat for the Department of Defense. We are an organization with roughly the population of metropolitan Washington D.C.; the complexity of a small nation; the resources to sustain a global reach; and an information infrastructure that relies heavily on old, legacy computer systems. The Y2K problem is particularly critical because of DoD's dependence on computers and information technology for its military advantage. The Department of Defense helped nurture the computer industry, but now we must deal with the difficulties generated by retaining legacy systems.

As you know, of all the Departments in the Federal Government, DoD has the largest number of computer systems. These are not simply weapons systems, the category best prepared for Year 2000, but command and control systems, satellite systems, the Global Positioning System, highly specialized inventory management and transportation management systems, medical equipment, and important systems for payment and personnel records. The complexity of DoD operations results in an enormous scope, variety and number of information technology systems, all potentially vulnerable to the Y2K problem.

As of the 8th Quarterly Report to the Office of Management and Budget, DoD has approximately 9,900 systems, of which 23 percent (or approximately 2,300) are active mission critical systems. DoD also operates over 600 military bases, which are much like small towns, where the infrastructure is also vulnerable to Year 2000 problems. Due to our extensive reliance on information technology systems, there are severe consequences for not meeting deadlines for Y2K preparedness. As a result, DoD spent much of last year getting its act together on fixing systems.

DoD's 1998 Focus – Fixing Systems

As I testified last June, we spent much of 1998 getting a management structure and strategy in place to focus DoD efforts on Y2K. I'd like to review our management efforts and then go over our progress towards Y2K compliance through the end of 1998.

Management Focus

Our management efforts last year were focused on four key enablers: publishing a DoD Management Plan for Y2K, implementing effective management oversight, making Y2K a Chief Executive Officer (CEO) problem rather than a Chief Information Officer (CIO) problem, and getting accurate reporting mechanisms in place.

DoD Y2K Management Plan

We developed and published a DoD management plan that specified responsibilities for fixing Y2K problems and outlined DoD use of the five-phase OMB process for attaining Y2K compliance for systems. We also made some key decisions about how to track "systems" at the Departmental level as well as categorizing systems as either Mission Critical, Mission Essential, or Non-Mission Critical. This categorization was initially done by information technology specialists on CIO staffs and provided an initial screening and prioritization mechanism. Through the last quarter of 1998, that list was reviewed and scrubbed by CEO staffs and became a much more reliable management tool.

Effective Senior Management Oversight

Every month I chair a DoD Y2K Steering Committee meeting to review our progress toward achieving readiness for Y2K. Senior leaders from across DoD attend, to include Service Under Secretaries and Vice Chiefs, Principal Staff Assistants (PSAs) from the OSD staff, and department and defense agency CIOs. These meetings provide a corporate assessment of collective progress, a mechanism to address key management issues, and a mean to reinforce that Y2K is a CEO problem, not a CIO problem.

CEO Involvement

The key event in energizing the Department's CEOs was publication of Secretary Cohen's 7 August 1998 memorandum. This document firmly fixed responsibility for ensuring DoD's capability to continue operations regardless of the Y2K problem on the shoulders of the Department's CEO leadership. In addition, on 24 August 1998, I issued a memorandum that further specified responsibilities for testing of functional capabilities, certification of systems, and verification activities among the Chairman of the Joint Chiefs of Staff (CJCS), Commanders-in-Chief (CINCs), PSAs, Defense Agencies, and Services. A key element of our ability to track progress in these areas was implementation of a common DoD database of systems.

Accurate Reporting Mechanisms

As has been frequently noted in many reports, DoD had to work hard to establish a stable baseline and list of systems against which to measure progress. Based on some extremely hard work by people throughout DoD, we have significantly improved our ability to track Y2K compliance from a single authoritative database. The culmination of those efforts is captured in

the reports on our progress contained below. We are pretty much "there" in getting our reporting mechanisms sorted out. Some additional work remains to be completed to ensure we can accurately capture the results of our testing and evaluation efforts taking place this year.

Progress Report

Through much of 1998, DoD's engagement in Y2K preparations was extensively documented in numerous reports. We have made significant progress from our former 'Tier One' agency rating. I'd like to quickly review our progress against our original plan, where we are and plan to be on key milestones, and finally, talk about our nuclear systems.

Our Plan and The Results

The Department has made steady progress in Y2K compliance for mission critical systems. Figure 1 (below) summarizes DoD's actual progress against our October projections. DoD showed significant improvement during the last quarter as we approached our self-imposed deadline of 31 December for mission critical systems.

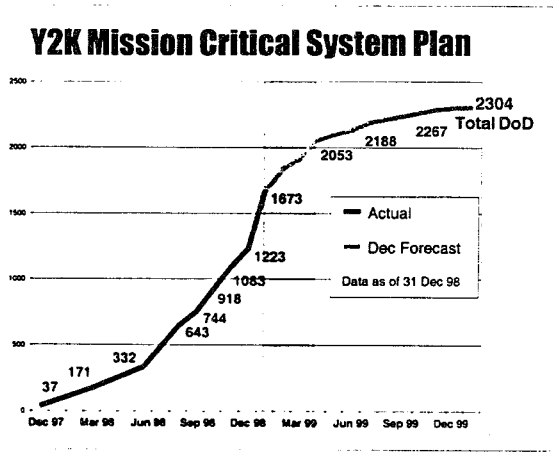


Figure 1 DoD Y2K Compliance Forecasts and Results

Status at Key Dates

As you can see from Figure 2 (below), on 31 December 1998, 81% of our systems were validated as being Y2K. Of that 81%, approximately 8% were still in the process of being fielded. In addition, DoD forecasts that approximately 93% will be fixed by the OMB deadline of 31 March 1999. Of that 93%, approximately 4% require further fielding beyond that date.

For systems that did not meet our internal DoD deadline or will not meet the OMB deadline, we have implemented an exceptional measure of management focus and oversight. The status and impact of systems that slip or will be completed after 31 March 1999 are briefed to me at each Steering Committee meeting. While it is impossible to prevent all slippage, we are working hard to ensure every system that can be completed in time for CINC, PSA, or Service testing and evaluation makes its target date. Systems that continue to slip may have development and fielding efforts frozen, particularly if intended to replace an already compliant system.

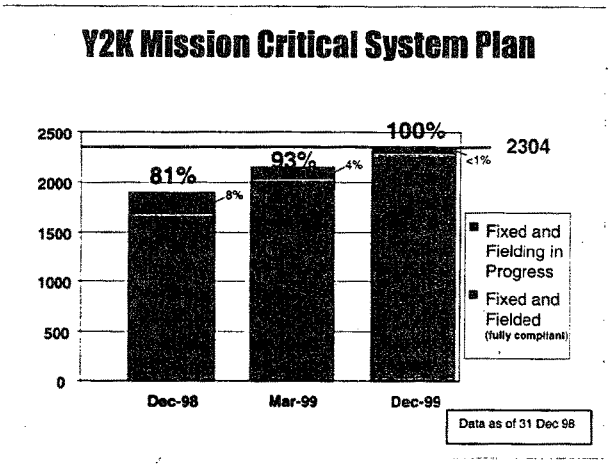


Figure 2 DoD Status at Key Milestones

Nuclear Systems

I would also like to take this opportunity to state unequivocally that our nuclear command and control system has been thoroughly tested and has performed superbly. We will continue to further test and evaluate our systems involved in this most important function as our highest priority. Later I will discuss our efforts with other nations in this sensitive area.

DoD's Leadership Focus for 1999 – Ensuring Mission Capability

In early January of this year, we held a daylong meeting to review the results of our efforts to fix systems in 1998. There are still important efforts to be made in getting all systems Y2K compliant, particularly by the 31 March 1999 OMB deadline for mission critical systems. Our management efforts in 1999, however, are shifting to end-to-end evaluations of functional capabilities, contingency plan preparation and testing, and preparing for Y2K operations in the

period surrounding the millennium change. As shown in Figure 3 below, this year our focus will be in the following areas:

- Evaluation and testing of our mission and functional capabilities
- Preparation and testing of contingency and continuity of operations plans
- Preparing our leadership for Y2K situation decision making
- Supporting others in preparing for Y2K
- Consequence management planning and operational reporting

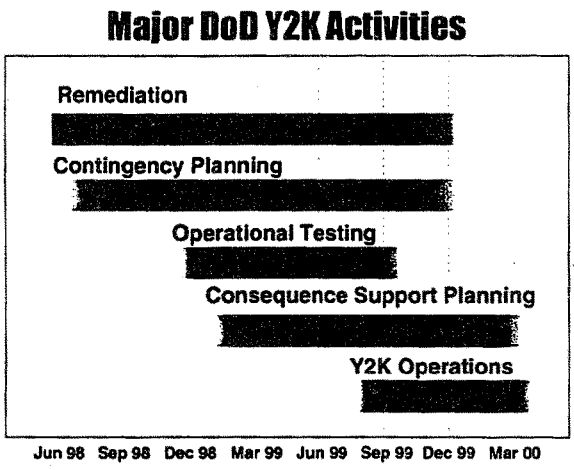


Figure 3 - Major DoD Y2K Activities in 1999

Evaluation and Testing of Capabilities

Our efforts this year are principally focused on improving our confidence in the Department's ability to continue to execute the National Military Strategy. DoD has already completed initial testing of most individual systems and their immediate interfaces. In 1999, the "Year of Testing," DoD will raise the standard. We will concentrate on complex, real-world end-to-end testing of DoD "business functions" and Warfighter missions – the things that we do in carrying out the national military strategy.

During 1999 we will test everything from paying service members to exercising vital command and control capabilities from "sensor to shooter." This will involve a "thin line

thread" or "skein" of systems that must operate in concert in order to perform a function. Testing in this manner is as complex as going to war and, therefore, involves all areas of the Department of Defense: the Services, the functional areas overseen by the Principal Staff Assistants of the Office of the Secretary of Defense, and the CINCs.

Our evaluation and testing efforts will generally follow a pattern of increasing scope and complexity. Therefore, the Services will be expected to test the Y2K performance of specific weapons systems before the PSAs perform end-to-end supplier capability tests. Finally, the CINCs, the Warfighters, have each selected among their own unique missions to devise real-world operational evaluations to exercise various warfighting missions.

The number and complexity of testing and evaluation efforts is managed in synchronization sessions co-chaired by members of OSD and the Joint Staff. The DoD Inspector General provides oversight and another review to search for holes in our evaluation program. Finally, the GAO and the OMB provide a review by external auditors. The number of activities, finite amount of key resources (particularly testing experts and time) and demands of real world day-to-day operations have forced an iterative and highly centralized deconfliction of our evaluation plan.

The key events in our evaluation plan are CINC Operational Evaluations, PSA functional end-to-end evaluations, and Service end-to-end and integration testing.

Operational Readiness Evaluations

We are using the Department's Warfighters, the CINCs, to evaluate operational readiness to conduct operations unaffected by the Y2K problem. The Fiscal Year 1999 Defense Authorization and Appropriations Acts require us to conduct at least 25 operational evaluations with each unified or specified commander conducting at least 2 exercises. We will exceed those requirements and, as shown in Figure 4 (below), have 31 CINC operational evaluations already scheduled.

Our approach has been to validate the complete warfighting process, from "sensor-to-shooter" using the significant dates specified by the GAO Testing Guide. Initial results from the three already conducted confirm that this kind of evaluation is essential to providing the additional assurance that our systems will remain operational over the millennium date change.

In addition to the CINC Operational Evaluations, CJCS is holding a series of Contingency Assessments of our ability to execute warfighting operations that will be discussed later under "Leadership Preparation for Decision-Making."

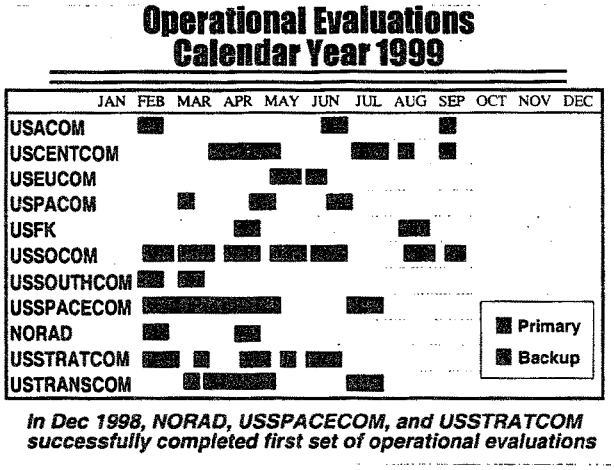


Figure 4 DoD Combatant Command Operational Evaluation Activities in 1999

Functional End-to-End Evaluations

We are using the Department's Business Process Managers – the Functional Proponents – to evaluate our ability to continue core support functions despite Y2K. Each of our functional process owners, logistics, finance, communications, intelligence, personnel, medical and others will conduct end-to-end evaluations of their core business functions as shown in Figure 5 below.

In some functional areas, particularly logistics, the Services are conducting end-to-end evaluations of their internal functional systems prior to a DoD-wide functional evaluation. These tests are in addition to the CINC operational evaluations and include, in many cases, organizations and systems outside of DoD.

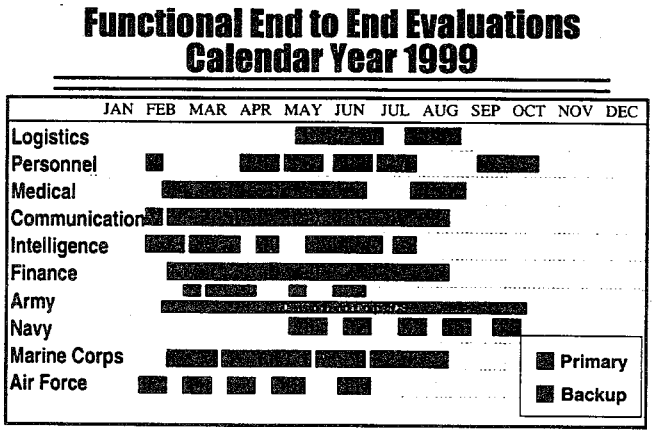


Figure 5 - DoD Functional End-to-End Evaluations in 1999

Integration Testing

Service integration testing will fix responsibility with the Department's System's owners – the Military Departments – to ensure continued functioning of other key processes that allow for Title 10 functions of organizing, training, and equipping our forces. This testing is over and above the five-phase OMB process each individual system must complete to be certified as Y2K compliant.

The Services' testing is critical to the ability of the CINC Service Components to carry out their parts of the CINC warfighting plans. Service testing provides a useful foundation prior to more complex, real-world CINC operational evaluations. The successful testing of several weapons' systems (Kiowa, Apache, Hellfire, and Multiple Launch Rocket System) at White Sands, New Mexico, for example, provided an excellent basis for future CINC operational evaluations. The testing conducted by the Military Departments is in addition to CINC operational evaluations and functional proponent end-to-end testing. These tests are the third method we are using to ensure departmental compliance with the evaluation requirements contained in the Defense Authorization and Appropriations Acts. Those Acts specify "all mission critical systems that are expected to be used if the Armed Forces are involved in a conflict in a major theater of war are tested in at least two exercises."

Finally, OSD and the Joint Staff are working together to develop a configuration management plan to ensure we maintain the hard won confidence in our systems that will result from this comprehensive series of evaluations. While still under development, the underlying tenet is a coordinated approach to configuration control involving the CINCs, PSAs, Services, and the OSD and Joint Staff.

In summary, we have the largest and most comprehensive evaluation plan in the Department's history, and we are continuing to work on refining our plans and improve the overall evaluation of core DoD functions. This plan will significantly improve our level of confidence in our ability to carry on operations despite Y2K. While these extensive efforts will mitigate our risk, the interconnectedness of everything guarantees that Y2K will have an impact on DoD. To deal with this reality, we must focus on realistic contingency planning and continuity of operations planning.

System/Operational Contingency Planning

Contingency planning is a normal aspect of DoD operations. What we are doing is applying our experience to the special case generated by the Y2K problem. The key elements of our contingency planning effort involve common guidance, focusing on core missions and functions, an adequate management oversight structure, and DoD engagement with other agencies and activities.

Common Guidance

Using the GAO guidelines, we have published DoD policy and guidance that requires every system, mission, and function owner to develop and test contingency and continuity of operations plans.

Our efforts at managing the individual component Contingency Planning activities are designed to ensure the Department as a whole can accomplish the eclectic and myriad missions assigned. To ensure that these plans are adequate, oversight responsibility for these plans is delegated to the Joint Staff for the CINCs and to the PSAs for all other plans.

Focus on Core Missions and Functions

A key part of our planning process is a focus on core missions and functions. We are using the CINCs to manage our core warfighting missions and the PSAs and Military Departments to manage the core support functions.

Warfighting capability is the domain of the CJCS and the CINCs. The CJCS and CINCs use the Universal Joint Task List (UJTL) to hierarchically group critical activities involved in execution of CINC Operational Plans. UJTL tasks are apportioned across the CINCs for evaluation during operational evaluations of "Thin-Line Threads" or core missions and functions. If systems on the "thin line thread" have not yet completed the Y2K compliance process, the system contingency plan is used.

Enterprise-wide support is the domain of the PSAs. Each core business function has internally derived "mission critical" capabilities that must execute to accomplish the DoD mission. Logistics, transportation, medical services, finance, procurement, supply, and a host of

other proponents are charged with assessing vulnerability and interdependencies and developing Contingency Plans to quickly restore services or otherwise accomplish the mission.

Core missions and capabilities not addressed by the CINCs or PSAs are bridged by Y2K Contingency Plans developed by the various combatant activities charged with those missions. For example, Title 10 Service missions address "training, organizing, and equipping" the constituent components. Each Military Department has a series of business activities with core missions and functions that serve this crucial need.

In summary, through a designed overlap of individual system contingency plans, CINC warfighting contingency plans, PSA functional contingency plans, and Military Department mission and functional contingency plans DoD achieves an overall collective organizational contingency plan.

Effective Management Oversight

To ensure that oversight is executed with a common standard, the OSD Y2K Program Office is conducting a workshop on oversight activities. The target audience is senior Service, Joint Staff, and PSA management and contingency planners and other oversight organizations such as the DoD IG. We will generate questions and emphasis areas for management oversight for use on subordinate Service, Command, and Agency activities.

The OSD Y2K Program office has conducted several workshops for Service, Command, and Agency contingency planners detailing proven methodologies for developing viable systems and operational contingency plans. Content of these workshops includes risk assessment techniques, interdependency management, value-chain analysis, and the top 100 questions a world-class contingency planner must ask/answer to assure organizational Y2K readiness. Workshop plans in progress include content development on "zero-day" response, preparations and risk mitigation strategies executed immediately before potential date outages to prepare organizations for the rollover.

DoD Involvement with Others

Finally, DoD is engaged with external organizations for systems and operational contingency planning. OSD is decisively engaged in developing an understanding of the demands that might be placed upon the Department of Defense as a result of Y2K induced disruptions in the US infrastructure. We are working closely with the White House, the National Security Council, Federal Emergency Management Agency, and a variety of other organizations to achieve a balance between DoD mission requirements and support to others. DoD must be able to assure operational readiness to react to challenges to US National Security while at the same time assisting the Nation in such a fashion as may be necessary to negate disruptions to the domestic infrastructure. This Intra-Governmental Contingency Planning is ongoing and likely to continue up to and through 1 January 2000.

Each system, function, and business process owner in DoD is responsible for developing, testing, and refining contingency and continuity of operations plans that ensure DoD can carry out its mission regardless of Y2K. Many of these plans will be exercised during the spectrum of DoD evaluation activities that will occupy us for most of the 2nd and 3rd calendar quarter. Certain

common elements in many activity contingency plans highlighted the need for special efforts to prepare decision-makers for potential Y2K situations.

Leadership Preparation for Decision-Making

There are two major activities in preparing DoD leadership for dealing with Y2K, Table Top Exercises and the CJCS-Sponsored Exercise POSITIVE RESPONSE Y2K (PRY2K).

Table Top Exercises

We announced the DoD plan for preparing the DoD leadership for the impact of Y2K on national security in an 8 December 1998 memorandum titled, "Participation in Department of Defense and National Level Year 2000 Table Top Exercises." The memorandum outlines the exercise activities that will be conducted at the defense and national level. These exercises will expose the participants to a reasonably worst case scenario induced by potential Y2K failures. These activities will enhance participants' understanding of potential Y2K impacts on national security; assist in the development of policy recommendations; provide continuing impetus to accelerate progress on fixing Y2K systems problems; and facilitate effective contingency planning. The four-part program includes:

- A set of three functionally oriented one-day policy seminars held in November and December that identified some 70-80 policy-level issues that formed the foundation for further Table Top Exercise activities.
- A daylong Table Top Exercise policy workshop held on 30 January. Participants represented the key decision-makers of DoD (to include myself), the State Department, Federal Emergency Management Agency (FEMA), the President's Y2K Coordinator, and congressional staffers.
- A DoD Defense/National Security game planned for April and to be completed prior to the national level exercise. The DoD game will focus on policy and crisis management in response to a national security emergency. The DoD senior leadership will fully participate, including myself, the Vice-Chairman, Joint Chiefs of Staff, the Service Under Secretaries, the DoD CIO, and selected Principal Staff Assistants and Directors of specified Defense Agencies. State Department and FEMA participation is planned also.
- This activity will lead up to a National-level Y2K Table Top Exercise in June. This will be a White House Y2K office inter-agency exercise, supported jointly by DoD and FEMA.

POSITIVE RESPONSE Year 2000

In addition to Table Top Exercises, CJCS is conducting exercise POSITIVE RESPONSE Year 2000 (PRY2K). PRY2K is a series of four command post exercises scheduled from February to September 1999 and is the first national level exercise conducted under conditions of multiple Y2K mission critical system failures. PRY2K assesses the ability of DoD to respond with timely decisions in a Y2K environment and focuses on the strategic national tasks of

mobilization, deployment, employment, intelligence-surveillance-reconnaissance (ISR), and sustainment.

This series of exercises is designed to achieve senior participation in and awareness of the operational impact of Y2K mission critical systems failure during the mobilization, deployment, employment, and sustainment processes. The concept is to remove mission critical systems and capabilities from play during the conduct of a robust warfighting scenario and then assess DoD ability to respond with timely decisions. In addition, the exercises assess the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K. Finally, senior members of the warfighting community will share lessons learned and other vital information via secure videoteleconference (SVTC). The Secretary of Defense, CJCS, Service Chiefs, and CINCs will participate in the SVTC following the exercise with a goal of recommending a strategy to the National Command Authority to mitigate the impact of mission critical systems failure.

To date, these leadership preparation events have already surfaced several interesting issues and we are working on solutions. In many cases, the situations result from likely requests for DoD assistance from other agencies and activities. Consequently, as this year progresses, we will become increasingly involved in DoD support to others.

Supporting Others

The principal focus of our efforts this year to ensure cross-organizational awareness and coordination necessary for continued operations across the millennium change within the Department of Defense, Federal Government, allies and coalition partners. In compliance with The President's Council on Y2K and other guidance, DoD has been fully engaged in assisting other activities in preparing for Y2K, including other federal sectors, the National Guard's work with the States, and our international partners and allies.

Federal Sector Outreach

The Department of Defense engages in critical functions or shares unique interests with other Federal participants. We have engaged thirteen Federal Sector Outreach Working Groups that cover the full spectrum of business activities, from Health Care to Emergency Management/Disaster Response to Benefits Payments; and International Trade.

A good example of our outreach engagement has been in the Health Care sector where DoD is the lead agent for the Federal Government in the area of biomedical equipment.

DoD biomedical equipment is currently 96 percent Y2K compliant. The remaining 4 percent will be compliant by Mar 31, 1999. "Biomedical" means instruments and equipment typically found in a clinic, hospital, doctor's or dentist's office. As an example, some electrocardiogram (EKG) machines have a date function that could be affected by Y2K. The EKG equipment, however, records analog signals that are not date-dependent. Thus, the equipment deals with dates only to tag the data.

DoD Health Affairs has taken the lead on verifying biomedical equipment compliance along with a multi-agency federal working group consisting of the Army, Navy, Air Force,

Veterans Affairs, Indian Health Service, the National Institutes of Health, and Public Health Service. The group has collaborated with equipment manufacturers to develop a database of compliance information for biomedical equipment used in the military health system.

In essence, DoD assessment and remediation efforts for biomedical devices allow other users access to up-to-date Y2K compliance information. This spares the other users the time and expense of duplicating Y2K compliance assessment.

Another area of focus has been to ensure critical functions and services on our installations will continue uninterrupted during and beyond the Year 2000. We engage Y2K topics at the state and local level for the following five Federal Sectors: Police/Public Safety/Law Enforcement/Criminal Justice Sector; Energy (Electric Power); Water Supply and Wastewater; Waste Management; and the Fire and Emergency Services Sector. Our goal is to identify all dependencies outside DoD within the Federal, State and Local Governments that affect the Department's ability to perform mission critical activities.

These efforts in ensuring our installations are supported during the millennium change are also related to the National Guard Bureau's efforts in preparing for Y2K.

National Guard Planning for Y2K

As part of its contingency planning, the National Guard Bureau will conduct a communications exercise this summer to test its, the high frequency radio network from the headquarters to the 54 States, Territories, and the District of Columbia. Success is measured by the National Guard Bureau's ability to communicate with all states simultaneously.

States have been asked by the National Guard Bureau to ensure they are capable of performing their federal missions as elements of the Army and Air Force. The States are also asked to ensure that they can answer the call of the respective Governors, should a call be required. Y2K compliance is as essential to a blizzard response, earthquake, flood or other disaster as it is to meeting the Governor's potential call for Y2K related incidents, should they occur.

There are no federal plans to mobilize/recall the National Guard. Each State Governor makes a determination on calling the National Guard based on the needs of the respective State. Several States have indicated they will alert elements of the National Guard in case they are needed. Some states (Washington and Oregon, for example) already have concluded detailed agreements regarding National Guard response during a Y2K induced emergency. An alert or call to State Active Duty is a State prerogative.

These and other issues have been raised during our internal DoD Table Top Exercises thus far and may continue to surface in subsequent exercises. In addition to our focus on operational within the United States, we have been working hard to engage with our international partners and allies on the Y2K issue.

International Outreach to Allies

Much of DoD's effort to ensure mission capability is directed toward organizations outside DoD. We are encouraging allies and partners to address the Y2K problem vigorously in an effort to mitigate the potentially destabilizing effects of international Y2K disruptions. Where there are mission critical dependencies we are working to ensure continuity of operations through systems remediation and development of contingency plans.

DoD's extensive participation in international outreach efforts is another example of foresight in consequence management and contingency planning efforts. These initiatives can be categorized in five areas: Remediation, Testing, Table Top Exercises, Consequence Management, and International Outreach. The first four have already been mentioned and I'd like to briefly summarize our efforts in the international arena.

Most of DoD's international outreach efforts have focused on Allies, Partners, and threat reduction efforts. Additionally, the DoD IG recently recommended increased involvement of the Defense Security Cooperative Agency in Y2K Outreach to nations that purchase military equipment via Foreign Military Sales. Other direct involvement is as follows:

Allies and Partners

- Participated in a NATO conference hosted by Ministry of Defence (MOD) United Kingdom in mid-November 1998 to continue planning for Y2K-related exercises and contingency plans.
- Conducted follow-up visits to SHAPE headquarters in Belgium in November 1998.
- Participated in UN Y2K conference on 11 December 1998, to initiate contact with nations strategic to U.S. National Security interests. Contacted delegations from 42 nations impacting DoD missions.
- Participated in conference of economically and strategically vital Pacific Rim hosted by Australian government, 15-23 February 1999.
- Participated in a follow-up conference with Canadian officials on Y2K lessons learned, Coming Challenges, and Mission Critical Systems Status in February 1999.
- Broadened Canadian-US Y2K working groups to include Mexico.

Threat Reduction

- Joint Staff visit on threat reduction issues to Russia and Belgium in January 1999.
- Follow up DoD visit to Russia and Belgium on Y2K Threat Reduction plans in February 1999.

Our dialog and plans with Russia on the critical area of nuclear weapons command, control, and communications and shared early warning are continuing. DoD has had limited dialog with other nations, and question about the specific status of other nations should be referred to the intelligence community.

Our work with other Federal Agencies and international partners highlight the potentially significant demands that might be place upon DoD as the millennium change draws nearer. Consequently, we began centralized planning and management of certain key aspects of our responses to large-scale events affecting the nation

Consequence Management Planning

The Department of Defense, working with other Federal Agencies on contingency and continuity of operations planning, has recognized the potential for multiple competing demands for scarce resources. We began "consequence management" planning several months ago to deal with the elements common to most mission and function contingency plans. Major components are: planning, request management, and operations and reporting during the millennium change period.

At my direction, the Department has just completed a review of its posture for Y2K Consequence Management. We formed an Integrated Process Team (IPT) consisting of representatives from all elements of DoD, including the Joint Staff, PSAs, the Military Department, and the Director of Military Support (DOMS). The IPT reviewed current guidance, processes, and procedures for Military Support to Civil Authorities (MSCA), organizational structures to support MSCA, processes and procedures for disaster response overseas, and several other issues that could impact the ability of the DoD to execute both its military responsibilities and provide MSCA. Recommendations fell in three major areas:

Planning

- Public affairs planning and guidance. Deals with the problem of expectation management. For example, what are reasonable expectations about what will occur and what should our leaders be issuing to their subordinates about prudent preparations.
- International issues, such as Host Nation Support. These efforts are an in confluence with our International Outreach efforts and also relate to our installations overseas and their support from local communities.

Request Management

- Resource visibility and allocation. We are in the process of refining the list of assets that have utility in MSCA within DoD. Because Y2K is a special case of MSCA in that many concurrent emergencies may occur, special procedures may be required to ensure the most effective use of these resources.
- Personnel policies. Personnel turbulence and rotation are common issues, particularly with DoD's military population. We are trying to hammer out workable policies that ensure continuity of key personnel over the millennium event.

Operations and Reporting

- Developing the common lexicon and operational picture. This is an issue within the Federal Government that has major implications for DoD's normal reporting

procedures and formats. We are fully engaged in helping ensure a common lexicon is used for Y2K that can be applied to other potential national issues.

- Training. We need to ensure that everyone involved in MSCA knows the specific means and methods for dealing with Y2K. In addition, we will need to rehearse and exercise our procedures for request management and reporting.

As we continue to refine our plans for preparing for and managing the millennium event, the Department's reliance on activities and agencies outside DoD becomes key. In addition, we can reasonably expect that DoD will be called upon to assist other agencies and activities during this process. Towards that end, we have begun preparing the DoD leadership for the types of decisions likely to be required during this period.

The Department's reliance on other nations to conduct its missions and functions has been an eye-opening outgrowth of the Y2K problem. In this regard, our work on the Y2K problem has had several salutary effects and suggests several implications for future DoD information technology operations.

Lessons Learned and Implications for the Future

We have learned many lessons about managing information technology systems in the course of dealing with the Y2K problem. Out of that hard work have come several "good news" stories as well as some obvious next steps.

Good News

There have been many positive outcomes of the enormous amount of energy and effort devoted to fixing the Y2K problem. As a result of our preparations for Y2K, the Department now has:

- An excellent inventory of all information technology (IT) systems: hardware, software, and embedded systems. In addition, we have the management structure in place to deal with management of the approximately 9,900 systems in DoD.
- Improved procedures for managing IT assets. Of note has been a significant increase in the awareness of issues associated with configuration management as a CEO issue related to mission performance.
- More uniform, up-to-date versions of software throughout the organization. In particular, many long overdue upgrades were completed to achieve Y2K compliance for our enterprise-wide support functions.
- A detailed map and agreements with interfaced organizations. The interface listing provides a clear picture of where DoD relies upon others or is relied upon for data. Coupled with the increased appreciation for configuration management issues, we are better able to determine the true costs of issue associated with enterprise-wide upgrades.
- A contact network in place to deal with future enterprise-wide IT issues. Perhaps the greatest benefit of this operation has been to educate DoD senior management of the

consequences of failing to "pay the bill" to ensure our IT infrastructure keeps pace with industry standards.

- Developed the groundwork for network-centric warfare. In many ways, the Y2K problem acts as a worldwide virus requiring everyone to respond. As a result of our efforts on Y2K, DoD is much better prepared to deal with overt and covert attempts to undermine our IT capabilities.

Next Steps

The enormity and pervasiveness of the Y2K challenge has caused us to focus almost exclusively on the period surrounding the millennium change. As we continue these preparations, the Department will be working to develop plan to implement the results of some of our lessons learned from this process. In particular, many challenges will remain to completing resolution of issues generated by Y2K, including:

- Our reliance on legacy automation systems. In many cases, DoD has applied several years' worth of software upgrades in a very short period of time to achieve Y2K compliance. The long-term costs of failing to budget for and execute an enterprise-wide common configuration baseline have been crystal clear. It truly is a "pay me now or pay me later" situation.
- Replacing "windowing" solutions with reliable software code. Applying a software patch that told the computer to treat certain 2 digit dates as if they were indeed 4 digits completed many of our remediation efforts. By doing so, we've bought ourselves a grace period, but not a final solution. During this grace period we must either fully resolve the date management code in the software or replace the system.
- Completing fielding of systems delayed by Y2K efforts. Again, one outgrowth of our Y2K compliance efforts was to slow down development of some systems that did not seem likely to be Y2K compliant in time. We must deal with these system delays and ensure that the subsequent development and fielding efforts do not undermine our Y2K compliance status.
- Rescheduling work held in abeyance for the more urgent goal of Y2K compliance. In summary, there is a substantial opportunity cost for delaying the development of other systems in order to pay for, schedule, attain compliance, and observe the configuration control to ensure continued Y2K compliance. This cost has put DoD very far behind in a field that introduces an new generation of technology every 18 months. We must work hard to catch up and pay for it.
- Sustaining and improving our mapping of interfaces and reliance on systems and organizations outside DoD. The August 1998 SecDef memorandum requiring signed interface agreements for all systems was a critical step in jump starting our efforts. We must continue the momentum developed during Y2K to further refine and map our system and capability dependencies within and exterior to DoD.
- Continuing our efforts to replace stovepipe systems with enterprise-wide solutions. As part of our management approach, we fixed responsibility for enterprise-wide business processes with the PSAs. As this process developed and each PSA worked

to develop evaluation plans and report progress, it became clear that there were large differences in the maturity of our consolidation efforts. In some areas, such as logistics, the conversion from mainly stovepipe systems to common enterprise-wide software was reasonably far along. In others, a bewildering Tower of Babel is still, lamentably, the order of the day.

- Continuing to replace expensive, proprietary systems with commercial off the shelf (COTS) and government off-the-shelf (GOTS) products and modules. This effort will promote more uniform and more current software, hardware, and system maps.
- Continuing to centralize management of the Department's "business processes" such as logistics, finance, and communications. In particular, our experience with personnel systems during Y2K argues strongly for movement to an enterprise-wide common group of systems. These efforts, while enormously difficult, hold the potential for huge long-term payoffs for the Department.

Conclusion

DoD has recognized and attacked the Year 2000 problem as a threat to the core of our military superiority. The superior ability of the United States Warfighters to obtain, process, analyze, and convey information is our most powerful weapon on the battlefield. It is a cornerstone of our military strategy captured in Joint Vision 2010.

The leaders in the Department respect the complexity and pervasiveness of the issue, and recognize that the Y2K challenge requires:

- Our best leadership to motivate, educate, facilitate, and interface with the myriad other Federal, State, civilian industry, Allied and international organizations upon which we depend.
- Support, recognition, and incentives both for successful program managers and for the information technology workers who are doing the hard work. The software engineers, in and out of uniform, who must slog through millions of lines of code to repair our systems, are an important defense resource and there is no time to replace or train more.
- Meticulous prioritization and focus on the most important systems. We must constantly fight to stay focused on our critical systems and not let our efforts become diluted by attempting to fix everything at once.
- Ruthless stewardship of our most constrained resource –time. Time is critical. We can't slow it down. We cannot change the deadline. The Department of Defense is like a large ship headed toward an iceberg. We have successfully changed course to avoid the tip but we must continue our efforts to ensure me miss the submerged portion.

We have fixed most of our mission critical systems and are working hard on the remainder. We are developing and exercising continuity of operations plans for all key functions and processes. We are preparing our leadership and our organizations for Y2K operations. We are working with those who rely on DoD and upon whom we rely. We have focused special

attention on nuclear systems and have already tested them several times. We are looking ahead to leverage our Y2K experience for future DoD information technology operations.

DoD has gained a great amount of experience facing the Year 2000 challenge, and we stand ready to support other Federal Agencies with which we interface. Rest assured, although there will be increasing unpredictability and some degradation in some systems, the armed forces will be ready to ensure national security before, on, and after the Year 2000.

UNCLASSIFIED

US AIR FORCE YEAR 2000 (Y2K) PROGRAM

- The Air Force will be fully mission-ready on 1 Jan 2000

- Four principal focus areas for Air Force program: Systems, Installations, Mission Testing, and Consequence Management—working them simultaneously

- Systems focus completing DoD's 5-phase resolution process—emphasis on moving to left
  - Tracking over 3,300 weapon and information systems; more than 400 systems are mission critical
  - As of 31 Dec 98, AF reported 82% of mission critical systems complete
    - Projecting 90% of mission critical will meet 31 Mar 99 OMB deadline
    - No surprises, all estimated completion dates in time to test prior to 31 Dec 99
  - AF leadership fully engaged—system Y2K status has appropriate visibility

- Installation focus promoting commander involvement at every level
  - By 31 Mar 99 installation and Major Command (MAJCOM) commanders will certify that essential systems are Y2K compliant or have viable contingency plans
  - By 30 Jun 99 installations will test contingency plans and continuity of operations plans (COOPs)
  - By 30 Jun 99 wing commanders will provide "end of runway check"—assessment of ability to execute critical missions, based on status of equipment, facilities, and contingency plans and COOPs
  - Encouraging installation commanders to bring local municipalities into their planning efforts and to aggressively publicize Y2K preparations
  - Air Force "strike teams"—teams of Y2K "consultants"--visit bases to assist installation commanders in such areas as contingency planning and COOP development
  - Air Force Audit Agency conducting Y2K-focused Management Advisory Services (MAS) at numerous installations to ensure efforts on-track, to recommend areas for improvement, and provide leadership at every level an assessment of Y2K progress at installation level
    - More than 50 bases visited so far, 20K+ contact hours; will visit 71 bases in Mar-Apr, including all overseas bases; MAS results used to target HQ Air Force Y2K efforts

- Mission testing of mission critical systems will ensure Y2K compliant systems remain interoperable
  - Air Force Tasks outlined in Air Force Doctrine Directive 1-1 have been assigned to each Major Command--have developed mission threads and lists of systems essential to execute those threads
  - Systems will be tested in CINC Op Evals, functional end-to-end tests, and Air Force Op Demos
  - Have already conducted several CINC Op Evals and system Ops Demos—to date we have encountered no significant Y2K anomalies
  - Although confident base telecommunications and LAN systems are compliant, we'll test an entire installation in May-Jun

- The first three areas are preparation for Y2K, Consequence Management is how we'll handle events
  - Will use existing command and control structure to monitor and report
  - Envision anomaly and "ops normal" reporting; and we'll feed back what what's being reported to keep field units informed
  - Will have experts—"Red Adairs"—in key areas of expertise (civil engineering, software experts, etc) standing by to initiate workarounds and work long-term fixes, should anomalies occur

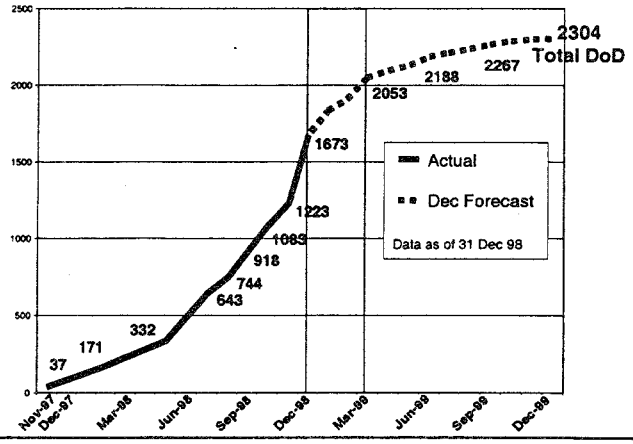
Lt Col B. Pasierb, AFY2KO, 602-2217, 23 Feb 99

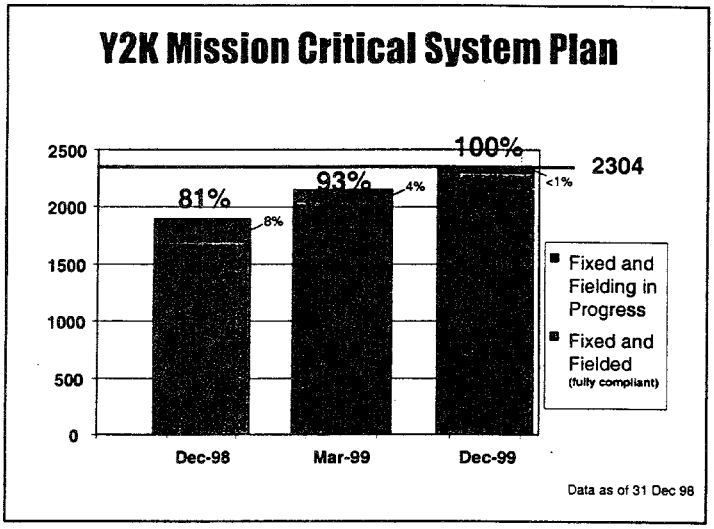
DepSecDef Testimony

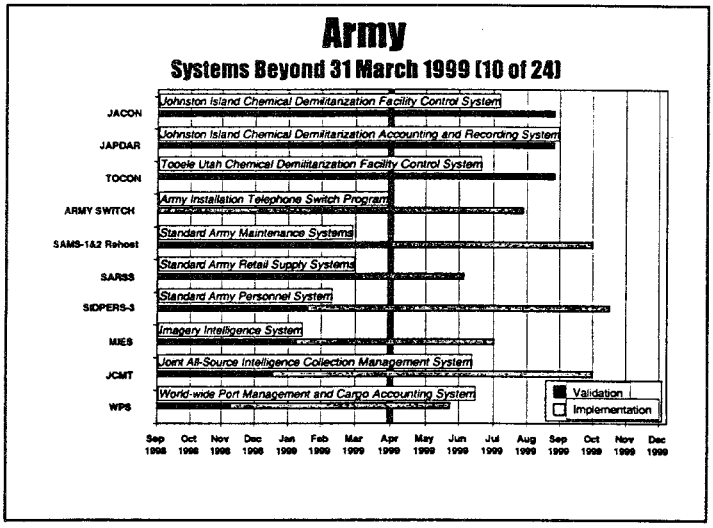
House Committee on Government Reform

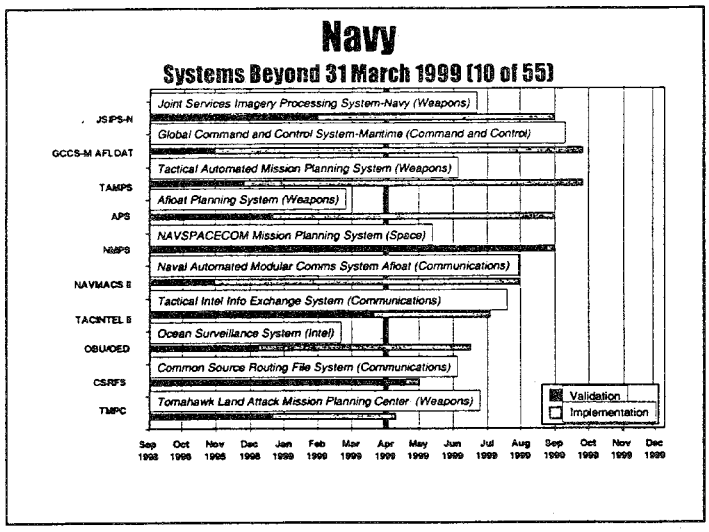
2 March 1999

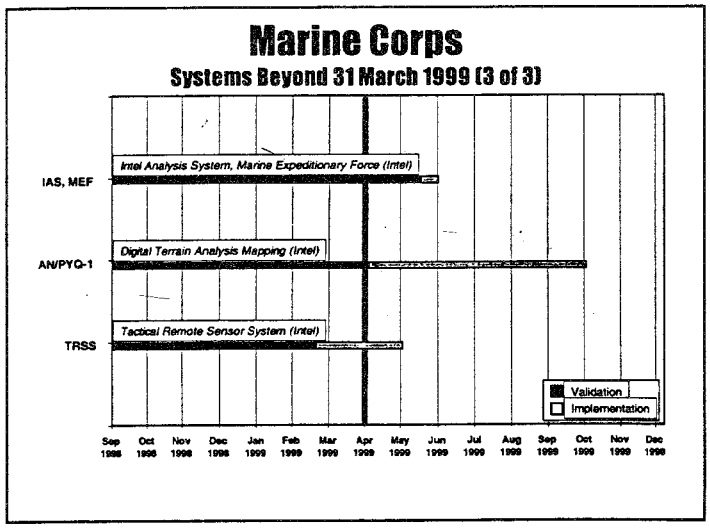
Y2K Mission Critical System Plan

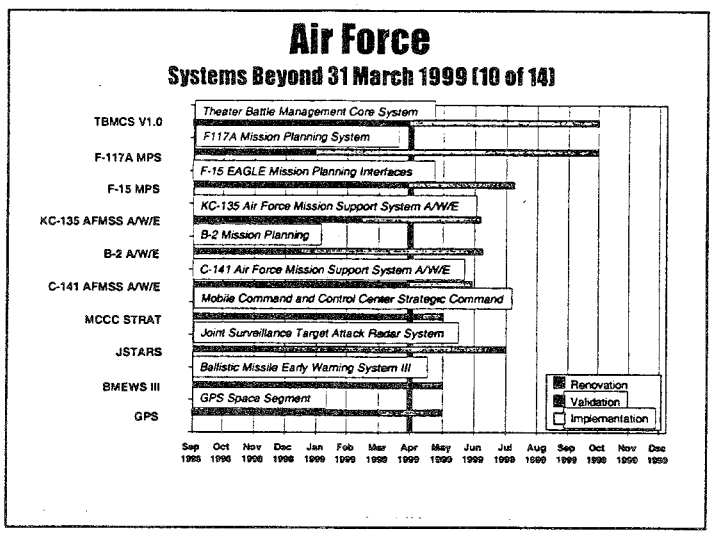


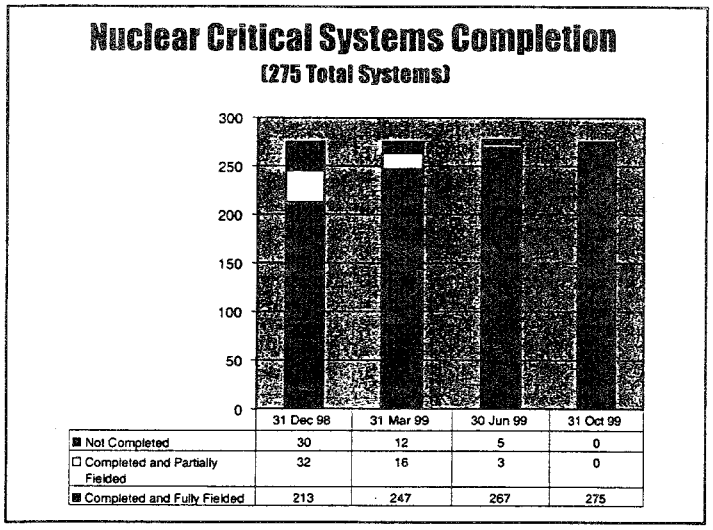

Y2K Mission Critical System Plan
2500
2000
1500
1000
500
0
81%
8%
93%
4%
100%
<1%
2304
Dec-98
Mar-99
Dec-99
Fixed and Fielding in Progress
Fixed and Fielded
(fully compliant)
Data as of 31 Dec 98


Army
Systems Beyond 31 March 1999 (10 of 24)
JACON
JAPDAR
TOCON
ARMY SWITCH
SAMS-1&2 Rehost
SARSS
SIDPERS-3
MIES
JCMT
WPS
Johnston Island Chemical Demilitarization Facility Control System
Johnston Island Chemical Demilitarization Accounting and Recording System
Tooele Utah Chemical Demilitarization Facility Control System
Army Installation Telephone Switch Program
Standard Army Maintenance Systems
Standard Army Retail Supply Systems
Standard Army Personnel System
Imagery Intelligence System
Joint All-Source Intelligence Collection Management System
World-wide Port Management and Cargo Accounting System
Validation
Implementation
Sep 1998
Oct 1998
Nov 1998
Dec 1998
Jan 1999
Feb 1999
Mar 1999
Apr 1999
May 1999
Jun 1999
Jul 1999
Aug 1999
Sep 1999
Oct 1999
Nov 1999
Dec 1999


Navy
Systems Beyond 31 March 1999 (10 of 55)
JSIPS-N
Joint Services Imagery Processing System-Navy (Weapons)
GCCS-M AFLDAT
Global Command and Control System-Maritime (Command and Control)
TAMPS
Tactical Automated Mission Planning System (Weapons)
APS
Afloat Planning System (Weapons)
NSPS
NAVSPACECOM Mission Planning System (Space)
NAVMACS II
Naval Automated Modular Comms System Afloat (Communications)
TACINTEL II
Tactical Intel Info Exchange System (Communications)
OBU/OED
Ocean Surveillance System (Intel)
CSRFS
Common Source Routing File System (Communications)
TMPC
Tomahawk Land Attack Mission Planning Center (Weapons)
Validation
Implementation
Sep 1998
Oct 1998
Nov 1998
Dec 1998
Jan 1999
Feb 1999
Mar 1999
Apr 1999
May 1999
Jun 1999
Jul 1999
Aug 1999
Sep 1999
Oct 1999
Nov 1999
Dec 1999


Marine Corps
Systems Beyond 31 March 1999 (3 of 3)
IAS, MEF
Intel Analysis System, Marine Expeditionary Force (Intel)
AN/PYQ-1
Digital Terrain Analysis Mapping (Intel)
TRSS
Tactical Remote Sensor System (Intel)
Validation
Implementation
Sep 1998
Oct 1998
Nov 1998
Dec 1998
Jan 1999
Feb 1999
Mar 1999
Apr 1999
May 1999
Jun 1999
Jul 1999
Aug 1999
Sep 1999
Oct 1999
Nov 1999
Dec 1999





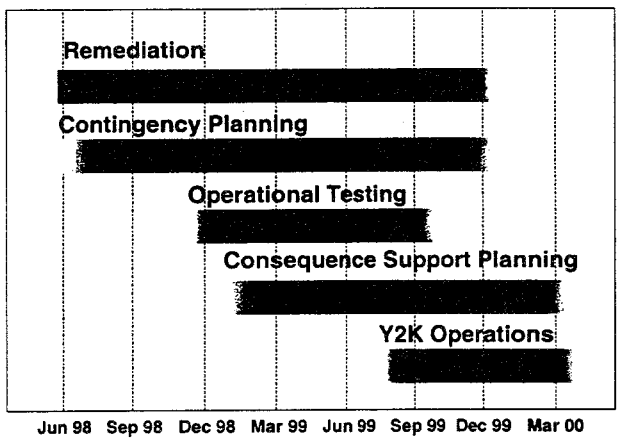
	31 Dec 98	31 Mar 99	30 Jun 99	31 Oct 99
■ Not Completed	30	12	5	0
□ Completed and Partially Fielded	32	16	3	0
■ Completed and Fully Fielded	213	247	267	275

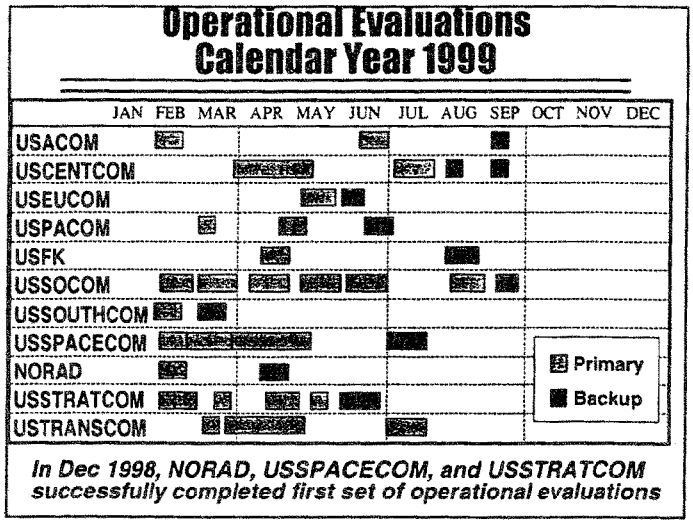
Center for Year 2000 Strategic Stability Plan

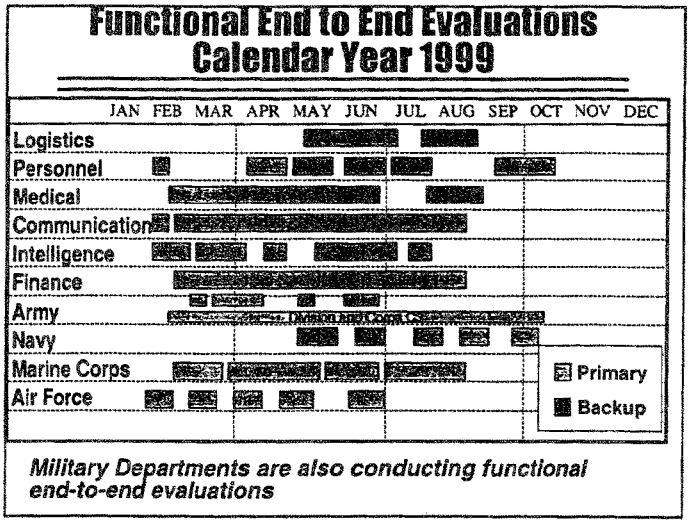
Designed to:

- reduce the risk of accidental or inadvertent release of nuclear weapons during the Year 2000 roll over period
- allow U.S. and Russian personnel to observe, side-by-side, all relevant missile launch events during the critical transition period
- share other information that might be interpreted as threatening national security
- be located in Colorado Springs
- be in operation only a short period of time

Major DoD Y2K Activities




Operational Evaluations
Calendar Year 1999
JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
USACOM
USCENTCOM
USEUCOM
USPACOM
USFK
USSOCOM
USSOUTHCOM
USSPACECOM
NORAD
USSTRATCOM
USTRANSCOM
Primary
Backup
In Dec 1998, NORAD, USSPACECOM, and USSTRATCOM successfully completed first set of operational evaluations


Functional End to End Evaluations
Calendar Year 1999
JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
Logistics
Personnel
Medical
Communication
Intelligence
Finance
Army
Navy
Marine Corps
Air Force
Primary
Backup
Military Departments are also conducting functional end-to-end evaluations

DoD Operational Readiness and Consequence Management Priorities

- **Priority 1:** Units engaged in:
  - Direct Support to National Command Authority
  - Conduct of ongoing or imminent military operations
  - Conduct of ongoing or imminent intelligence operations
  - Conduct of nuclear command and control
  - Maintenance of Defense and commercial essential infrastructures to support the above
- **Priority 2:** Units assigned to support standing operations plans and scheduled for early (within 60 days) deployment
- **Priority 3:** Provision of DoD Support to Civil Authorities for the Maintenance of public health and safety
- **Priority 4:** Provision of DoD Support to Civil Authorities for the Maintenance of the Economy and the Nation's Quality of Life

Summary

- DoD completely ready on January 1, 2000
  - Demonstrated capability, not just words
- The warfighters are responsible for testing
  - Largest and most comprehensive test in DoD history
- Contingency plans
  - Most systems plans are in place
  - Developing operational contingency plans
- Nuclear systems receiving special attention
  - All under positive control
  - Sharing information internationally
- DoD supporting Federal efforts through the President's Council on Y2K Conversion

Mr. HORN. Please, come to the table and take whichever one of these sad microphones you can put your fingers on.

Colonel SMITH. Will that be sufficient?

Mr. HORN. That is fine. Just speak into the mic.

Colonel SMITH. Mr. Chairman, Madam, for the next 5 minutes I would like to give you some understanding of what your North American Aerospace Defense Command has been doing for the last 4 or 5 months in the skirmish in the operational evaluation of the Y2K problem.

I am going to show you a number of fairly technical charts. Your staff will have those charts. I trust you understand my intention is not to confound the committee and not to impress, but rather to express the level of detail with which we have examined the problem, and the amount of rigor that has been applied to testing them in the operational environment.

Next chart, please.

[Chart shown.]

Colonel SMITH. As you heard described, there are four parts to the DOD Y2K plan. Each of the 11 combined and unified Commanders-in-Chief have been tapped with the responsibility of taking the work that has been done by the system program offices doing individual technical testing and the services and agencies and functional deputies doing various portions of their string and functional area tests and apply that system's approach to the actual mission environment.

In other words, take a sensor to shooter string of operational systems; apply an exercise scenario over the top of that; operate the systems in the Y2K environment and ensure that we can conduct the mission.

Next chart, please.

[Chart shown.]

Colonel SMITH. These are the two critical missions that North American Aerospace Defense Command has and General Myers is responsible to you and to the American people for aerospace warning and aerospace control. Integrated tactical warning and attack assessment is the warning of ballistic missile attacks, nuclear attacks, atmospheric and space attacks. The control part is the air sovereignty and air defense part. The portion of this chart shown in red is the portion that we addressed in our December operational evaluation. The remainder was addressed in the last 2 weeks during our February operational evaluation, otherwise known as Amalgam Virgo 99–2.

Next chart, please.

[Chart shown.]

Colonel SMITH. This is obviously a chart to choke a horse. Again, the purpose of this chart is not to address in detail each of the systems involved, but to express the level of detail we went to to ensure that we understood the complete missile warning mission architecture: every box, every connecting communication system that is involved in that architecture.

From that architecture we carved out the minimum number of systems, from sensor to shooter, if you will, required to execute each of the two missions I showed you on the previous chart.

Next, please.

[Chart shown.]

Colonel SMITH. What that looks like in an operational sense is that the global missile warning system, for example, to include the radar sensor systems shown in yellow; the infrared satellite detection systems and their sensor processor systems, shown in blue; the correlation centers where all of the radar and infrared information is brought together and correlated shown in pink, principally Cheyenne Mountain; and in green, the forward users or shooters, in this case the principals being the National Military Command Center, the National Defense Headquarters in Ottawa and CINCSTRAT's headquarters in Omaha.

Next chart, please.

[Chart shown.]

Colonel SMITH. This is what I call a blue box chart, if you will. It is the thin line that we carve out of that, that is, the minimum number of systems. This is what we looked at in December. We looked at a representative sample of each of those three kinds of radars that I showed you and the infrared processing system. We processed it through the two correlation centers. In this case, principally the alternate missile warning center at Offutt and forward to STRATCOM headquarters to the National Military Command Center. In participation with the Nuclear Command Control and Communications process, we also forwarded that information to site R to make sure one, that we had a good proof of process for operational evaluations; and two, that we could take a look at some of our systems. Each of the blue blocks that you see here represents a system that has a clock in it, whether it be a distribution or a process system, or a SECURECOM interface or some kind of a display.

Next chart, please.

[Chart shown.]

Colonel SMITH. What we found from that December operational evaluation were no failures. Not only did we have good performance in the real-world environment, which suggested to us that, whatever happens, our real-world system is going to operate properly for us. Our final report was posted on January 5th, 1999, and that can be made available.

Next chart.

[Chart shown.]

Colonel SMITH. Having established a good proof of process for operational evaluations and an understanding of our systems, we went forward this last 2 weeks in our second operational evaluation looking at all of that space and missile warning architecture, as well as the air warning and control architecture. We ran runs prior to clock rollovers, across the clock rollover, and after the clock rollover for each of the four critical dates, the so-called 9/9/99 date, dated September 9th, the December 31st rollover, and the two leap years, February 28th and 29th.

We looked at a representative sample again at the IR missile sites and space sites. In the air side, we looked at like and simulated tracks to make sure that we had good redundant data, and we looked again at the same environment there looking at critical sites.

Next chart, please.

[Chart shown.]

Colonel SMITH. This is a missile warning thin line. In addition to what we did in December, we picked up that last ballistic missile early warning radar system that we had not looked at. In addition, we looked at several elements of the survivable endurable nuclear command and control system to include the mobile ground stations and the mobile consolidated command centers. We also brought forward the national defense headquarters in the Canadian NORAD Region, along with the Fylingdales radar station in the United Kingdom.

Next chart, please.

[Chart shown.]

Colonel SMITH. The space warnings thin line is very much similar to that with the exception of the radar that we added at Eglin Air Force Base.

Next chart, please.

[Chart shown.]

Colonel SMITH. Looking at that air warning system, the second week, we took of the over 100 radars that ring the North American continent for aerospace early warning, we took five representative samples of the five key types of radars that constitute that entire system.

Next chart, please.

[Chart shown.]

Colonel SMITH. What those look like when you apply them to that thin line environment, is the radar processors that we looked at through the radar display systems and processing systems at each of the regions, CONUS, Canada, and Alaska, through Cheyenne Mountain again, a slightly different display system, but essentially the same processing through to those same forward users or shooters at the National Command Center, STRATCOM, and the NDHQ in Canada.

Next chart, please.

[Chart shown.]

Colonel SMITH. The summary, then, is that the first exercise of Vigilant Virgo 99–1 went without a hitch. We had high confidence based on nominal performance after that evaluation. We just completed our second evaluation of the entire mission string that we require. Our quick look is that there were no hard failures for our NORAD system. And, I will tell you that we were running some non-mission-critical systems in the background to take advantage of the architecture that we put together, and in one of those systems, we had a situation similar to what Admiral Willard described with a message handling piece, but the system program office that is responsible for that tells us that it will be 60 days or less before we have that one fixed. And in any case, it is not a mission-critical system. So, we were successful in finding some problems and in time to have them fixed.

The last message that I would give you here is a continuity of operations bullet. My point there is that, having completed our operational evaluations, we at NORAD do not consider ourselves finished. We are responsible now to put together a real-world operations plan so that we can deal with the actual dates as they occur, so that we work with our local community to make sure that we

have prioritization and sharing of resources to deal with unexpected consequences, that we have the right people in the right place to deal with the systems, and that we are prepared to distribute messages throughout the system to validate the performance immediately after each rollover. So that we don't have to wait until a real-world event occurs to find out whether it is actually working or not.

So, we are going to apply very rigorous process to that operational planning, so that we are prepared to deal not only with what we have discovered in our test, but what happens in the real world. The bottom line is the Commander-in-Chief, NORAD General Myers, is going to be able to provide that warning and control, just as Dr. Hamre has described, on January 1st and every day thereafter.

Subject to your questions, that concludes my statement.

[The prepared statement of Mr. Smith follows:]

NORAD Y2K OPEVAL

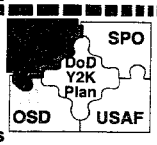
VIGILANT VIRGO 99-1
AMALGAM VIRGO 99-2

Col R. F. Smith
Vice Director,
NORAD Combat Operations

NORAD OPEVAL

Department of Defense Perspective

VV 99-1 AV 99-2



- ***SECDEF #1 Priority***
- Four-part approach
  - System Program Offices - Individual Systems
    - Five-stage process to reach technical solutions
    - Awareness, Assessment, Renovation, Validation, Implementation
    - Critical Systems complete by: 31 Dec 98
    - Remainder to be complete: 31 Mar 99
  - Services and Agencies - End-to-end testing
    - Sensor to shooter - test everything twice
  - Functional Deputies - Functional systems tests
    - Logistics, Communications, Intel, Personnel, Medical, Finance
  - CINCs - Operational Evaluations (OPEVAL)
    - Critical Missions & Systems - thin lines/ops environment

NORAD OPEVAL

Missions

VV 99-1 AV 99-2

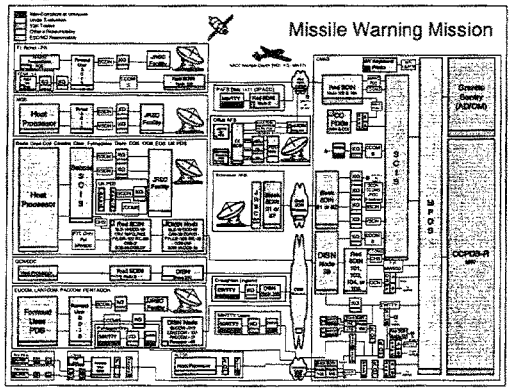
- Aerospace Warning
  - Provide Integrated Tactical Warning and Attack Assessment
    - Ballistic Missile Attack
    - Nuclear Detonation
    - Atmospheric Vehicle Attack
    - Space System Attack
- Aerospace Control
  - Provide Air Sovereignty & Strategic Air Defense
    - National and Multinational Surveillance
    - Detection
    - Identification
    - Tracking
    - Interception

NORAD OPEVAL

Missile Warning Architecture

VV 99-1 AV 99-2

Missile Warning Mission

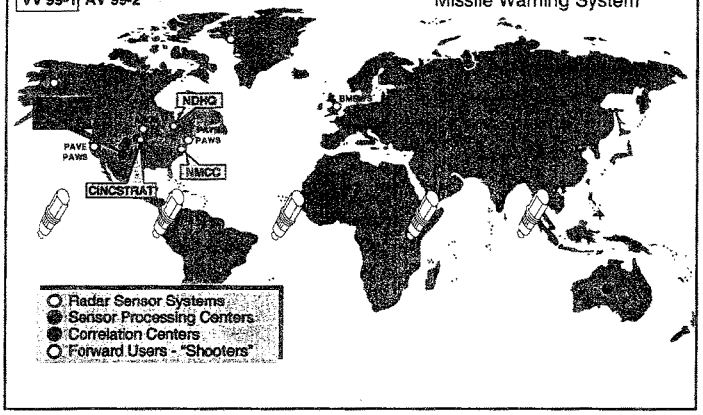


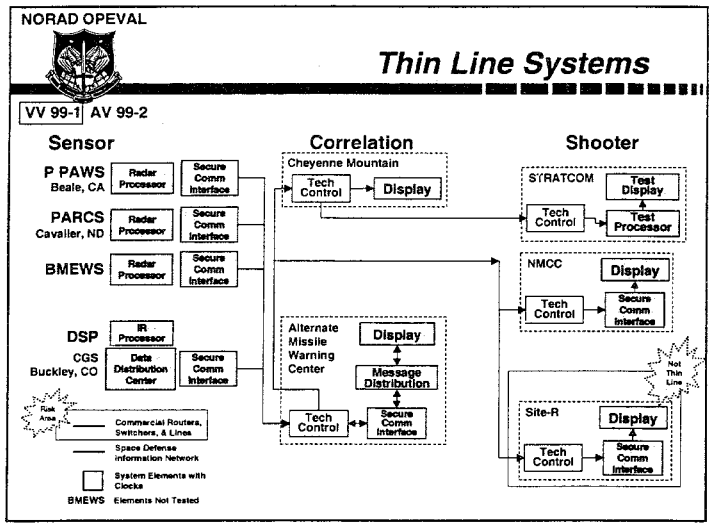
NORAD OPEVAL

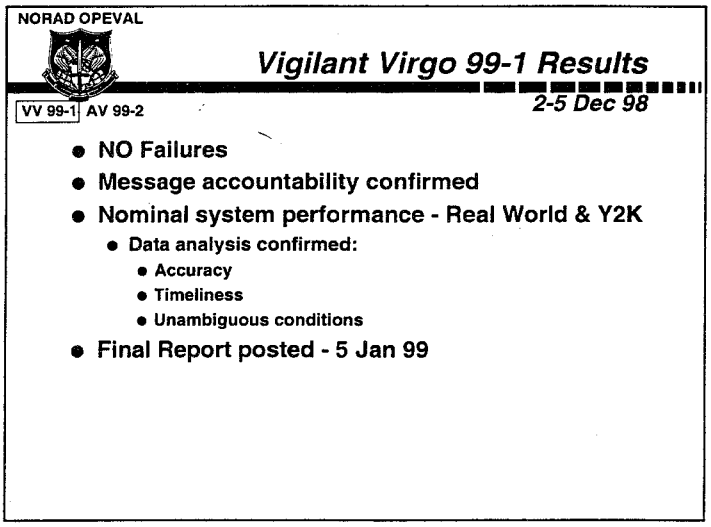
Operational Architecture

VV 99-1 AV 99-2

Missile Warning System




NORAD OPEVAL
Thin Line Systems
VV 99-1 AV 99-2
Sensor
Correlation
Shooter
P PAWS
Beale, CA
PARCS
Cavalier, ND
BMEWS
DSP
CGS
Buckley, CO
Radar Processor
IR Processor
Data Distribution Center
Secure Comm Interface
Cheyenne Mountain
Tech Control
Display
Alternate Missile Warning Center
Message Distribution
STRATCOM
Test Display
Test Processor
NMCC
Secure Comm Interface
Site-R
Not Thin Line
Risk Area
Commercial Routers, Switches, & Lines
Space Defense Information Network
System Elements with Clocks
BMEWS Elements Not Tested


NORAD OPEVAL
Vigilant Virgo 99-1 Results
2-5 Dec 98
VV 99-1 AV 99-2
NO Failures
Message accountability confirmed
Nominal system performance - Real World & Y2K
Data analysis confirmed:
Accuracy
Timeliness
Unambiguous conditions
Final Report posted - 5 Jan 99

NORAD OPEVAL

Amalgam Virgo 99-2

VV 99-1 | AV 99-2

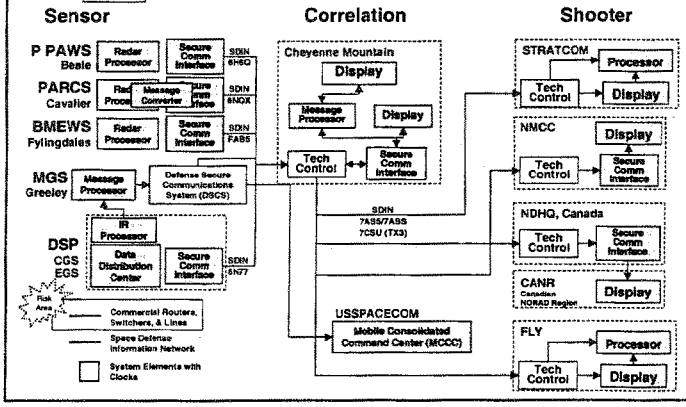
- **16 - 19 Feb: Space and Missile Warning - Complete**
  - Scenario includes 4 events each run
    - Pre-, Trans-, and Post-Rollover
    - Three IR sites, 3 Missile Radar sites, 4 Space Radar sites
- **22 - 26 Feb: Air Warning and Control - Complete**
  - Scenario includes live and simulated tracks
    - Built-in contingency & platforms for aircraft control
    - Pre-, Trans, and Post-Rollover
    - One each of five critical radar sensor types; all three regions

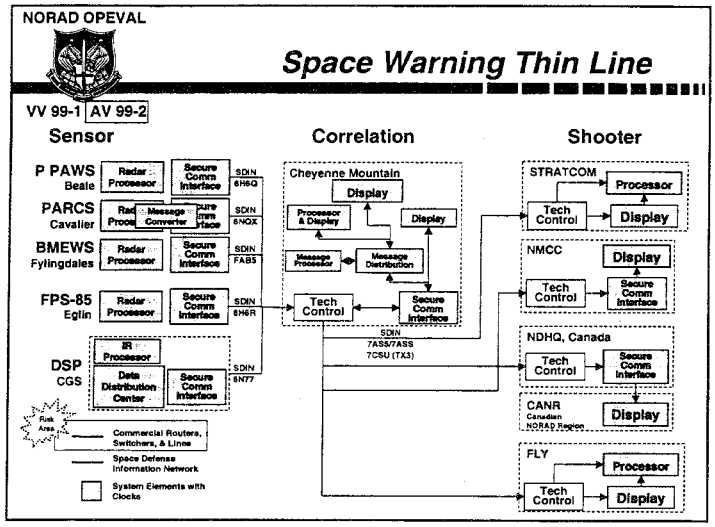
	14 Feb	M	T	W	T	F	S
Complete		Holiday	Date 1	Date 2	Date 3	Date 4	
		M	T	W	T	F	S
		Baseline	Date 1	Date 2	Date 3	Date 4	

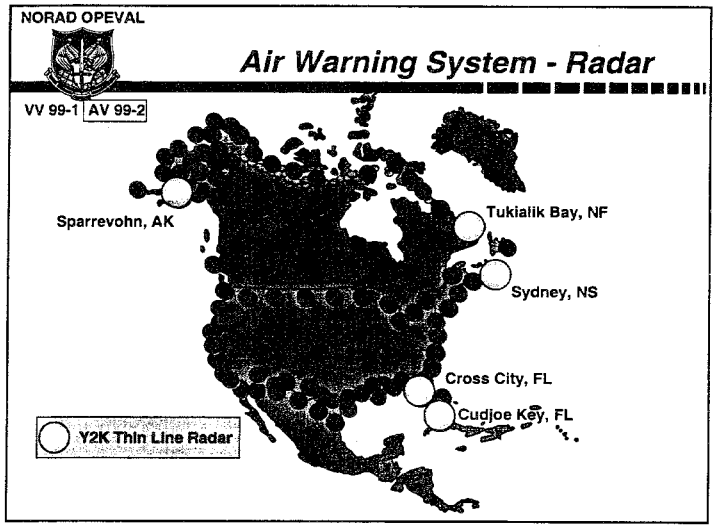
NORAD OPEVAL

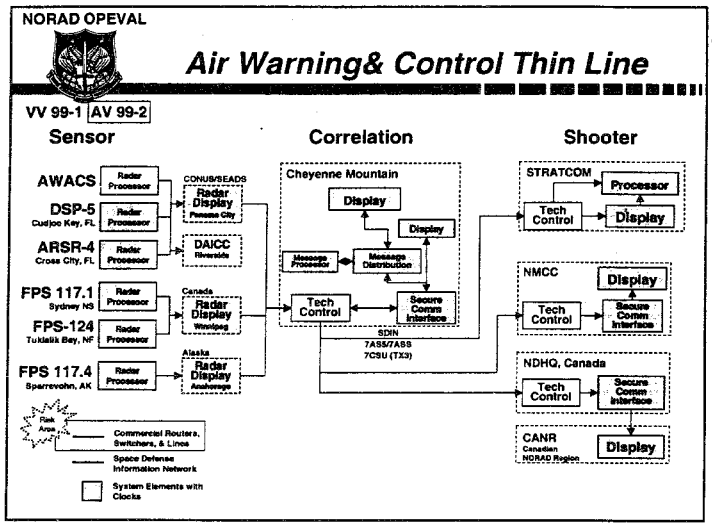
Missile Warning Thin Line

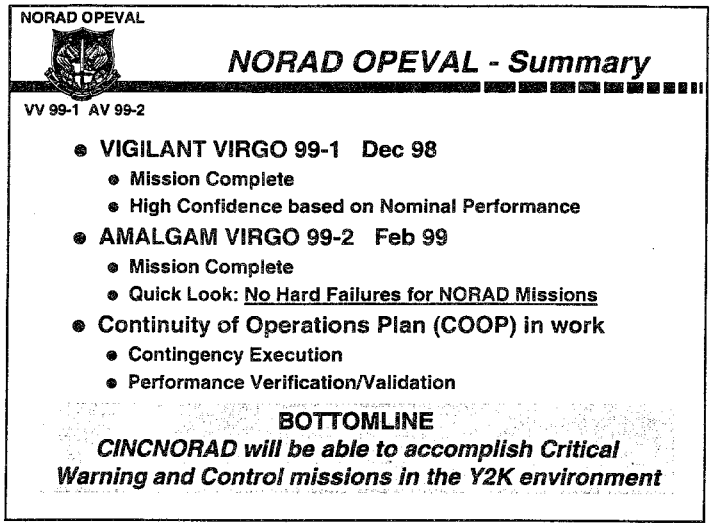
VV 99-1 | AV 99-2




NORAD OPEVAL
Space Warning Thin Line
VV 99-1 AV 99-2
Sensor
Correlation
Shooter
P PAWS
Beale
PARCS
Cavalier
BMEWS
Fylingdales
FPS-85
Eglin
DSP
CGS
Radar Processor
Secure Comm Interface
SDIN
Cheyenne Mountain
Display
Processor & Display
Message Processor
Message Distribution
Tech Control
STRATCOM
Processor
NMCC
NDHQ, Canada
CANR
FLY
Commercial Routers, Switchers, & Lines
Space Defense Information Network
System Elements with Clocks


NORAD OPEVAL
Air Warning System - Radar
VV 99-1 AV 99-2
Sparrevohn, AK
Tukialik Bay, NF
Sydney, NS
Cross City, FL
Cudjoe Key, FL
Y2K Thin Line Radar


NORAD OPEVAL
Air Warning& Control Thin Line
VV 99-1 AV 99-2
Sensor
Correlation
Shooter
AWACS
DSP-5
Cudjoe Key, FL
ARSR-4
Cross City, FL
FPS 117.1
Sydney NS
FPS-124
Tuktalik Bay, NF
FPS 117.4
Sparrevohn, AK
Radar Processor
CONUS/SEADS
Radar Display
Panama City
DAICC
Riverside
Canada
Radar Display
Winnipeg
Alaska
Radar Display
Anchorage
Risk Area
Commercial Routers, Switchers, & Lines
Space Defense Information Network
System Elements with Clocks
Cheyenne Mountain
Display
Display
Message Processor
Message Distribution
Tech Control
Secure Comm Interface
SDN
7AS5/7AS5
7CSU (TX3)
STRATCOM
Processor
Tech Control
Display
NMCC
Display
Tech Control
Secure Comm Interface
NDHQ, Canada
Tech Control
Secure Comm Interface
CANR
Canadian NORAD Region
Display


NORAD OPEVAL
NORAD OPEVAL - Summary
VV 99-1 AV 99-2
VIGILANT VIRGO 99-1 Dec 98
Mission Complete
High Confidence based on Nominal Performance
AMALGAM VIRGO 99-2 Feb 99
Mission Complete
Quick Look: No Hard Failures for NORAD Missions
Continuity of Operations Plan (COOP) in work
Contingency Execution
Performance Verification/Validation
BOTTOMLINE
CINCNORAD will be able to accomplish Critical Warning and Control missions in the Y2K environment

Mr. HORN. Well, let just sum it up. You have had extensive testing and interactions in a real-world environment for most of your systems in NORAD, and you only have very few left to go. And as I have looked at the basic Y2K mission-critical system, we are talking about the Army, at 10 out of 24, OK; USN, 10 out of 55; USAF, 10 out of 14, and then the nuclear side, of the 275, most will be completed by the end of March, except for 12 different systems, as I heard the testimony. So, how much is really left here after the President's date of March 31st?

Colonel SMITH. As far as our mission-critical systems——

Mr. HORN. Yes.

Colonel SMITH [continuing]. For NORAD? All of the mission-critical systems for NORAD, those that are supplied to us by the Army, Navy, Air Force, are compliant. We have some non-mission-critical systems of which only one will extend, as far as I understand it, past the 31 March deadline.

Mr. HORN. OK, they are compliant and that is after the testing in a regular real-world interaction going on around it?

Colonel SMITH. That is correct, sir.

Mr. HAMRE. Mr. Chairman, if I might just wrap up just to say that I think Admiral Willard said something very important to me while we were listening to R.F., and that was, we are glad that we saw a couple of failures, because if they just came back and said everything worked fine, we would think our testing wasn't good. So we look on failures not as a sign that we have got problems, but, frankly, that the test environment is working. And I think that it is very important.

Sir, that really wraps up what we wanted to say to you. Of course, I got all the smart guys here to answer the real hard questions.

Mr. HORN. Since you are going to succeeded by Assistant Secretary Money, is part of the problem why the Pentagon was delayed, the fact that General Paige retired as Assistant Secretary, then his Deputy Assistant Secretary retired, then two Directors under them retired, so, I taketh you have had a tough time filling that area.

Mr. HAMRE. Well, sir, I think that in fairness, it is half right and half wrong. What is right about it, is that you are absolutely right. Art Money has made all the difference in the world to get in there. And we went for a period of time of 8 months without having somebody in the job. So, that was a huge change. I remember attending my first Y2K session back about 4 years ago when I was a Comptroller, and it was very hard to get people to feel that this was something other than just a computer geek problem. You know, this was largely viewed as just a technical problem. And it really took until last summer, when we said, and this isn't about computers; this is about fighting and winning wars; this is about people; this is about leadership. And it was bringing them onboard, and fortunately, what Art was able to do was to bring a discipline process that he and Marv and Bill had worked out, so that we really could take advantage of that energy that the Secretary put into the system.

It is working. I think we are going to be OK. I don't want to give you the impression that we won't have some surprises, but we are going to be able to take care of this country.

Mr. HORN. Let me ask you one last question for me, and I will yield to my colleagues. The microchip situation, not just the critical mission bit. How many? You have probably got a billion or so——

Mr. HAMRE. Yes, lots of them.

Mr. HORN [continuing]. Somewhere throughout the Department of Defense. What are we doing on that?

Mr. HAMRE. Sir, some others here know. I think the answer is we have done some testing already. We found that the problem isn't nearly bigger than we thought it was, and who——

Admiral WILLARD. I can cover it in general. Sir, the process of checking microprocessors is part of our remediation series of events. It is actually handled in the management plan. And these systems that you are seeing tested here are not strictly date functions that are associated with software, but, indeed, date functions associated with microprocessors as well. And you are right, there are a great many of them in our systems. But, once again, as we took the systems through testing and through remediation, in addition to our software requirements, microprocessors were part of that entire checks-and-balances issue.

Mr. HORN. I yield 5 minutes to Mrs. Morella, the co-chairman of the task force.

Mrs. MORELLA. Thank you very much. I thank you for your testimony and the charts, and I think the testimony has been somewhat comforting.

I have a number of concerns. One was the personality; you have tried to address that. Computer chips was another one. I am concerned about the contractors that you deal with, knowing that you deal with so many of them. How are you going to handle making sure that not only they say they are compliant, but that they have been adequately tested? I don't know whether you have a special department or group that are looking at that, or whether each of the compartments is looking at its own, in terms of its contractors, and have you found them reticent to respond to your inquiry in terms of validating or assuring that they are compliant?

Mr. HAMRE. Mrs. Morella, of course, we have so many contractors.

Mrs. MORELLA. Yes.

Mr. HAMRE. I mean, several hundred thousands of contractors that we work with, and, of course, all the utilities all around the country, et cetera. So, it is not a process that we can run centrally. This is one where we have to give individual organizations responsibility to check with who they work with most and that sort of thing. And everybody has been given that job.

And our answer is that, for example, if we have a contractor we are not sure if they are going to be able to provide spare parts, you know, in a Y2K environment, let's not go out and stockpile a bunch of spare parts. Let's find a contractor who is. You know, let's find somebody. Let's use the power of the marketplace here to get people to fix their systems.

Now, we have found it difficult for companies to give us unequivocal answers about where they will be. And it is partly this

fear of lawsuits, you know, that has frozen up so many people here with year 2000. This is a big problem. This is a problem that, frankly, rests—there is only one place in the world that you can settle it; that is here in Congress, and that is to reconcile the relative priorities of the legal due process rights that belong with both aggrieved parties and claimants and defenders versus the problem we are having getting unequivocal answers to questions.

We are doing our best to work around that, but, frankly, the environment people that are in there are never going to give you 100 percent guarantees. I can understand that because of the environment we have. So, we work other ways of trying to get a handle on, are they going to be ready; aren't they? We ask to see, well, tell us about your testing plan. Tell us about how you are going through your internal procedures to confirm you will be compliant. You can get a pretty good sense pretty quick. I mean, if they get kind of a blank bovine and stare, you know that we are in trouble.

Mrs. MORELLA. I hope so, because I still find that daunting and rather frightening. Are you also indicating that you feel some kind of liability legislation is appropriate? I mean, you know we have legislation that is saying that it is not a waiver of immunity; it does not offer the immunity, not a waiver of liability, but it looks at frivolous lawsuits, talks about alternative dispute resolution, and has a series of other components that might well reduce that chilling effect. Do you have a feeling about it?

Mr. HAMRE. Madam Chairwoman, I really have to defer to John Koskinen, to speak on behalf of the administration, I think, for that, rather than I don't—the Department of Defense wouldn't have views independent of what the administration would have, and I really need to have him answer that question.

Mrs. MORELLA. I understand the situation, and I guess I was just kind of thinking personally.

Mr. HAMRE. And we would like to work together with you to get that, yes.

Mrs. MORELLA. My other concern, and I would certainly invite, if time allows, our Inspector General and GAO representative to comment on—I am very concerned about other countries; you mentioned Russia; you mentioned trying to assuage their concerns and to help them, and I assume this is Kazahkstan and all of the other Republics, too, of the former Soviet Union. But, I also traveled in Asia and even to Tokyo, to Japan, and of course, Indonesia and Korea, and they are just so far behind in terms of remedying of being compliant with Y2K. I don't even think they understand all the ramifications of it.

My concern is, of course, obviously, the interoperability, the fact that we have bases on so many of those places, too. Are we placing our own people in jeopardy about the world? Would you like to comment further on that?

Mr. HAMRE. I will try to be very brief. We are not worried about our war-fighting systems, because, frankly, they are kind of designed to operate independently, wherever they are. But we are worried about, you know, the living conditions and the support functions that go on that we have overseas. We are apprehensive about where things stand in Korea and Japan, not that they don't have very talented people to fix things; they do, enormously capa-

ble people. But, you know, they have had their hands full with some serious economic problems for the last year and a half and they probably haven't been spending as much attention to this as have we. So, we are nervous about it. We have asked our Commander-in-Chief for United States Forces in Korea to work with the Koreans, and I believe that we really do have a good dialog now established with the Koreans about it.

We are particularly worried about things like electrical power, things of that nature, telecommunications. Probably our biggest concern, if we have it overseas, is with nuclear power reactors in the old Soviet Union. We don't know that there are very good safety backup arrangements for them. That makes us worried. You know, we are nervous about that. Again, it is not so much that it affects our ability to operate our military ability, but I think in a broader sense, I think Americans should worry about that.

Why don't I see if our colleagues here have some followup notes.

Mrs. MORELLA. Thank you.

Mr. BROCK. I think that is a very important area, Mrs. Morella. The potential for Y2K disruptions in other countries I believe is much greater than it is in the United States. I think that Deputy Secretary Hamre is correct when he states that it might not have an immediate impact on our forces, but it, obviously, has an impact on economic relationships, on trade relationships, on our ability to get goods and services into the United States, and on our ability to have effective harmonious relationships with other countries that might be having disruptions caused by large-scale failures. The problem is, it is unlike the Department of Defense where we are able to go in and identify the issues and come up before you and discuss them; we don't have that same level of visibility within the international arena.

Mrs. MORELLA. Mr. Lieberman.

Mr. LIEBERMAN. Within the last few weeks, I have had people doing extensive work in Korea and in the Middle Eastern countries, where we have forces stationed, and we have also done some work in Europe. I would concur that most countries in the world, other than most of the European countries, Australia, New Zealand, and Canada, are well behind us. We need to do a lot more communicating with them than has been done in the past.

We have found basically a lot of situations where they are waiting for U.S. officials to come talk to them and we have not done that yet. So, the auditors have been trying to close those communication gaps.

Actually, I think the level of awareness is going up very steeply in all of those countries, for a variety of reasons. There was a World Bank report in January which shook up lots of countries when the World Bank reported that they were not doing well in Y2K. In the Republic of Korea's case, they didn't answer the mail from the World Bank, so they got a blank on the chart which showed whether or not you were doing anything, and they are very upset, because they do have an active program now.

We are dependent on these foreign countries for everything from air traffic control in Kuwait and using Kuwaiti hospitals to Republic of Korea railroads, power, water, all kinds of things. So, this is a critical concern. And it is one of those areas that, as I mentioned

in my statement, still has to be worked very intensively as the year goes on. You probably couldn't have done that much 6 months ago because the countries simply weren't ready to talk, but I think now they are.

And all of those that are members of the Organization for Economic Cooperation and Development, which include Japan, Korea, and most of the European countries where we have bases, are pushing forward much more vigorously with this now than they were before the turn of the year.

Mrs. MORELLA. Thank you. I know my time has expired.

Mr. HORN. Thank you.

Mrs. MORELLA. China is another country, too, that, you know, enormous proportions. Thank you.

Mr. HORN. Thank you. I now yield 5 minutes requesting to Mr. Turner of Texas, the ranking member of the subcommittee.

Mr. HAMRE. If you will indulge me, sir, Mr. Money, who knows everything, anyway, I am going to ask him to sit in my place.

Mr. HORN. Well, can you indulge me for 30 seconds?

Mr. HAMRE. Oh, yes, sir, of course; you are the chairman.

Mr. HORN. And I will tell you this: You will know with your experience on the Hill, but occasionally, a Member will throw in something when they have got the big man in front of them. So, this is a big man question that has come over from the Pentagon. "For as long as anybody can remember, we Pentagon employees have been walking from the parking lot to the building, no matter how far from the building we have had to walk. Reason: it is against regulations to use government vehicles for employment commuting purposes, which is what a shuttle would be. Now, we find out the Defense Supply Center in Columbus, Ohio, operates a parking lot shuttle in a parking lot much smaller than the Pentagon's. As justification, they site DOD Regulation 4500.36–R. If that regulation can justify shuttle service for DOD employees in Columbus, Ohio, then why can't it justify the same service right here at the Pentagon."

I merely bring this up because they might be working on the Y2K problem—[laughter]—and if you would not mind, Mr. Secretary——

Mr. HAMRE. I will look into it.

Mr. HORN [continuing]. Making sure there is an answer on disparity of treatment with this Department.

Mr. HAMRE. I absolutely will look into it. It is in our interest to get the workers there earlier. So, I will find out what is going on.

Mr. HORN. OK. Thank you very much. [Laughter.]

Mr. Money, then, will replace you.

And, Mr. Money, tell us how long it took to, one, to get your appointment up there, and, two, to get confirmed?

Mr. MONEY. It is not even up there yet. [Laughter.]

Mr. HORN. Because we have all been wondering, you know, where are you? And, I take it, it took rather lengthy or what?

Mr. MONEY. No, sir. I am still the senior civilian official.

Mr. HORN. I see. OK. So, you haven't been confirmed yet?

Mr. MONEY. I was confirmed about 3-plus years ago as the Assistant Secretary of the Air Force for Research, Development, and Acquisition. Dr. Hamre asked me to come down about a year ago

to take on this job. So, pending, if I am nominated and if I am confirmed, then I would be the Assistant Secretary, but today I am the senior civilian official of the Department of Defense.

Mr. HORN. This is the Assistant Secretary C3 plus intelligence?

Mr. MONEY. Yes, sir.

Mr. HORN. Yes, we are glad to have you onboard.

Mr. MONEY. My pleasure.

Mr. HORN. And Mr. Turner now has the floor.

Mr. TURNER. Thank you, Mr. Chairman.

Secretary Money, after listening to Dr. Hamre, I think we all are very much reassured that the Department of Defense has gotten this house in order, and obviously, you are due much of the credit for that. And I think we heard some very interesting proposals that you are planning to implement, one of which I found very interesting, and that is the idea that you are going to invite the Russian military to come look over the shoulders of those who man our nuclear weapon systems on January 1. I wondered if that had ever been done before. This seems like certainly a groundbreaking event?

Mr. MONEY. Not in the nuclear area, to my knowledge, Mr. Turner. The State Department is actually working that. We came up with the idea several months ago, but it is being worked through the State Department. As it was alluded to earlier; there have been several groups going back and forth to Russia discussing this. Also, I believe there is some discussion about bringing in anti-nuclear power, so that in fact they can, in fact, see that, through our early warning systems, if anything else is going on, to assure them that if there are screens that go blank or all light up, whatever may be a problem out of Y2K, that there is an independent or yet another source of information to preclude any inadvertent reactions.

I might, if I could, just add onto a previous question that the IG responded to. Mr. Curtis, back here, he has been overseas a lot. We have had several workshops with various countries. In particular, what comes to mind are several NATO allies. We have also gone into Australia, Canada, into Russia, more recently. So, we have had an outreach program from the DOD. But the overall outreach program, and in fact it was being handled under the coordination with the Y2K coordinator, John Koskinen, but of note, he has had a meeting, I want to say, maybe 6 weeks ago, 2 months ago, up at the United Nations, where there were over 100 countries present, where the problem was talked about, awareness was heightened, as a beginning to get other countries in the world more aware, if not, into remediation.

So, there has been a fair amount of outreach, albeit, there always could be more. But the State Department is also looking into that. But, when it comes to Y2K, we look to John Koskinen as being the defining authority on all those activities.

Mr. TURNER. What kind of potential problems do we face with our NATO allies where we have joint operations, say Bosnia? What kind of potential problem do we have, and have we done anything to try to remedy that?

Mr. MONEY. Absolutely. We have the Supreme Allied Commander, General Wes Clark. He is also CINC for European command. So, he has those two hats. He stands up in front of the Sec-

retary and the Deputy on certifying that the United States Forces in Europe are ready, but, also, we have looked at him and tried to help in the NATO area.

Frankly, I have some concerns in NATO. Some of the countries are going after the Y2K problem with a vengeance; others are less so. The U.K., Netherlands, France, are very much up on Y2K. Germany is maybe a little bit behind, and then some of the other countries are quite a ways behind. In particular, operations into Bosnia today rely on circuits that are not Y2K compliant. We are trying to get them to be Y2K compliant by the end of the year, but there are some worries about that. We also have backups, though, from a U.S. standpoint, that would help.

So, I can't give you a blanket guarantee that all the communications and command and control of the NATO are up and compliant to date because they are not. But there is effort being made against those areas, albeit I think it is a little late and maybe too short, not enough being done.

Mr. TURNER. So, the reports that we have been given today really are directed our own systems, and really do not represent an assessment of what kind of problems we might have when we are doing a joint operation with NATO?

Mr. MONEY. You are absolutely right. What we are talking about is what the DOD can do for operations when there is a coalition or an allied operation; these folks will also look at that. So, let me just give Admiral Willard here a chance, but, also, the people here from the Army, Navy, Air Force, and Marine Corps.

Admiral WILLARD. I would say this: Very recently, the Y2K Task Force lead for the North Atlantic Treaty Organization [NATO] visited us in the Pentagon, in fact, visited with me for some time just to compare notes in terms of the approaches to our respective problems. He is from the United Kingdom and was assigned the responsibility to oversee their remediation process and evaluation process. And, as Mr. Money points out, they are not as far along as this Department is right now, but are enthusiastic, and they understand the process. If not in remediation of actual systems, then in building the necessary contingency plans to be able to work around them. Also, we have an ongoing dialog between our European command and NATO, and NATO has an infrastructure that is, in fact, in place to address the problem.

Mr. MONEY. Admiral Johnson, you want to talk about the Navy, and in particular, Mr. Turner's question?

Admiral JOHNSON. We started last year recognizing that we had to deploy ships year 2000 compliant at least 6 months ahead of time because of the length of our cycle. The first year 2000 compliant battle group is the Constellation. We just finished the year 2000 joint systems integration test. Well, actually we haven't finished it. It is ongoing right now. But, New Year's Day 2000 was at 1600 local in the SOCAL operating areas on Saturday. I was there. The clocks rolled over and flight operations and the man overboard drill and everything else just continued, and they held a New Year's Eve party on board.

The HMCS Regina, a Canadian ship, is deploying with that battle group. She has been involved in our testing and planning. Much of our C3 interoperability with our allies in the battle group envi-

ronment are the results of FMS sales. Our FMS offices have contacted our allies, have informed them which ones of our sales are year 2000 compliant, which ones aren't, and what the fixes are. We are providing that information to our allies so that they can implement those changes. Regina is an example where we had the Canadians involved in our testing because they are going to deploy with us, and have gotten her capability tested in a year 2000 environment.

Mr. HORN. General Ambrose.

General AMBROSE From the Air Force perspective, we are absolutely sure that our systems and our people will be ready to go on January 1, 2000. For foreign systems on the FMS side of things, we do a very good job of telling foreign countries to whom we export technology, what the status of that equipment is. And we know what the status of it is on the day that we transfer it to that foreign country. Now, quite honestly, if that country chooses to modify the equipment somehow or add a third country's technology to it, then we no longer know the status of it.

For that reason, interoperability has become an important issue to us. And what we have done, is engaged our major commands, most of whom are components to a commander-in-chief somewhere in the world, and asked them to engage those commanders-in-chief, because the approach that you take to interoperability will be different in every theater because of the mix of countries you have there, because of the Y2K status of those countries, and there is certainly no uniformity in that anywhere across the globe.

So, the right answer to this, I believe, is the approach we have taken, and that is, to have the war-fighters engage our coalition partners and allies and to work out those interoperability issues with them in theater for the situation they encounter.

Mr. HORN. The answer to Mr. Turner's question?

Ms. BROWNING. Good morning, Mr. Horn. First, let me tell you that, as of right now, about 95 percent of the Army war-fighting systems are compliant, and the rest of our systems, as has been talked earlier, will be compliant toward the end of the year, between now and then.

Concerning the issue of interoperability, right now we are in the process of going through all our war-fighting divisions. Our 10 divisions are 4 corps, and we are testing all of the systems. Probably the biggest issue we have, as has been indicated by my colleagues, is the foreign military. We are working with our Army Materiel Command. We are working with our partners both in Korea and Europe to make sure that as we do the test not only in our corps and divisions, but also with unified commanders, that the equipment we are using in the coalition warfare, that information is knowledgeable to these folks, they are looking at our implementation of that, and if they have a system they need to adapt, that we provide them all the information in doing that. So, we guarantee when the United States, when the Army weapons are given to those other countries, we give them the status of the Y2K compliancy of those weapon systems.

Mr. HORN. Colonel McHale.

Colonel MCHALE. Thank you, sir. The Marine Corps presently has fixed 84 percent of our mission-critical systems, and we are on

track to finish the remainder prior to September of this year. The way the Marine Corps is configured, we are more expeditionary and less dependent upon overseas bases, so we don't have the problems that the Army and the Air Force would have. We just completed an operational evaluation that we conducted in Norway, which was not intended to be an interoperability exercise with the Norwegians, but they observed our exercises, and we traded information with them about the status of where they were, and came away quite confident that they were taking similar measures, although they are not on the same time line that we are. We demonstrated some interoperability with them in Y2K systems, although it was not part of a detailed technical plan, and again, came away with the idea that they were on track and performing very similar measures that we were.

Mr. HORN. Good. I thank the gentleman for that question, and now yield the 5-minutes to the vice chairman of the Subcommittee on Government Management, Information, and Technology, Mrs. Biggert, of Illinois.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Rear Admiral Willard, I had the opportunity 2 weeks ago to be at the Southern Command on my way on counternarcotics, visiting six countries in Central and South America, and was very impressed with what was happening down there. You mentioned that the Y2K problem was not jeopardizing their mission down there, that they were able to do both at once. I wondered if, since it seems to have been a lot of progress made down there and doing the end-to-end testing, if they are providing help to other areas, if they are sending anybody there to work on this problem or are all these commands doing it separately?

Admiral WILLARD. In the case of Southern Command, the entire area of responsibility for that CINC, the commands, both interagency and within Southern Command proper, are all participating in this event. That said, there is ongoing dialog with some of our host nations to involve them in our year 2000 assessments, and it has met with limited success. I would say that the true successes have been with our Uniformed Services in the operating area, as well as the Coast Guard and the other agencies down there that we are coordinating with. But, as is the case in Europe and as is the case in Asia, we find it challenging in the Southern Command to ascertain the exact status of infrastructures in and around our forces that are operating there, and we continue to strive to do that.

Mrs. BIGGERT. I guess then my next question, is there a coordination between the different commands, like in Europe? Is there anybody that is in charge of overseeing all of those areas and making sure where there are successes in the testing of one area that that is forwarded to the other areas and to see if there is any difference?

Admiral WILLARD. As you know, geographically, our world is divided among our uniformed commanders in chiefs, and they are, in fact, responsible for the conduct of the operations evaluations that you have seen illustrated this morning. They all have a reporting requirement not only insofar as their operations evaluations are concerned, but also as an ongoing assessment of the status of their

forces within those regions of the world. So they are maintaining visibility on both the success of their operations evaluations as well as the forces that are in country by the various Services.

And I would say too that the Uniformed Services individually maintain a great deal of visibility on their foreign base and facilities structures overseas and are continuously reporting their status as the year 2000 is concerned.

Mrs. BIGGERT. I guess what I am asking is, at what point is there coordination between all the services? At what level is there someone who is coordinating all of the services?

Admiral WILLARD. That is Mr. Money.

Mrs. BIGGERT. Mr. Money would probably know.

Admiral WILLARD. It is also the Joint Staff to some extent. So, though we focus primarily on the unified commands, the real focal point of effort, the real coordinating effort within the Pentagon is the conduct of the synchronization meetings that were described earlier where the uniformed services are represented. We in the Joint Staff represent our commanders-in-chief, and all of the agencies are responsible for their functional areas, and their tasks are also represented there, and we discuss at that level all of our interactions.

Mr. MONEY. Ma'am, if I could just add to that—this admiral here is the joint staff representative that also pulls all of that together. And he and my deputy, Marv Langston, meet weekly now on these harmonizing meetings, if you will, to sort those things out.

I also want to just mention, not one CINC stands alone. There is supporting CINCs like transportation or space command, or whatever; that information is also being brought to those CINCs. By law, we have two tests for everything we are doing, and you can see there is 27, going to 31 tests; there is 30 CINCs, so there is a lot of duplication of support functions that are also being tested. So, they are not totally standalone per se.

Mrs. BIGGERT. Thank you.

I guess then, Mr. Brock, you talked about the management function and how there needs to be improvement with that. Is this the area that you are talking about?

Mr. BROCK. Yes, ma'am, exactly. The example you saw earlier regarding the NORAD operational evaluation, was an example of a timely controlled test, well-defined test parameters, a well-defined test script; a test script was followed, and things worked. When things didn't work, there was a way of going around it, and people were able to track it. That, we have been finding, is fairly typical of what we are seeing in the operational evaluations.

However, on the functional evaluations, and when we review the plans of the functional evaluations—these are things like logistics, health, personnel, accounting, processes that the Department depends on on a day-to-day basis to support everything—and when we review their plans, we don't find that same level. I mean, we see a lack of test schedules, a lack of identification of specific goals and objectives, and it is more difficult to track what is going on there.

I think the synchronization meetings that Mr. Money was talking about go a long ways toward resolving some of these differences, and we attend those synchronization meetings. But, to some de-

gree, they are just reports of individual components and they are not funneled in such a way that all the information comes in in the same format or the same form that is easy for the top managers to make decisions about, and to determine what is going wrong and what is going right. So, this is the area that we are recommending that they need to improve, the type of management information coming in, so that there can be better oversight over these processes.

Mrs. BIGGERT. Thank you.

Mr. HORN. If I might just interject a minute, to clarify that answer—you make a very good point, Mr. Brock. I would like to ask Mr. Money and yourself if you have seen not only a report that comes in on a regular cycle to the responsible manager—I would be curious, Mr. Money, in answer to Mr. Brock's answer to Mrs. Biggert—to what degree do you have them on, say, weekly reports, every other week, or monthly reports? What is our timetable there to get a sense of urgency throughout the whole establishment?

Mr. MONEY. Let's see, at the Department level, we meet monthly, reviewing what has transpired according to a plan from the previous month. Each of these functional people or PSA's, Principal Staff Authorities, over whatever these functional areas are, are meeting more often with whatever is going on in their particular area.

I don't dispute or find any deviation from what Jack is talking about. Those plans aren't as rigorous and robust as we'd like them. We will continue to work with those folks. But I would say, this is now getting daily attention at some level. It rolls up, and we will have a roughly a 2-hour session with the Deputy Secretary once a month. Your staff, other committee's staff from Congress are invited and attend, as well as the IG, GAO, and John Koskinen has been very good at attending every one of those as well. So, it depends on what level you are on. There are various daily to monthly attention being given.

I want to just foot-stomp, if I might, what Dr. Hamre said; some of the reporting, though, is obviously late, but also, it is burdensome. Let me give you an example. Every time you put out a report card for us, and when we were still at the "F" or the "D-minus" level, my office, frankly, it would be the Secretary of Defense, or, frankly, the President, would get letters from the general public. Those would then go to the Secretary of Defense and eventually get to my office. We have 10 people, or thereabouts, continuously responding to the private citizen. I would rather have those 10 people off working on Y2K compliance versus answering mail, where our policy is we will answer every piece of mail. So, that is part of the additional duties, if you will, that maybe aren't quite as productive as we would like, but we will do that.

Mr. HORN. Well, if you are successful in getting all the mail answered, we would like you to come over and spend a few weeks on Capital Hill. They keep telling us why they can't get it answered.

I now yield to the gentlewoman from New York, Mrs. Maloney.

Mrs. MALONEY. Thank you.

I would like to ask the IG, your office has completed 50 reports on the Y2K efforts in DOD. You have already completed 50 reports,

and I am told that you have an additional 50 reports in progress. Is that true?

Mr. LIEBERMAN. Yes, ma'am.

Mrs. MALONEY. Well, then it is obviously, I would say, the highest priority of your office. I would like to know, has the Department of Defense responded adequately to your concerns and the problems that you have raised?

Mr. LIEBERMAN. Yes. I think it is fair to say that we probably never have had as much responsiveness from the most senior levels of the Department to any given body of audit work than we have had to these Y2K audits.

References have been made to some of the positive outcomes or silver linings in the cloud from Y2K—I think one of the lessons learned is that a lot of managers in the Department have learned how to use their internal auditors constructively, and to unleash us instead of trying to keep us out of areas. I would say, with very few exceptions, that there are mechanisms to work those exceptions, management has normally taken corrective action even before we formally report.

Mrs. MALONEY. As recently as last September, you found that 9 of the 16 weapon systems contracts that you reviewed, that they did not contain the required language for Y2K 2000 compliance. And this seems like a widespread problem due to DOD's decentralization of contracts and procurements in weapons systems. Do DOD contracts now contain a standard Y2K compliance assurance clause?

Mr. LIEBERMAN. They are supposed to. We are still finding isolated instances where they don't, but I would say the problem basically is as close to being solved as it is going to be. We will still look for that in every single audit that we do, but I think the Department has come a long way. Initially, auditors were finding this non-compliance quite frequently, but now it has become an isolated exception.

Mrs. MALONEY. The DOD report to OMB, no longer contains information on the status of the intelligence community. And again, I would like to ask the IG, the current status of the intelligence computer system and whether there is a concern within the intelligence community. And I would also like to add that possibly we shouldn't be asking detailed questions about the intelligence community in public hearings. If you would be more comfortable, I have a series of questions in writing I could give to you on the intelligence community.

Mr. LIEBERMAN. That would be fine. And Mr. Money runs the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), so he can weigh-in also.

Mr. HORN. And if you can't respond here, we will have Mrs. Maloney's questions go over to you, and at this point in the record, without objection, the answers and questions will be put in.

Mr. MONEY. Yes, sir, but I can give you an answer here. All those numbers included every critical system that DOD needs to conduct any operations, including intelligence systems. The data base issue was dropped out, meaning it is handled at a classified data base because we were concerned about how much information

was present in that data base. So, it is still being reported as handled in a classified manner.

Mrs. MALONEY. But I tell you, the report that you put up there, it was quite comprehensive, and it had many tests taking place at the same time.

Mr. MONEY. Yes, ma'am. And those included the intelligence system that whatever that test needed.

Mrs. MALONEY. Right. OK, I will still put my questions in though.

Mr. MONEY. And we will be glad to answer.

Mrs. MALONEY. On the weapons systems, again, I would like to go back to the IG. How safe are we that we won't have some weapon that goes off? And we have got some serious weapons now. I understand that most of our nuclear weapons have a manual process that is required to launch them. They have to be manually activated, but that we have other serious weapons that aren't manually operated, that are computer operated. And how safe are we? What is the status of these weapons systems? Is it correct to say that they will fail safe, that they will not accidently misfire? Have you been reviewing all of these and making sure there won't be a problem?

Mr. LIEBERMAN. We have only looked at a small sampling of weapon systems, I would say probably about 20. In none of those cases were there any dangers of that type. Statistically, the Department is reporting that about 90 percent of the weapon systems are compliant at this point. There are 40 some that still need to be worked through as the year progresses. But I would have to defer to my colleagues here to the left to talk to those systems that the IG hasn't looked at.

Mr. MONEY. Let me answer one question and then pass it down, because this is not only a joint staff answer, but each service.

But just go back a few weeks. We had missiles about to be in the air, and we had positive recall in a command-and-control sense. They may be an automated sense, but initially they are started, and there is a person in the loop. Some of that requires Presidential authority and release; others require CINC. So, it is not just that things are all totally automatic; there is something that starts it, and there is a human in that loop. But each of these people can answer that as well.

Admiral WILLARD. With regard to weapons, I would just remind everyone that it is a special functional area. It receives very particular oversight by Mr. Money. As well, we have a system where each of our mission-critical systems and the weapons that fall into that category have been or are being remediated and checked Y2K compliant. Overarching that is the systems integration testing by the Services and they are testing all of their weapons systems, and above that, are the CINC operational evaluations that are testing from sensor to shooter. So, these mission-critical systems are receiving not only the attention that they need to make them compliant in the first place, but are undergoing rigorous integration and warfighting testing, as well, in several ways. I would defer to the Services to speak to their individual weapons systems, but you can be assured that the weapons systems are getting all the attention they deserve.

Admiral JOHNSON. I want to emphasize that we have tried not to put any new processes in place to try and resolve this problem. We have used existing processes that have been proven over the years—our weapons systems safety processes, our safety of flight, our submarine safety programs, and the like. We know how to do systems integration and systems engineering. We have added Y2K aspects onto those, but our weapons systems are safe.

General AMBROSE. And I will add to what Admiral Johnson said that safety is an important part of our business, day in and day out. You can't use something to defend the Nation if you are destroying it yourself. So, we are very, very careful. Y2K is just one more thing we are very careful about.

Now, when it comes to testing, we test our systems when we are in the process of certifying them. But when we go into these operational evaluations, we will only test Y2K compliant systems. So, we won't be testing systems that we are not yet sure are absolutely safe. In addition, I am not personally aware of very many weapons that have date-sensitive functions in them. That doesn't mean there aren't any, but I am just not aware of very many.

Finally, in our testing to date, the Air Force has not encountered a catastrophic failure of any sort involving any weapons. So, our weapons are all safe.

Ms. BROWNING. The Army is in very good shape on its weapons systems. About 95 percent are already Y2K compliant. You need to know, too, that the Army has no nuclear weapons. That is just a fact. The Army started testing of its weapons systems and its divisional units back in the fall. Let me just give you a brief snapshot of some of those tests and what we found.

We did a lot of tests, as you know, at White Sands Missile Range. We did live fire tests. We tested our helicopters, our infrastructure, our command-and-control pieces. We found very few Y2K errors. The one or two we did find, they were easily fixable and we moved on.

We have also tested our first deployable forces of the 18 Airborne Corps at Fort Bragg. We did a number of communications tests back in the fall. They are part of our testing of our divisions and our corps units. Again, we found very few, if any, Y2K problems. We tested the 3rd Corps Field Artillery at Fort Sill, OK—that is an ongoing test—and the 10th Mountain Division in Fort Drum, NY, which will be deployed to Bosnia shortly. They have requested a full Y2K test.

I would also echo what General Ambrose has said. Many of our weapons systems do not process dates, so you can rest more comfortably with that. But the ones that do, we have tested them and we are very confident that they will work.

Colonel MCHALE. The Marine Corps is a shopper, not a developer, of weapons systems; 49 percent of our weapons systems are developed by the other services. The Army is the primary developer of our ground combat systems, and the Navy is the developer of our aviation systems. And we are tracking with them very closely on the status of their systems, and we take their compliant reports and ensure that the equipment is in fact certified, that we are using them and that we have incorporated them into our operational evaluations.

We have conducted two operational evaluations to date, one in December, and one just last month in Norway, that I mentioned earlier, and have found no failures in any of the systems that we are operating.

Mrs. MALONEY. Thank you.

Mr. HORN. Thank you. And I now yield 5 minutes to Mr. Ose, the gentleman from California.

Mr. OSE. Thank you, Mr. Chairman. I want to also share with you that I was with Mrs. Biggert when we visited South Comm, and thereafter on Chairman Mica's reprise of the Bataan death march for the rest of the trip. I am still tired.

I had a couple of questions, and I want to ask them in the context of, are there things that Congress needs to provide to make this happen, so that, come December 31, we have got it solved, this Y2K problem solved? If I understood the testimony today, the battle groups that we have out on deployment operating independently of any host-nation by virtue of being on international waters, they are OK. Am I correct on that? Go ahead.

Admiral JOHNSON. We never operate independently. We are always in a combined environment of Naval forces or a joint environment, because we are always communicating with our Air Force, Marine Corps, Army counterparts, as we do our operations and supply maritime support from the sea. To that respect, we do rely upon the shore infrastructure; we do rely upon the space infrastructure. In the Constellation battle group test, we actually carved out a separate communications node so that we could use our Reachback Comms in the year 2000 testing environment this last weekend and ongoing today.

So, to the extent that our forces are off the coast, and they are using their own capabilities for surface surveillance, undersea surveillance, air surveillance, and mission performance, yes, they are independent. Like every force in a coalition or joint environment, we are dependent upon the shore infrastructure and the other capabilities that might come to bear from either host nations or our joint commanders. And we are testing those in our operational evaluations.

Mr. OSE. Does our dependence on those joint operations impact us to the degree that we are not capable? I thought I heard the testimony today that said we are OK irrespective of those joint interactions.

Admiral WILLARD. There are a couple of things to consider. The battle groups themselves are being tested as an entity in the——

Mr. OSE. That is the question that I am trying to get to.

Admiral WILLARD. The answer is, yes, very rigorously. In fact, there is a sequence of five battle groups that will be tested, and the testing is very rigorous and extends throughout the battle group to ensure its Y2K compliance as an entity. In addition, the component Services are all captured in both their individual integration testing and unified command operations evaluations. So, those important interfaces between Services and between headquarters in the individual components' Services are all part of this examination.

Mr. MONEY. The comments you have may be related to—I don't know if I made it or Dr. Hamre—when we are in garrison, if you

will, in foreign countries, we are dependent on local power, and so forth. When we go to the field, we are self-sufficient.

Mr. OSE. It was Dr. Hamre——

Mr. MONEY. Yes.

Mr. OSE [continuing]. But I am most concerned about the deployed battle groups, not the ones that are in drydock, and not the ones spinning up for the next mission.

Admiral WILLARD. Sir, and again, I should defer to Admiral Johnson, but the entire Navy approach currently is to ensure that the integral battle group, to include the amphibious ready group component, is Y2K compliant as a whole, and they are actually being sequenced through their testing in accordance with their deployment dates, to ensure that we don't push a battle group across the millennium that has not been fully integration tested and captured in our operations evaluation process that is not Y2K compliant.

Admiral JOHNSON. Today, the Peleliu and the Constellation battle group are operating off the coast of southern California, and all the clocks on those ships read, now it is January 2, 2000.

Mr. OSE. To reference the test they are doing.

Admiral JOHNSON [continuing]. And they are flying sorties. They are conducting practice bombing runs. They are doing AAW. They are doing man overboard drills, everything that they would normally do as part of their battle group qualifications, because PAC Fleet is a force provider to the joint commanders, responsible that those forces, when provided, will be fully certified to do their warfighting mission in a year 2000 environment.

Mr. OSE. We have battle groups that are nuclear; we have battle groups that are non-nuclear. Are the battle groups that are nuclear, have the core reactors been tested?

Admiral JOHNSON. The Naval reactors, I won't speak for Admiral Bowman, except to say that the nuclear propulsion plants are year 2000 compliant.

Mr. OSE. Right. Mr. Chairman, I am not going to get to all of my questions, but I do appreciate your patience. That gets me to my second question.

On these operational evaluations for calendar year 1999, you have the various command locations, and this is somewhat frightening and I am actually understanding what the acronyms mean. Some of them have primary; some of them have backup. The one that does not have a backup is the transportation command down at the bottom. Does that affect our logistics ability and what are we doing about that?

Admiral WILLARD. In fact, Transportation Command—this may be a slight error. Every unified command operations evaluation must be backed up. So I would ask you to allow us to correct that slide and provide you the dates of their backup period. In fact, it was our requirement that, as they scheduled their operations evaluations, that they carve out an adequate period of time to handle further remediation and retesting, if required. So, it is mandatory that they have that available.

Mr. MONEY. That is exactly right. That period from, roughly, July 1st, through the end of the September, in fact, is being viewed as, if we don't, if something goes haywire the first time or two,

then there is where it will be tested yet again. So, I think the chart is wrong here.

Mr. OSE. All right, thank you. I have two more questions. My time is going to expire, Mr. Chairman——

Mr. HORN. No, it hasn't.

Mr. OSE [continuing]. So I will get to one.

Mr. HORN. It hasn't expired, and my rule is, if you can get the question out, they can take a half hour to answer it.

Mr. OSE. Holy smokes. Hold on. Fasten your seatbelts. [Laughter.]

Two questions. The first is having to do with the communication facilities for our forward-deployed units. I see we have on that same page a primary system, but no back up. And my second question is, with respect to Russia, I know that we talked about the command control systems that are in place there, but with respect to their perceived lack of civilian control in that country and the third-party organizations that might operate, they are dependent on computers. Does Y2K cause a problem in terms of, if you will, proliferation of nuclear weapons or development of nuclear weapons within countries that are now nuclear capable but who lack civilian control? That is two completely unrelated questions. I appreciate the chairman's dispensation on the communication.

Admiral WILLARD. Sir, I can handle the communication question that you asked. The functional areas are being handled a little bit differently than the unified command operations evaluations. These functional end-to-end tasks, their detailed planning and the tests are being executed by the agencies responsible for our DOD-wide or, in some cases, national networks. They don't fall under the same categorization as the commander in chief OPEVALs (Operational Evaluations). And as such, they are being handled differently.

You don't see backup periods against all of them because they are fairly extensive tests that occur within the timeframe that you see, but in some cases stop and go leverage off of CINC OPEVALs on occasion, even venture into the public domain.

And we have collaborative efforts ongoing, for example, in the public phone network, to check public switches with them. It is being spearheaded by Mr. Money and his agencies, but, again, it is being handled a little bit differently, and you don't see necessarily a backup date in there, but in fact there is adequate time to remediate and retest.

Mr. OSE. Do we end up with a dual or a backup system, a backup communication system for forward-deploying units?

Admiral WILLARD. We have numerous redundancies in our communication systems and command and control systems, for that matter, for deployments.

Mr. OSE. That are Y2K compliant?

Admiral WILLARD. Absolutely.

Mr. OSE. All right.

Mr. HORN. You want to ask a question?

Mr. MONEY. I was just going to add, by law, we have two tests for every one of these. So the charts are not showing you backup, but we will guarantee you there will be two tests for every one of

these systems as it goes through, whether it is an OPEVAL or a functional end-to-end test, or, in some cases, it is duplicated.

Mr. OSE. Mr. Chairman, in the interest of time, I will yield back, if I could submit in writing my other question for response.

Mr. HORN. Without objection, the questions and answers will be put in at this part of the record.

[The information referred to follows:]

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

April 15, 1999

Honorable Stephen Horn
Chairman
Subcommittee on Government Management,
Information, and Technology
Committee on Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Mr. Chairman:

This is in response to your March 16, 1999 letter to the Secretary of Defense requesting written responses to additional questions from the March 2, 1999, joint hearing. We have provided additional information amplifying Deputy Secretary of Defense Hamre's prepared statement and oral testimony in the areas covered by the additional questions.

We appreciate this opportunity to share with you our progress toward validating our national security capabilities and the readiness of our forces in relation to the Year 2000.

Sincerely,

Arthur L. Money
Senior Civilian Official

Enclosure

Questions for the Record

From the Joint Hearing of the

Subcommittee on Government Management, Information, and Technology

and

Subcommittee on Technology

Committee on Government Reform

United States House of Representatives

Tuesday, March 2, 1999

Year 2000 Preparedness

Questions for the Record from the Joint Hearing of the Subcommittee on Government Management, Information, and Technology and Subcommittee on Technology, Committee on Government Reform, United States House of Representatives, Tuesday, March 2, 1999

Table of Contents

1. Systems Not Tested in Operational Evaluation.

Please provide a list of all currently noncompliant systems that will not be tested in an operational evaluation.

Attached at Appendix 1 is a list of systems that are noncompliant as of March 31, 1999. The list indicates which of these systems are scheduled to be evaluated in either an Operational Evaluation by a Unified Command, an End-to-End evaluation conducted by one of the Principal Staff Assistants who are responsible for the "business functions" of the Department of Defense, or in Military Department Integration Testing.

As of March 25, 1999, the Department of Defense had 164 systems not scheduled to be compliant on March 31, 1999. Of these 164 systems, 37 were scheduled to be evaluated by either Operational or End-to-End evaluation or Integration Testing. Of these 37 systems, 3 were scheduled for Operational Evaluations.

2. Systems Tested by Functional Test.

Please provide a list of all currently noncompliant systems (by functional unit) that will be tested only by a functional test.

Attached at Appendix 2 is a list of systems that are noncompliant as of March 31, 1999, sorted by primary function. The list indicates which of these systems are scheduled to be evaluated in either an Operational Evaluation by a Unified Command, an End-to-End evaluation conducted by one of the Principal Staff Assistants who are responsible for the "business functions" of the Department of Defense, or in Military Department Integration Testing.

As of March 25, 1999, the Department of Defense had 164 systems not scheduled to be compliant on March 31, 1999. Of these 164 systems, 37 were scheduled to be evaluated by either Operational or End-to-End evaluation or Integration Testing. Of these 37 systems, 18 were scheduled for End-to-End evaluation by a functional proponent.

3. Status of Intelligence Systems.

Please provide a detailed explanation of the status of the intelligence community's computer systems. Please identify intelligence systems that are currently noncompliant, and the estimated date they will be compliant. If this information is classified, please tell us how we might obtain this information.

The detailed listing of intelligence systems with completion dates is classified and will be forwarded under separate cover.

4. Weapons Technology Proliferation.

You stated that Year 2000 readiness in Russia is a concern. Could Year 2000 disruptions in Russia result in the leakage of classified weapons technology, which could lead to nuclear proliferation?

The Department of Defense (DoD) engagements with the Russian Ministry of Defense (MOD) are in the preliminary stages and to date efforts have focused primarily on management techniques and commercial solutions. The current emphasis is to assist the MOD in effectively assessing the YEAR 2000 problem, making sound resource decisions, determining which resources to dispose of, and the establishment of organization standards that continually address critical YEAR 2000 issues. The application of competent management techniques and solutions is important to the reduction in the risks of proliferation. One area of concern to the U.S. is the impact of Y2K in the area of nuclear stockpile security, specifically the security of nuclear materials. The DoD, through its Cooperative Threat Reduction (CTR) Program, currently provides assistance to the MOD to improve the management of nuclear weapons stockpiles at storage sites throughout Russia. One of the primary goals of this increased effort is the continuous safe and secure storage, transport, and accounting of these Weapons of Mass Destruction, especially during the Year 2000 transition. DoD will continue the YEAR 2000 dialog with Russia throughout the remainder of this year.

5. Overseas Installations.

U.S. troops stationed abroad rely on the infrastructures such as power and water of foreign countries for numerous services. Is the military taking precautions to ensure that U.S. troops stationed abroad will be safe and that military bases will be fully operational in the event that foreign infrastructures fail?

As noted in the prepared statement, DoD has over 600 installations around the world and in the United States. Each of these installations is being tracked for YEAR 2000 compliance, and information is available in our DoD YEAR 2000 database. Each installation is, in essence, a small city with utility, services, and infrastructure issues similar to a metropolitan area. Consequently, each installation has a different situation with regard to water supply, electrical power, emergency services, support equipment, etc. Each installation commander is tracking the YEAR 2000 compliance of the supporting utilities. In addition, the Defense Logistics Agency (DLA) and the OSD staff are working these issues through the President's Council on YEAR 2000 Conversion.

Some of the initiatives include establishing liaison with foreign governments, state governments, and NATO. DLA is the DoD energy outreach representative for these issues on the President's Council. Their efforts oversee the availability of energy supplies for installations both stateside and overseas. DLA works closely with the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Council (NERC). As also indicated in the prepared statement, we are working outreach to states via the National Guard Bureau as well as addressing the issues of support to local areas by DoD Table Top Exercises, Chairman's Contingency Assessments, and Consequence Management Planning.

Within DoD, installations currently have emergency contingency plans in place. As part of their YEAR 2000 compliance work, these plans are being reviewed to ensure that the base-level mission can be supported under YEAR 2000 difficulties. The Services and DLA have established an installation YEAR 2000 focus within their CIO and functional organizations. They are working through established military chains-of-command to enable the installations to produce water, waste water, energy, safety, and security products and services at base-level.

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	*System No*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Army	DA00097	MIRS	MEPCOM Integrated Resource System	15-Apr-99		31-May-99	E2E
Army	DA00108	SIDPERS-ARNG	Standard Installation/Division Personnel System - Army National Guard	14-May-99		28-May-99	E2E
Army	DA00113	WPS	Worldwide Port System	15-Oct-98		28-May-99	E2E
Army	DA00172	SIDPERS-3	Standard Installation/Division Personnel System - 3	21-Jan-99		15-Oct-99	E2E
Army	DA00212	SAAS-MOD	Standard Army Ammunition System-Modernization	5-Mar-99		2-Jul-99	E2E
Army	DA00483	ULLS-G	Unit Level Logistics System - Ground	19-Mar-99		24-Jun-99	E2E
Army	DA00484	ULLS-A	Unit Level Logistics System - Aviation	18-May-99		15-Jun-99	E2E
Army	DA00486	SARSS-1(0)	Standard Army Retail Supply System Level 1 Objective	5-Mar-99		4-Jun-99	E2E
Army	DA00487	SARSS-2AD	Standard Army Retail Supply System - 2AD	5-Mar-99		4-Jun-99	E2E
Army	DA00488	SARSS-2AC/2B	Standard Army Retail Supply System-Level 2A Corps/Level 2B	5-Mar-99		4-Jun-99	E2E
Army	DA00720	JCMT	Joint Collection Management Tools	9-Dec-98		1-Oct-99	
Army	DA00728	DTSS	Digital Topographic Support System	30-Nov-98		16-Jul-99	
Army	DA00730	M1A2	Abrams M1A2 Tank System	1-Mar-99		1-Oct-99	
Army	DA00802	SAMS-1&2 Rehost	Standard Army Maintenance System - 1 & 2 Rehost (TACCS Replacement)	31-Mar-99		30-Sep-99	
Army	DA00827	ASCRC	Automated System Crime Records Center	31-Mar-99		30-Jun-99	
Army	DA00956	JACON	JACADS Control Code	31-Aug-99		31-Aug-99	
Army	DA00957	JAPDAR	JACADS Process Data Acquisition Reporting	31-Aug-99		31-Aug-99	
Army	DA00958	TOPDAR	TOCDF Process Data Acquisition and Recording	31-Mar-99		30-Apr-99	
Army	DA01070	CGS: AN/TSQ-179(V)1	JSTARS Common Ground Station (CGS)	23-Dec-98		31-Jul-99	
Army	DA01074	TOCON	TOCDF Control System	31-Aug-99		31-Aug-99	
Army	DA01260	MIES	Modernized Imagery Exploitation System	31-Dec-98		30-Jun-99	
Army	DA01308	RISER	Resource Information System, Engineer, Reserve	30-Mar-99		15-Apr-99	
Army	DA01421	ARL-C AN/ASQ-216	Airborne Reconnaissance Low - COMINT	31-Jul-99		31-Jul-99	IT
Army	DA01423	ARL-M AN/ASQ-223	Airborne Reconnaissance Low - Multifunction	15-Mar-99		31-May-99	
Army	DA01824	Keystone- Request - CS	Keystone-Request Client Server	11-May-99		11-May-99	E2E
Army	DA02139	RLAS	RSC Level Application Software	1-Apr-99		1-Apr-99	

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	System No	Acronym	System Name	Validation ECD	Validation ACD	Completion Date	Evaluation Plan
Army	DA02163	RCAS RPAM	Retirement Point Accounting Management	31-Jul-99		31-Jul-99	
Army	DA02186	GCCS-A D1	Global Command and Control System - Army	31-Oct-98		12-Apr-99	
Army	DA02187	GCCS-A D2	Global Command and Control System - Army	18-Dec-98		5-May-99	
Army	DA02206	E-TRACKWOLF	Enhanced TRACKWOLF (SEC)	3-Jun-99		31-Aug-99	
Army	DA02221	ACUS ATM	Area Common User System - Asynchronous Transfer Mode	30-Jun-99		30-Jun-99	IT
Army	DA02232	SSS	Single Shelter Switch	31-Aug-99		31-Aug-99	
Army	DA02286	MANPOWER-Voucher Redesign	Manpower Voucher Redesign	30-Jun-99		30-Jun-99	
Army	DA02445	ARMY SWITCH	Army Switch Program	31-Dec-98		30-Sep-99	IT
Army	DA02707	SYSTEM 2	PMCISS SYSTEM 2	29-Dec-98		30-Jun-99	
Navy	2781	TAMPS	Tactical Automated Mission Planning System		18-Dec-98	30-Sep-99	IT
Navy	5492	NECC	NAVY EHF Communications Controller		29-Oct-98	2-Jul-99	
Navy	5496	EHF LDR	EHF Low Data Rate Terminal -AN/USC-38(V)		12/23/1998	16-Jul-99	IT
Navy	5499	TACINTEL II+	Tactical Intel Info Exchange System II		18-Mar-99	1-Jul-99	IT
Navy	5502	TRE (EDM)	Tactical Receive Equipment (Engineering Design Model)		29-Oct-98	30-Apr-99	
Navy	5506	CDF AN/SRS-1	Combat Direction Finding AN/SRS-1		1-Dec-98	30-Jun-99	
Navy	5507	COBLU PHASE 0	Cooperative Outboard Base Line Update Phase 0		29-Dec-98	31-Jul-99	IT
Navy	5513	OBU/OED	Ocean Surveillance Information System (OSIS) Baseline Upgrade/OSIS Evolutionary Development		10-Dec-98	15-Jun-99	
Navy	5523	SURTASS (Passive)	Surveillance Towed Array Sensor System		29-Oct-98	25-Apr-99	
Navy	5525	METMF(R)	Meteorological Mobile Facility (Replacement)		11-Feb-99	30-Apr-99	
Navy	5530	BBS-IRM	Baseband Switch Integrated Resource Manager		29-Oct-98	2-Jul-99	IT
Navy	5535	ISABPS	Integrated Submarine Automated Broadcast Processing System - Ashore		29-Oct-98	15-Apr-99	
Navy	5541	NKMS	Navy Key Management System		29-Oct-98	30-Jun-99	
Navy	5547	GATEGUARD	GATEGUARD		29-Oct-98	21-May-99	
Navy	5554	NAVMACS II	Naval Automated Modular Communications System Afloat Component AN/SYQ-7A(V) AN/SYQ-7B(V)		29-Oct-98	31-Jul-99	IT
Navy	5557	SNAP I (UNIX Port)	Ported SNAP I Shipboard Non-Tactical ADP Program	31-Mar-99		30-Jun-99	E2E
Navy	5558	NALCOMIS IMA	NALCOMIS IMA	31-Mar-99		30-Jun-99	IT
Navy	5559	NALCOMIS OMA	NALCOMIS OMA	31-Mar-99		30-Jun-99	
Navy	5567	AV3M	Aviation Maintenance Material Management	31-Mar-99		30-Jun-99	

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	*System No*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Navy	5568	SNAP-SAMS	SNAP Automated Medical System		23-Dec-98	31-May-99	IT
Navy	5587	SURTASS- LFA	SURTASS- LFA Low Frequency Active		29-Oct-98	25-Apr-99	
Navy	5592	IVTT	Integrated VERDIN Transmit Terminal		29-Oct-98	15-Apr-99	
Navy	5595	MOMMS	Micro Organizational Maintenance Management System		28-Dec-98	31-May-99	
Navy	5599	NTCSS-DANA	NTCSS-DANA Desk Top Environment			30-Jun-99	
Navy	5616	CDF AN/SRS-1A	Combat Direction Finding AN/SRS-1A		28-Jan-99	31-May-99	
Navy	5634	ADNS	Automated Digital Network System		9-Nov-98	31-Jul-99	IT
Navy	5642	SMQ-11	AN/SMQ-11, Receiver Recorder Set, Meteorological Data		29-Oct-98	30-Jun-99	IT
Navy	5649	TESS NC Transition	Tactical Environmental Support System- Transition		29-Oct-98	30-Jun-99	
Navy	5651	GCCS-M AFLOAT	Global Command and Control System Maritime - Afloat Naval TAC CMD System - Afloat		29-Oct-98	30-Sep-99	IT
Navy	5652	SNAP II (UNIX PORT)	Ported SNAP II Shipboard Non-Tactical ADP Program	31-Mar-99		30-Jun-99	E2E
Navy	6505	Auto ID	Automatic Identification System		26-Feb-99	30-Jun-99	
Navy	7310	IMAPMIS	Inactive Manpower and Personnel Management Information System	13-Aug-99		3-Sep-99	E2E
Navy	7449	ATWCS TCGR	Advanced TOMAHAWK Weapon Control System Track Control Group Replacement		15-Dec-98	30-Jun-99	
Navy	7451	TMPC	TOMAHAWK Land Attack Mission Planning Center		22-Dec-98	10-Apr-99	
Navy	7452	APS	Afloat Planning System		22-Dec-98	31-Aug-99	
Navy	7453	JSIPS-N	Joint Service Imagery Processing System- Navy		27-Jan-99	31-Aug-99	
Navy	7922	EA-6B TEAMS	EA-6B TSQ-142 (V5/6) TEAMS Software Release 205.04	1-Apr-99		1-Oct-99	
Navy	7932	CSRFS	Common Source Routing File System	15-Apr-99		30-Apr-99	
Navy	8035	OIS	Oceanographic Information System		24-Nov-98	30-Apr-99	
Navy	8120	TFMMS	Total Force Manpower Management System	21-Jun-99		25-Jun-99	
Navy	8330	RESFMS	Reserve Financial Management System		4-Mar-99	19-Apr-99	E2E
Navy	8430	AN/BSY-2	AN/BSY-2 Submarine Combat System		2-Dec-98	30-Jun-99	IT
Navy	8520	CCS REV 5.5	CCS REV 5.5		16-Sep-98	31-Aug-99	
Navy	8522	CCS REV 6.3	CCS Rev 6.3		16-Sep-98	30-Apr-99	
Navy	8528	CEC - BASELINE 2	Cooperative Engagement Capability Baseline 2		6-Feb-99	30-Aug-99	
Navy	8918	ROLMS	Retail Ordnance Logistics Management System			30-Sep-99	E2E
Navy	10176	MPTM&AS	MPT Management & Administration System	11-Jun-99		14-Jun-99	

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	*System No*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Navy	10225	BSS	BUPERS Support System	21-Apr-99		26-Apr-99	
Navy	10332	NMPDS	Navy Military Personnel Distribution System	6-Aug-99		11-Aug-99	
Navy	10632	NMPS	NAVSPACECOM Mission Processing System (NMPS)	23-Aug-99		30-Aug-99	
Navy	10642	ISCS	Integrated Satellite Control System	26-May-99		30-Jun-99	
Navy	10646	NAEDSS	Navy EHF SATCOM Program (NESP) Adaptation and Ephemeris Data Support System	9-Apr-99		9-Apr-99	
Navy	**11260**	**SDS**	**Pay and Personnel Source Data System**		**12-Mar-99**	**21-May-99**	**E2E**
Navy	11403	ACDS BLK 1	Advance Combat Direction System BLK 1 (LHD 1, CV 67 and CVN 69 only)		12-Mar-99	30-Apr-99	
Navy	11638	ATWCS US SUB	Advanced Tomahawk Weapon Control System for US Sub		15-Dec-98	31-Aug-99	
Navy	**12765**	**ACDS BLK 0**	**Advanced Combat Direction System Blk 0 (LHA 2 & 4 only)**	**11-Jun-99**		**30-Jul-99**	**IT**
USMC	5721	IAS, MEF	Intelligence Analysis System, Marine Expeditionary Force	15-May-99		30-Jun-99	
USMC	5802	TRSS	Tactical Remote Sensor System (USMC)		19-Feb-99	30-Apr-99	
USMC	11624	AN/MSC-63A	Communications Central (A0258)		4-Jan-99	30-Aug-99	
USMC	11627	AN/PYQ-1	Digital Terrain Analysis Mapping System (AO504)	1-Apr-99		30-Sep-99	
USAF	2000054	CAMPS	Consolidated Air Mobility Planning System		12-Feb-99	9-Apr-99	
USAF	31001729	FARR	FAA/AF Radar Replacement, ARSR-4		29-Oct-98	1-Jun-99	
USAF	31002095	JSTARS	Joint Surveillance Target Attack Radar System		23-Nov-98	28-Jun-99	
USAF	31002615	PAVE PAWS	PAVE PAWS Phased Array Radar	31-May-99		31-May-99	
USAF	**99001626**	**GATES**	**Global Air Transportation Execution System**	**30-Apr-99**		**30-Jun-99**	**E2E**
USAF	99004534	F-117A MPS	F-117A Mission Planning System		29-Dec-98	30-Sep-99	
USAF	99004762	GMP	GEODSS Modernization Program	31-May-99		31-May-99	
USAF	99008003	BMEWS III	Ballistic Missile Early Warning System III	30-Apr-99		30-Apr-99	
USAF	99008020	VCS - NEW	Voice Callsign System - New	1-Apr-99		1-Apr-99	
USAF	99008031	B-1B A/W/E	B-1B Mission Planning		8-Mar-99	14-May-99	
USAF	99008155	TBMCS V1.0	Theater Battle Management Core System	19-Apr-99		30-Sep-99	
USAF	99008282	F-15 EAGLE	F-15 EAGLE Mission Planning Interfaces	31-Mar-99		8-Jul-99	
USAF	99008286	F-16 MSN PLAN	F-16 Falcon - Mission Planning Environment	28-May-99		28-May-99	
USAF	AS002838	SBIRS - High Ground	Space Based Infra-Red High Ground Component	13-Apr-99		1-Oct-99	
USAF	AS003521	GPS	GPS Space Segment	1-Apr-99		30-Apr-99	
USAF	AS004312	MCCC STRAT	Mobile Command and Control Center Strategic Command	30-Apr-99		30-Apr-99	

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	*System No*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
USAF	AS006505	KC-135 AFMSS A/W/E	KC-135 Air Force Mission Support System A/W/E		19-Feb-99	11-Jun-99	
USAF	AS006845	AWACS US 20/25	Airborne Warning and Control System 20/25 – US		9-Feb-99	30-Sep-99	
PACOM	1	C2S2	Command and Control Support System LAN		9-Nov-98	31-Aug-99	OE
PACOM	16	USFJ LAN	HQ LAN	8-Jul-99		8-Jul-99	
SOCOM	44	SMRS	Special Mission Radio System	31-Oct-99		31-Oct-99	
SOCOM	46	SOCA	Special Operations Communications Assemblage	31-Mar-99		30-Apr-99	
SOCOM	166		Privateer	30-Oct-99		31-Dec-99	
SOUTHCOM	South-002	TACCMS	Tactical Command and Management System		1-Feb-99	30-Jul-99	
SOUTHCOM	South-003	CNCMS	Counternarcotics Command and Management System		1-Feb-99	30-Apr-99	OE
SPACECOM	M157-5	SMPAS	Space Mission Payload Assessment System	15-Apr-99		15-Apr-99	OE
BMDO	BMDO-10	PAC-3	Patriot PAC-3	20-Mar-99		1-Jan-01	
BMDO	BMDO-6	AWS Baseline 6 Phase 3 AEGIS	AEGIS Program, AWS Baseline 6 Phase 3, TBMD	15-Mar-99		1-Jan-03	
BMDO	BMDO-7	SM-2 Block IV/IVA	Standard Missile Program, SM-2 Block IV/IVA, Area TBMD		10-Feb-99	1-Jan-01	
BMDO	BMDO-8	SM-3 (LEAP)	Standard Missile Program, SM-3 (LEAP), Theater TBMD		10-Feb-99	1-Jan-05	
DLA	DLA0012	BOSS	Base Operations Support System		15-Jan-99	31-May-99	
DLA	DLA0054	DFAMS	Def Fuels Auto Mgmt Sys (also FAS & AVEDS)	31-May-99		31-May-99	
DTRA	1	CMTS	Compliance Monitoring Tracking System	1-Apr-99		30-Apr-99	
DeCA	9	COUPONS	DeCA Automatic Coupons System	16-Apr-99		30-Apr-99	
DeCA	19	DIBS 2000	DeCA Interim Business System	31-Mar-99		31-Oct-99	
DeCA	40	POS-M	Point of Sale Modernization	31-Mar-99		31-Jul-99	
DeCA	44	SAVES	Standard Automated Voucher Examination System	3-May-99		25-May-99	
DFAS	AR6161	SIFS	Standard Industrial Fund System		27-Jan-99	30-May-99	
DFAS	AR7208	SOMARDS	Standard Operations and Maintenance, Army R&D System	15-Mar-99		31-May-99	
DFAS	DE2107	DJMS-AC	Defense Joint Military Pay System - Active Component		26-Feb-99	30-Apr-99	
DFAS	IN3511	DTRS	Defense Transportation Pay System	5-Mar-99		5-Apr-99	
DFAS	IN4115	SRD I	Standard Finance System Redesign (Subsystem I)-	30-May-99		30-May-99	
DFAS	IN6266	STARFIARS-MOD	Standard Army Financial Inventory Accounting and Reporting System - Modernization	30-Mar-99		30-May-99	
DFAS	IN7207	STANFINS	Standard Finance System	30-May-99		30-May-99	
DFAS	IN7851	HQARS	Headquarters Accounting And Reporting System	15-Mar-99		5-Apr-99	

Appendix 1 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plans by Component

Component	*System No*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
DISA	D205	DISN-DVS-G	DISN - Video Services – Global			30-Apr-99	
DISA	D326	DSN	Defense Switched Network			30-Sep-99	
DISA	D334	SPECTRUM XXI	SPECTRUM XXI			30-Sep-99	
DISA	D635	ADNET	Anti-Drug Network	30-Nov-98		30-Jun-99	
DISA	D646	NCCS-AMH	National C2 System - Automated Message Handler	1-Mar-99		30-Jun-99	
DISA	WE01	DMC	Defense Megacenters Including all 434 Domains	31-Jan-99		30-Nov-99	
AFIS	AFRTS01	AFRTS-BC TV Auto	AFRTS-Broadcast Center TV Automation System			1-Aug-99	
AFIS	AFRTS02	AFRTS-BC TV CMP	AFRTS-Broadcast Center TV Compression System			1-Aug-99	
AFIS	AFRTS03	AFRTS-BC RAS	AFRTS-Broadcast Center Radio Automation System			1-Aug-99	
WHS	99004653	DITS	Directives Issuance Tracking System	9-Apr-99		23-Apr-99	
WHS	99005137	AFTS	Adjudication Facility Tracking System	1-Jun-99		1-Jun-99	
OUSD (All)	99001531	FDS	Foreign Disclosure System	31-Mar-99		14-May-99	
OUSD (All)	99001532	TPS	Technology Protection System	31-Mar-99		14-May-99	
OUSD (All)	99001533	FVS	Foreign Visits System	31-Mar-99		14-May-99	
OUSD (All)	99001534	USVISITS	U.S. Visitor International Technology System	31-Mar-99		14-May-99	
OUSD (All)	99001535	NDPS	National Disclosure Policy System			14-May-99	
OUSD (All)	99001536	SDSS	Security Policy Automation Network Decision Support System	31-Mar-99		14-May-99	
OUSD (All)	99005522	PIMS	Policy Intranet Management System	31-Mar-99		14-May-99	
OUSD (All)	99005716	HAOA	Health Affairs Office Automation			1-May-99	
OUSD (All)	99005725	LRSTS	Legislative Reference Service Tracking System	30-Jun-99		31-Aug-99	
OUSD (All)	99005729	DOTEAS/U	DOT&E Unclassified Office Automation System	1-May-99		1-Jun-99	
OUSD (All)	99005730	DOTEOA/C	DOT&E Office Automation Classified System	1-May-99		1-Jun-99	
OUSD (All)	99006018	PTS	Personnel Tracking System	31-Jul-99		30-Sep-99	
OUSD (All)	99006210	SPAN	Security Policy Automation Network	31-Mar-99		14-May-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Command and Control	Army	DTSS	Digital Topographic Support System		30-Nov-98	16-Jul-99	
Command and Control	Army	GCCS-A D2	Global Command and Control System - Army		18-Dec-98	5-May-99	
Command and Control	Army	GCCS-A D1	Global Command and Control System - Army		31-Oct-98	12-Apr-99	
Command and Control	**Navy**	**GCCS-M AFLOAT**	**Global Command and Control System Maritime - Afloat Naval TAC CMD System-Afloat**	**1-Dec-98**	**29-Oct-98**	**30-Sep-99**	**IT**
Command and Control	USAF	AWACS US 20/25	Airborne Warning and Control System 20/25 -- US	10-Mar-99	9-Feb-99	30-Sep-99	
Command and Control	USAF	BMEWS III	Ballistic Missile Early Warning System III		30-Apr-99	30-Apr-99	
Command and Control	USAF	CAMPS	Consolidated Air Mobility Planning System	26-Feb-99	12-Feb-99	9-Apr-99	
Command and Control	USAF	FARR	FAA/AF Radar Replacement, ARSR-4	22-Aug-98	29-Oct-98	1-Jun-99	
Command and Control	USAF	GMP	GEODSS Modernization Program		31-May-99	31-May-99	
Command and Control	USAF	JSTARS	Joint Surveillance Target Attack Radar System	16-Dec-98	23-Nov-98	28-Jun-99	
Command and Control	USAF	MCCC STRAT	Mobile Command and Control Center Strategic Command		30-Apr-99	30-Apr-99	
Command and Control	USAF	PAVE PAWS	PAVE PAWS Phased Array Radar		31-May-99	31-May-99	
Command and Control	USAF	TBMCS V1.0	Theater Battle Management Core System		19-Apr-99	30-Sep-99	
Command and Control	USAF	VCS - NEW	Voice Callsign System - New		1-Apr-99	1-Apr-99	
Command and Control	**SOUTHCOM**	**CNCMS**	**Counternarcotics Command and Management System**	**15-Jan-99**	**1-Feb-99**	**30-Apr-99**	**OE**
Command and Control	SOUTHCOM	TACCMS	Tactical Command and Management System	31-Jan-99	1-Feb-99	30-Jul-99	
Command and Control	DTRA	CMTS	Compliance Monitoring Tracking System		1-Apr-99	30-Apr-99	
Command and	DISA	ADNET	Anti-Drug Network		30-Nov-98	30-Jun-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Control							
Command and Control	DISA	NCCS-AMH	National C2 System - Automated Message Handler		1-Mar-99	30-Jun-99	
Communications	Army	ACUS ATM	Area Common User System - Asynchronous Transfer Mode		30-Jun-99	30-Jun-99	IT
Communications	Army	ARMY SWITCH	Army Switch Program		31-Dec-98	30-Sep-99	IT
Communications	Army	SSS	Single Shelter Switch		31-Aug-99	31-Aug-99	
Communications	Navy	ADNS	Automated Digital Network System	9-Nov-98	9-Nov-98	31-Jul-99	IT
Communications	Navy	BBS-IRM	Baseband Switch Integrated Resource Manager	31-Oct-98	29-Oct-98	2-Jul-99	IT
Communications	Navy	EHF LDR	EHF Low Data Rate Terminal -AN/USC-38(V)	31-Dec-98	23-Dec-98	16-Jul-99	IT
Communications	Navy	NAVMACS II	Naval Automated Modular Communications System Afloat Component AN/SYQ-7A(V) AN/SYQ-7B(V)	2-Nov-98	29-Oct-98	31-Jul-99	IT
Communications	Navy	TACINTEL II+	Tactical Intel Info Exchange System II	19-Mar-99	18-Mar-99	1-Jul-99	IT
Communications	Navy	Auto ID	Automatic Identification System	31-Mar-99	26-Feb-99	30-Jun-99	
Communications	Navy	CSRFS	Common Source Routing File System		15-Apr-99	30-Apr-99	
Communications	Navy	GATEGUARD	GATEGUARD	2-Nov-98	29-Oct-98	21-May-99	
Communications	Navy	ISABPS	Integrated Submarine Automated Broadcast Processing System - Ashore	31-Oct-98	29-Oct-98	15-Apr-99	
Communications	Navy	IVTT	Integrated Verdin Transmit Terminal	31-Oct-98	29-Oct-98	15-Apr-99	
Communications	Navy	NECC	NAVY EHF Communications Controller	31-Oct-98	29-Oct-98	2-Jul-99	
Communications	Navy	NKMS	Navy Key Management System	30-Oct-98	29-Oct-98	30-Jun-99	
Communications	Navy	TRE (EDM)	Tactical Receive Equipment (Engineering Design Model)	1-Mar-98	29-Oct-98	30-Apr-99	
Communications	USMC	AN/MSC-63A	Communications Central (A0258)	1-Feb-99	4-Jan-99	30-Aug-99	
Communications	PACOM	C2S2	Command and Control Support System LAN	9-Nov-98	9-Nov-98	31-Aug-99	OE
Communications	PACOM	USFJ LAN	HQ LAN		8-Jul-99	8-Jul-99	
Communications	SOCOM	SMRS	Special Mission Radio System		31-Oct-99	31-Oct-99	
Communications	SOCOM	SOCA	Special Operations Communications Assemblage		31-Mar-99	30-Apr-99	
Communications	DISA	DSN	Defense Switched Network			30-Sep-99	
Communications	DISA	DISN-DVS-G	DISN - Video Services - Global			30-Apr-99	
Communications	DISA	SPECTRUM XXI	SPECTRUM XXI			30-Sep-99	
Environmental Security	DLA	BOSS	Base Operations Support System	15-Jan-99	15-Jan-99	31-May-99	
Finance	DeCA	COUPONS	DeCA Automatic Coupons System		16-Apr-99	30-Apr-99	
Finance	DeCA	DIBS 2000	DeCA Interim Business System		31-Mar-99	31-Oct-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Finance	DeCA	POS-M	Point of Sale Modernization		31-Mar-99	31-Jul-99	
Finance	DeCA	SAVES	Standard Automated Voucher Examination System		3-May-99	25-May-99	
Finance	DFAS	DJMS-AC	Defense Joint Military Pay System - Active Component	12-Feb-99	26-Feb-99	30-Apr-99	
Finance	DFAS	DTRS	Defense Transportation Pay System		5-Mar-99	5-Apr-99	
Finance	DFAS	HQARS	Headquarters Accounting and Reporting System		15-Mar-99	5-Apr-99	
Finance	DFAS	STARFIARS-MOD	Standard Army Financial Inventory Accounting and Reporting System - Modernization		30-Mar-99	30-May-99	
Finance	DFAS	STANFINS	Standard Finance System		30-May-99	30-May-99	
Finance	DFAS	SRD I	Standard Finance System - Redesign (Subsystem I)		30-May-99	30-May-99	
Finance	DFAS	SIFS	Standard Industrial Fund System	15-Feb-99	27-Jan-99	30-May-99	
Finance	DFAS	SOMARDS	Standard Operations and Maintenance, Army R&D System		15-Mar-99	31-May-99	
Health	**Navy**	**SNAP-SAMS**	**SNAP Automated Medical System**	**30-Dec-98**	**23-Dec-98**	**31-May-99**	**IT**
Human Resources	WHS	AFTS	Adjudication Facility Tracking System		1-Jun-99	1-Jun-99	
Human Resources	OUSD	PTS	Personnel Tracking System		31-Jul-99	30-Sep-99	
Information Management	OUSD	DOTEAS/U	DOT&E Unclassified Office Automation System		1-May-99	1-Jun-99	
Information Management	Navy	NAEDSS	Navy EHF SATCOM Program (NESP) Adaptation and Ephemeris Data Support System		9-Apr-99	9-Apr-99	
Information Management	DISA	DMC	Defense Megacenters Including all 434 Domains		31-Jan-99	30-Nov-99	
Information Management	AFIS	AFRTS-BC RAS	AFRTS-Broadcast Center Radio Automation System			1-Aug-99	
Information Management	AFIS	AFRTS-BC TV AUTO	AFRTS-Broadcast Center TV Automation System			1-Aug-99	
Information Management	AFIS	AFRTS-BC TV CMP	AFRTS-Broadcast Center TV Compression System			1-Aug-99	
Information Management	WHS	DITS	Directives Issuance Tracking System		9-Apr-99	23-Apr-99	
Information Management	OUSD	DOTEOA/C	DOT&E Office Automation Classified System		1-May-99	1-Jun-99	
Information Management	OUSD	FDS	Foreign Disclosure System		31-Mar-99	14-May-99	
Information Management	OUSD	FVS	Foreign Visits System		31-Mar-99	14-May-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Information Management	OUSD	HAOA	Health Affairs Office Automation			1-May-99	
Information Management	OUSD	LRSTS	Legislative Reference Service Tracking System		30-Jun-99	31-Aug-99	
Information Management	OUSD	NDPS	National Disclosure Policy System			14-May-99	
Information Management	OUSD	PIMS	Policy IntraNet Management System		31-Mar-99	14-May-99	
Information Management	OUSD	SPAN	Security Policy Automation Network		31-Mar-99	14-May-99	
Information Management	OUSD	SDSS	Security Policy Automation Network Decision Support System		31-Mar-99	14-May-99	
Information Management	OUSD	TPS	Technology Protection System		31-Mar-99	14-May-99	
Information Management	OUSD	USVISITS	U.S. Visitor International Technology System		31-Mar-99	14-May-99	
Inspector General	Army	ASCRC	Automated System Crime Records Center		31-Mar-99	30-Jun-99	
Intelligence	**Army**	**ARL-C AN/ASQ-216**	**Airborne Reconnaissance Low - COMINT**		**31-Jul-99**	**31-Jul-99**	**IT**
Intelligence	Army	ARL-M AN/ASQ-223	Airborne Reconnaissance Low - Multifunction		15-Mar-99	31-May-99	
Intelligence	Army	E-TRACKWOLF	Enhanced Trackwolf (SEC)		3-Jun-99	31-Aug-99	
Intelligence	Army	JCMT	Joint Collection Management Tools		9-Dec-98	1-Oct-99	
Intelligence	Army	CGS: AN/TSQ-179(V)1	JSTARS Common Ground Station (CGS)		23-Dec-98	31-Jul-99	
Intelligence	Army	MIES	Modernized Imagery Exploitation System		31-Dec-98	30-Jun-99	
Intelligence	**Navy**	**COBLU PHASE 0**	**Cooperative Outboard Base Line Update Phase 0**	**31-Dec-98**	**29-Dec-98**	**31-Jul-99**	**IT**
Intelligence	Navy	CDF AN/SRS-1	Combat Direction Finding AN/SRS-1	1-Dec-98	1-Dec-98	30-Jun-99	
Intelligence	Navy	CDF AN/SRS-1A	Combat Direction Finding AN/SRS-1A	31-Jan-99	28-Jan-99	31-May-99	
Intelligence	Navy	OBU/OED	Ocean Surveillance Information System (OSIS) Baseline Upgrade/OSIS Evolutionary Development	16-Dec-98	10-Dec-98	15-Jun-99	
Intelligence	Navy	SURTASS- LFA	SURTASS- LFA Low Frequency Active	30-Oct-98	29-Oct-98	25-Apr-99	
Intelligence	Navy	SURTASS (Passive)	Surveillance Towed Array Sensor System	30-Oct-98	29-Oct-98	25-Apr-99	
Intelligence	USMC	AN/PYQ-1	Digital Terrain Analysis Mapping System (AO504)		1-Apr-99	30-Sep-99	
Intelligence	USMC	IAS, MEF	Intelligence Analysis System, Marine Expeditionary Force		15-May-99	30-Jun-99	
Intelligence	USMC	TRSS	Tactical Remote Sensor System (USMC)	19-Feb-99	19-Feb-99	30-Apr-99	
Intelligence	USAF	SBIRS - High Ground	Space Based Infra-Red High Ground Component		13-Apr-99	1-Oct-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Biological Nuclear, Chemical, and Biological	Army	TOPDAR	TOCDF Process Data Acquisition and Recording		31-Mar-99	30-Apr-99	
Personnel and Readiness	Army	Keystone-Request -CS	Keystone-REQUEST Client Server		11-May-99	11-May-99	E2E
Personnel and Readiness	Army	MIRS	MEPCOM Integrated Resource System		15-Apr-99	31-May-99	E2E
Personnel and Readiness	Army	SIDPERS-3	Standard Installation/Division Personnel System - 3		21-Jan-99	15-Oct-99	E2E
Personnel and Readiness	Navy	IMAPMIS	Inactive Manpower and Personnel Management Information System		13-Aug-99	3-Sep-99	E2E
Personnel and Readiness	Navy	SDS	Pay and Personnel Source Data System	12-Mar-99	12-Mar-99	21-May-99	E2E
Personnel and Readiness	Navy	RESFMS	Reserve Financial Management System	5-Mar-99	4-Mar-99	19-Apr-99	E2E
Personnel and Readiness	Navy	BSS	BUPERS Support System		21-Apr-99	26-Apr-99	
Personnel and Readiness	Navy	MPTM&AS	MPT Management & Administration System		11-Jun-99	14-Jun-99	
Personnel and Readiness	Navy	NMPDS	Navy Military Personnel Distribution System		6-Aug-99	11-Aug-99	
Personnel and Readiness	Navy	TFMMS	Total Force Manpower Management System		21-Jun-99	25-Jun-99	
Reserve Components	Army	SIDPERS-ARNG	Standard Installation/Division Personnel System - Army National Guard		14-May-99	28-May-99	E2E
Reserve Components	Army	Manpower-Voucher Redesign	Manpower Voucher Redesign		30-Jun-99	30-Jun-99	
Reserve Components	Army	RISER	Resource Information System, Engineer, Reserve		30-Mar-99	15-Apr-99	
Reserve Components	Army	RCAS RPAM	Retirement Point Accounting Management		31-Jul-99	31-Jul-99	
Reserve Components	Army	RLAS	RSC Level Application Software		1-Apr-99	1-Apr-99	
Space and	Navy	ISCS	Integrated Satellite Control System		26-May-99	30-Jun-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Intelligence	SOCOM	Privateer	Privateer	30-Oct-99	31-Dec-99		
Intelligence	SPACECOM	SMPAS	Space Mission Payload Assessment System		15-Apr-99	15-Apr-99	OE
Logistics	Army	SAAS-MOD	Standard Army Ammunition System-Modernization		5-Mar-99	2-Jul-99	E2E
Logistics	Army	SARSS-2AD	Standard Army Retail Supply System - 2AD		5-Mar-99	4-Jun-99	E2E
Logistics	Army	SARSS-1(O)	Standard Army Retail Supply System Level 1 Objective		5-Mar-99	4-Jun-99	E2E
Logistics	Army	SARSS-2AC/2B	Standard Army Retail Supply System-Level 2A Corps/Level 2B		5-Mar-99	4-Jun-99	E2E
Logistics	Army	ULLS-A	Unit Level Logistics System - Aviation		18-May-99	15-Jun-99	E2E
Logistics	Army	ULLS-G	Unit Level Logistics System - Ground		19-Mar-99	24-Jun-99	E2E
Logistics	Army	WPS	Worldwide Port System		15-Oct-98	28-May-99	E2E
Logistics	Army	SAMS-1&2 Rehost	Standard Army Maintenance System - 1 & 2 Rehost (TACCS Replacement)		31-Mar-99	30-Sep-99	
Logistics	Navy	SNAP I (UNIX PORT)	Ported SNAP I Shipboard Non-Tactical ADP Program		31-Mar-99	30-Jun-99	E2E
Logistics	Navy	SNAP II (UNIX PORT)	Ported SNAP II Shipboard Non-Tactical ADP Program		31-Mar-99	30-Jun-99	E2E
Logistics	Navy	ROLMS	Retail Ordnance Logistics Management System			30-Sep-99	E2E
Logistics	Navy	NALCOMIS IMA	NALCOMIS IMA		31-Mar-99	30-Jun-99	IT
Logistics	Navy	AV3M	Aviation Maintenance Material Management		31-Mar-99	30-Jun-99	
Logistics	Navy	MOMMS	Micro Organizational Maintenance Management System	31-Dec-98	28-Dec-98	31-May-99	
Logistics	Navy	NALCOMIS OMA	NALCOMIS OMA		31-Mar-99	30-Jun-99	
Logistics	Navy	NTCSS-DANA	NTCSS-DANA Desk Top Environment		31-Mar-99	30-Jun-99	
Logistics	USAF	GATES	Global Air Transportation Execution System		30-Apr-99	30-Jun-99	E2E
Logistics	DLA	DFAMS	Defense Fuels Auto Mgmt Sys (also FAS & AVEDS)		31-May-99	31-May-99	
None	Army	SYSTEM 2	PMCISS System 2		29-Dec-98	30-Jun-99	
Nuclear, Chemical, and Biological	Army	JACON	JACADS Control Code		31-Aug-99	31-Aug-99	
Nuclear, Chemical, and Biological	Army	JAPDAR	JACADS Process Data Acquisition Reporting		31-Aug-99	31-Aug-99	
Nuclear, Chemical, and	Army	TOCON	TOCDF Control System		31-Aug-99	31-Aug-99	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Weather							
Space and Weather	Navy	METMF(R)	Meteorological Mobile Facility (Replacement)	10-Feb-99	11-Feb-99	30-Apr-99	
Space and Weather	Navy	NMPS	NAVSPACECOM Mission Processing System (NMPS)		23-Aug-99	30-Aug-99	
Space and Weather	Navy	OIS	Oceanographic Information System	24-Nov-98	24-Nov-98	30-Apr-99	
Space and Weather	USAF	GPS	GPS Space Segment		1-Apr-99	30-Apr-99	
Weapons	Army	M1A2	Abrams M1A2 Tank System		1-Mar-99	1-Oct-99	
Weapons	**Navy**	**ACDS BLK 0**	**Advanced Combat Direction System BLK 0 (LHA 2 & 4 only)**		**11-Jun-99**	**30-Jul-99**	**IT**
Weapons	**Navy**	**AN/BSY-2**	**AN/BSY-2 Submarine Combat System**	**1-Jun-99**	**2-Dec-98**	**30-Jun-99**	**IT**
Weapons	**Navy**	**TAMPS**	**Tactical Automated Mission Planning System**	**9-Dec-98**	**18-Dec-98**	**30-Sep-99**	**IT**
Weapons	Navy	ACDS BLK 1	Advance Combat Direction System BLK 1 (LHD 1, CV 67 and CVN 69 only)	26-Feb-99	12-Mar-99	30-Apr-99	
Weapons	Navy	ATWCS US SUB	Advanced Tomahawk Weapon Control System For US Sub	23-Dec-98	15-Dec-98	31-Aug-99	
Weapons	Navy	ATWCS TCGR	Advanced Tomahawk Weapon Control System Track Control Group Replacement	16-Dec-98	15-Dec-98	30-Jun-99	
Weapons	Navy	APS	Afloat Planning System	31-Dec-98	22-Dec-98	31-Aug-99	
Weapons	Navy	CCS REV 5.5	CCS Rev 5.5	31-Dec-98	16-Sep-98	31-Aug-99	
Weapons	Navy	CCS REV 6.3	CCS REV 6.3	30-Sep-98	16-Sep-98	30-Apr-99	
Weapons	Navy	CEC - BASELINE 2	Cooperative Engagement Capability Baseline 2	8-Feb-99	6-Feb-99	30-Aug-99	
Weapons	Navy	EA-6B TEAMS	EA-6B TSQ-142 (V5/6) TEAMS Software Release 205.04		1-Apr-99	1-Oct-99	
Weapons	Navy	JSIPS-N	Joint Service Imagery Processing System- Navy	31-Jan-99	27-Jan-99	31-Aug-99	
Weapons	Navy	TMPC	Tomahawk Land Attack Mission Planning Center	31-Dec-98	22-Dec-98	10-Apr-99	
Weapons	USAF	B-1B A/W/E	B-1B Mission Planning	2-Mar-99	8-Mar-99	14-May-99	
Weapons	USAF	F-117A MPS	F-117A Mission Planning System	1-Feb-99	29-Dec-98	30-Sep-99	
Weapons	USAF	F-15 EAGLE	F-15 EAGLE Mission Planning Interfaces		31-Mar-99	8-Jul-99	
Weapons	USAF	F-16 MSN PLAN	F-16 Falcon - Mission Planning Environment		28-May-99	28-May-99	
Weapons	USAF	KC-135 AFMSS A/W/E	KC-135 Air Force Mission Support System A/W/E	26-Feb-99	19-Feb-99	11-Jun-99	
Weapons	BMDO	AWS Baseline 6 Phase 3 AEGIS	AEGIS Program, AWS Baseline 6 Phase 3, TBMD		15-Mar-99	1-Jan-03	

Appendix2 - Mission Critical Systems Completed after 31 March 1999, Evaluation Plan by Function and Component

Function	*Component*	*Acronym*	*System Name*	*Validation ECD*	*Validation ACD*	*Completion Date*	*Evaluation Plan*
Weapons	BMDO	PAC-3	Patriot PAC-3		20-Mar-99	1-Jan-01	
Weapons	BMDO	SM-2 Block IV/IVA	Standard Missile Program, SM-2 Block IV/IVA, Area TBMD	20-Feb-99	10-Feb-99	1-Jan-01	
Weapons	BMDO	SM-3 (LEAP)	Standard Missile Program, SM-3 (LEAP), Theater TBMD	20-Feb-99	10-Feb-99	1-Jan-05	
	Navy	SMQ-11	AN/SMQ-11, Receiver Recorder Set, Meteorological Data	31-Oct-98	29-Oct-98	30-Jun-99	IT
	Navy	TESS NC Transition	Tactical Environmental Support System - Transition	15-Jun-98	29-Oct-98	30-Jun-99	

Congressional

SECRETARY OF DEFENSE ROUTING SLIP	ACT COPY	INFO COPY			ACT COPY	INFO COPY
SECRETARY OF DEFENSE		X		SECRETARY OF THE ARMY		
DEPUTY SECRETARY OF DEFENSE		X		SECRETARY OF THE NAVY		
THE SPECIAL ASSISTANT				SECRETARY OF THE AIR FORCE		
EXECUTIVE SECRETARY		X				
UNDER SEC FOR ACQUISITION & TECHNOLOGY				CHAIRMAN, JOINT CHIEFS OF STAFF		
Director, Defense Research & Engineering				Director, Joint Staff		
UNDER SECRETARY FOR POLICY		X				
ASD (International Security Affairs)				BALLISTIC MISSILE DEFENSE ORGANIZATION		
ASD (Special Operations/LIC)		X		DEFENSE ADVANCED RESEARCH PROJECTS AGENCY		
ASD (Strategy &Threat Reduction)				DEFENSE COMMISSARY AGENCY		
UNDER SECRETARY (COMPTROLLER)				DEFENSE CONTRACT AUDIT AGENCY		
Director, Program Analysis and Evaluation				DEFENSE FINANCE & ACCOUNTING SERVICE		
UNDER SEC FOR PERSONNEL & READINESS				DEFENSE INFORMATION SYSTEMS AGENCY		X
ASD (Force Management Policy)				DEFENSE INTELLIGENCE AGENCY		
ASD (Health Affairs)				DEFENSE LEGAL SERVICES AGENCY		
ASD (Reserve Affairs)				DEFENSE LOGISTICS AGENCY		
1 ASD (C3I)	X			DEFENSE SECURITY COOPERATION AGENCY		
ASD (LEGISLATIVE AFFAIRS)		X		DEFENSE SECURITY SERVICE		
ASD (PUBLIC AFFAIRS)				DEFENSE THREAT REDUCTION AGENCY		
GENERAL COUNSEL				NATIONAL IMAGERY AND MAPPING AGENCY		
INSPECTOR GENERAL				NSA/CENTRAL SECURITY SERVICE		
DIR, OPERATIONAL TEST & EVALUATION						
DIR, ADMINISTRATION & MANAGEMENT						

TYPE OF ACTION REQUIRED

	PREPARE REPLY FOR SEC OF DEF SIGNATURE		COMMENTS AND/OR RECOMMENDATIONS
	PREPARE REPLY FOR DEP SEC OF DEF SIGNATURE		INFORMATION AND RETENTION
1	REPLY DIRECT *(Forward copy of reply to CCD, Room 3A948)*	X	COORDINATE REPLY WITH LA USP
	APPROPRIATE ACTION		

Remarks:

REPLY DIRECT - MUST BE SIGNED BY COMPONENT HEAD

ACTION DUE DATE *(YYMMDD)*	ROUTING DATE *(YYMMDD)*	OSD CONTROL NUMBER	
990405 02	990319	U04259-99	

SD FORM 14, OCT 98 PREVIOUS EDITIONS ARE OBSOLETE. Designed using Perform Pro, WHS/DIOR, OCT 98
Overprint approved by OSD/WHS/DIOR, OCT 98

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

March 16, 1999

The Honorable William S. Cohen
The Secretary of Defense
Department of Defense
The Pentagon
Washington, D.C. 20301

Dear Secretary Cohen:

I would like to thank you for designating Dr. John Hamre, Deputy Secretary to represent the Department of Defense at the joint hearing of the Subcommittee on Government Management, Information and Technology and the Subcommittee on Technology on March 2, 1999. Dr. Hamre's comments were very helpful in our oversight of the department's status in solving the Year 2000 technology challenge. However, as I mentioned at the hearing's conclusion, there are several additional questions that we are formally submitting to you for a written response (see attachment).

Please send your responses to the subcommittee at B373 Rayburn House Office Building, Washington, D.C. 20515, by Friday, April 2, 1999. If you have any questions about this request, please have a member of your staff contact Matt Ryan of the subcommittee staff at (202) 225-5147.

Sincerely,

Stephen Horn

Stephen Horn, Chairman
Subcommittee on Government Management,
Information, and Technology

SH:mdr

ADDITIONAL QUESTIONS AND ISSUES FOR THE DEPARTMENT OF DEFENSE

Hearing on March 2, 1999

Questions for Dr. John Hamre

1. Please provide a list of all currently noncompliant systems that will not be tested in an operational evaluation.

2. Please provide a list of all currently noncompliant systems (by functional unit) that will be tested only by a functional test.

3. Please provide a detailed explanation of the status of the intelligence community's computer systems. Please identify intelligence systems that are currently noncompliant, and the estimated date they will become compliant. If this information is classified, please tell us how we might obtain this information.

4. You stated that Year 2000 readiness in Russia is a concern. Could Year 2000 disruptions in Russia result in the leakage of classified weapons technology, which could lead to nuclear proliferation?

5. U.S. troops stationed abroad rely on the infrastructures such as power and water of foreign countries for numerous services. Is the military taking precautions to ensure that U.S. troops stationed abroad will be safe and that military bases will be fully operational in the event that foreign infrastructures fail?

Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

1 April 1999

MEMORANDUM FOR SENIOR CIVILIAN OFFICIAL

THROUGH: PRINCIPAL DEPUTY
for DASD (CIO P&I)
PRINCIPAL DIRECTOR, Y2K

FROM: Director, Y2K Financial Management and Reporting SR 4/1/99
(Prepared by Kevin Garrison, 602-0961, ext. 141)

SUBJECT: Hearing on Subcommittee on Government Management, Information Technology – ACTION MEMORANDUM

PURPOSE: To provide responses to Questions for the Record (QFR) from the House Committee on Government Reform (Tab A).

DISCUSSION:

- The Deputy Secretary of Defense testified at a joint hearing of the Committee on Government Reform, Subcommittee on Government Management, Information and Technology, and the Subcommittee on Technology, on March 2, 1999. The QFR from the hearing were forwarded to the Secretary of Defense on March 16, 1999 (Tab B).
- The QFR involve:
  - Status of system Year 2000 compliance and testing efforts
  - Status of intelligence systems
  - Possibility of nuclear proliferation due to Y2K problems
  - Status of efforts to ensure US installations overseas are protected from host nation Y2K infrastructure problems
- Areas addressed by the QFR were covered in the prepared statement for the hearing as well as in oral testimony. The responses to these specific questions are amplifications of information already provided.

COORDINATION: ASD(LA) 1Apr99; DASD(P&E)/CA ~~No USD(P) concur~~.

RECOMMENDATION: That you sign the attached letter (Tab A) transmitting the responses to questions for the record to the House Committee on Government Reform.

USD(P) concur
for DASD Stam/SITR/Rice

Y2K Control No.: 03-167/99
C3I Control No.: 03-167/99
OSD Control No: U04259-99

4. Weapons Technology Proliferation.

You stated that Year 2000 readiness in Russia is a concern. Could Year 2000 disruptions in Russia result in the leakage of classified weapons technology, which could lead to nuclear proliferation?

The Department of Defense engagements with the Russian Ministry of Defense (MOD) are in the preliminary stages and to date efforts have focused primarily on management techniques and commercial solutions. The current emphasis is to assist the MOD in effectively assessing the YEAR 2000 problem, making sound resource decisions, determining which resources to dispose of, and the establishment of organization standards that continually address critical YEAR 2000 issues. The application of competent management techniques and solutions is important to the reduction in the risks of proliferation. ~~The greatest YEAR 2000 danger is~~ in the area of nuclear stockpile security, specifically the security of nuclear materials. ~~The Defense Threat~~ Reduction ~~Agency (DTRA)~~, through its Cooperative Threat Reduction (CTR) Program currently provides assistance to the MOD to improve the management of nuclear weapons stockpiles at storage sites throughout Russia. One of the primary goals of this increased effort is the continuous safe and secure storage, transport, and accounting of these Weapons of Mass Destruction, especially during the Year 2000 transition. ~~DTRA~~ will continue the YEAR 2000 dialog with Russia throughout the remainder of this year.

One area of concern to the US is the impact of Y2K

The Department of Defense

Mr. HORN. Did any other service want to comment on this? If not, I now yield time to the gentleman from Minnesota who is the vice chairman of the Science Technology Subcommittee, Mr. Gutknecht?

Mr. GUTKNECHT. Thank you, Mr. Chairman. I think at this point most of the important questions have been asked. But I do want to come back to a very important point, and in fact, if Mr. Ose would like, I would probably have time to yield to him, but I more or less want to make a statement here.

I really do believe that our own Defense Department is doing an excellent job, and I think you are all to be commended for the seriousness that you take relative to this problem. I think the concern that you have heard echoed in different ways is, what can we do to affect both our allies and those who may not be particular friendly toward us? There is a growing body of countries out there, friendly and unfriendly alike, who are working around the clock to develop intercontinental ballistic missiles, or at least different venues to deliver weapons to other places around the world. And my real fear, and I think the fear of Members of Congress, and I think I speak on behalf of the American people, I think the biggest concern about this is we really don't have a contingency plan in place if something should go wrong.

And part of the reason I have been a supporter through the years of development and deployment of a strategic defense program is, I think, highlighted by this circumstance. I mean, we are not just talking about Russia here; we are talking about Red China; we are talking about North Korea; we are talking about potentially countries in the Middle East. There is a growing list of potential problems out there whose technology is not necessarily what the United States is.

And so, while I applaud what you folks are doing to solve these problems relative to the United States, I really do think that we need to do more on an international basis, either through the United Nations, through our own State Department, whatever we can do to make certain that we avoid the potentiality of a problem on December 31st or January 1st, whichever way you look at it, so that we don't have a problem with an inadvertent launch or some other mistake that may happen as a result of this particular computer glitch.

And I don't know if you really want to respond to that or not, but I think it is something, Mr. Chairman and Madam Chairman, that we need to continue to pursue and put pressure on our government officials, as well as officials from around the country because this is a very serious potential problem.

Mr. MONEY. Yes, sir, we do have a couple of comments, if we might, Admiral Willard, and then I will add something.

Admiral WILLARD. I would just, sir, point out that only the United States and Russia have extremely robust strategic early warning systems that could be subject to the year 2000 failure. In fact, though proliferation is all of our concern. The only countries that you mentioned have somewhat limited early warning capacity. So, from the standpoint of the initiative that was mentioned earlier between the United States and Russia, it is focused on the partners

that have the worldwide early warning capability to begin with that could ever be prone to failure.

Mr. OSE. Would the gentleman yield?

Mr. MONEY. And if I just might add, you asked, and I failed to answer your previous question about, or whoever brought up about what can you all do. I encourage you in any interactions you will have with your counterparts, for example, in the Duma and other bodies that you may have some interaction with, to encourage them to get on with the Y2K remediation, and in the particular case, for the Duma support of this stability center.

We testified in front of Senator Bennett just the other day, I believe the Senate, and maybe you all would like to join in, is thinking about going over and having a conversation at the right time with folks in the Duma, for example. My request is if that in fact occurs. I would also recommend or ask you for your support to stopping in locations where we have troops stationed—Germany, South Korea, Southwest Asia—to encourage the local governments there to help make sure that our interdependency on whatever power water, telephones, and so forth, when we are in garrison and those countries, is in fact up to snuff, so that will alleviate some of demands on us. So, I would ask for that kind of consideration.

Mr. GUTKNECHT. Mr. Chairman, I yield——

Mr. HORN. I think that is a very good suggestion, and I can assure you a number of us will be doing that.

Mr. GUTKNECHT. Mr. Chairman, I will yield the balance of my time to Mr. Ose.

Mr. OSE. If I could followup on one thing—the early warnings systems joint effort with the Russians, is there any number of hotspots around this world or countries who might not have an early warning system, but might be receptive to the idea of having access to, at that point and time, where the technological failure is greatest, might welcome the chance to sit at this same table with direct communications to their CINCs, or what have you? I wonder, in particular, about you notwithstanding the recent comradery about India, Pakistan, for instance?

Mr. MONEY. Yes, sir. In fact, that is being suggested. The State Department, in fact, is working that. I could conceive this not just being there only for the Y2K period, but being there in a permanent sense. So, as countries develop nuclear weapons, they have some idea what their neighbor may or may not be doing that would, I think, add to the stability of that.

So, my recommendation, but it is a State Department action, is any country that has nuclear weapons ought to be invited to be there just to see what else is going on, so they have some assurance that they are not under attack or whatever suspicion they might have. So, I agree wholeheartedly with you, it ought to be broaden.

Mr. OSE. Mr. Chairman, I would welcome the chance to sign a letter of your aghast futilage to that effect, and I yield back the rest of my time.

Mr. HORN. I think it is a good suggestion. Mrs. Morella and I would be glad to join you in that with maybe all of our colleagues to get the message across. We do have relations, of course, with the European community. We have discussed this with them when Mr.

Gilman led the delegation over there. But, we also have a concern about the lackadaisicalness of some of the countries on the domestic side where they just sort of say, well, you know, if it happens, it happens. I mean, they are still in a state of denial in a few industrial countries, and in the developing countries, they simply don't have the money or the technology know-how to get at the problem on even the domestic side. So, I think we all face that problem.

Does the gentleman from Texas have any other questions he would like to ask?

Mr. TURNER. Mr. Chairman, maybe just a couple. And, I certainly want to commend our witnesses today for the testimony because I think it has been very reassuring to us. And, I think anyone who listens objectively to what has been said here should rest easier about the status of the Department of Defense and Y2K compliance.

I wanted to ask Mr. Money, just could you give us an estimate as to how much it will cost the Department of Defense by the time we get through to comply with Y2K?

Mr. MONEY. Yes, sir, and this is an estimate. There is not a lot of high precision behind this. But the current estimate, the latest to the OMB is we are somewhere around $3 billion.

Mr. TURNER. $3 billion?

Mr. MONEY. $3 billion.

Mr. TURNER. It always amazes me, and of course, we have had many of these hearings with Federal agencies, but the price tag that we have had to incur and pay to be sure we are Y2K compliant has been enormous. It makes you realize that, no matter how sophisticated we have become as a society, we are really not too smart after all. [Laughter.]

Mr. MONEY. Whoever is here 1,000 years from now, I hope they are not having the same problem.

Mr. TURNER. Right. One of the things that Mrs. Maloney asked you about earlier was what kind of—I believed she asked the Inspector General—what kind of contractual language do we have to protect the Department and the Government against Y2K problems? Have you, in all of your efforts to remediate, and after you will spend $3 billion to correct this problem, has any of the responsibility ever been shouldered by any of our outside contractors or suppliers of the various systems and computers that we utilize in the Department of Defense?

Mr. MONEY. Oh, yes, sir. Let me start with the answer on the contracts. As Bob mentioned, roughly a year—maybe it has even been longer than that, language was to be put into every new contract—whatever that contract was to deliver to the DOD, would be Y2K compliant. We chose not to go back and notate all the previous contracts. We said we would start from that point on.

Contractors, again, vary in degrees just like countries or maybe departments and governments, that some are taking it more seriously than others. But when systems are being delivered today, they are being tested. They are tested at—the contractors will test them. If they fall into a mission-critical system, some do, but not many, what we call mission-critical is what we will go to war with today or conduct any operation, whatever is called upon us. So that

is pretty much equipment that is already in the inventory. So, all that is being done. Some contractors are taking us on with a vengeance, some with more diligence than others, but I would say, by and large, the private industry, and so forth, have come onboard with what is needed.

I do worry about the 15th-tier supplier. We have talked with primes and second-tier and third-tier, but you get down to several tiers now. So I just picked the 15th-tier that supplies something. We fully expect, because we have gone through just-in-time inventories, regardless of who you are, in the government or contractor sub-tier, and so forth, that some missing some deadline there, rolling effect could, in fact, happen, and to me that is probably the biggest danger that we will be facing, and that is totally unpredictable. We can't. So we just have to wait for that to occur, and then we will react to it.

I can't overemphasize, though, that your Department of Defense can meet any operational problem that comes along, whether that is humanitarian operations in Africa or whatever may be called upon, or in Southwest Asia or Kosovo, wherever we may be in armed conflict. We have the wherewithal to conduct those operations, and if one of these systems does fail, we have contingency plans, and we are exercising those to back fill, so we can continue to operate in any of these calendar disruption periods.

Mr. TURNER. I guess I might ask—this is my last question. Is there any area of lingering concern that you have based on all your oversight of this process of remediation in the area, lingering concern, anything that still keeps you awake at night that you might want to share with the committee, so we will be thorough, to have examined every area of potential problem?

Mr. MONEY. Well, you just said it. There is no way, time, money, that we can examine every possibility. We talk about mission-critical systems, and then the thread through as you tie one to another to another. We are not testing all the infinite combinations of those threads. We are testing the threads that the CINCs are most likely need to use. Consequently, there are things that we are not testing, and that does worry me, but we are doing the best we can with the resources. Frankly, the biggest resource we are lacking now is time to pull all of this off. I am confident; I, frankly, do sleep at night. It may not be as long as I like.

Nevertheless, Dr. Hamre mentioned my name a couple of times. Frankly, these people down on the table here and the services are the ones, and many, many, many people that aren't here today—essentially, the Department of Defense has really taken this on. I admit there are some people maybe that don't have quite the awareness, but I believe everybody in the Department today at least knows what Y2K means and how that might impact them.

The other part of this is—Bob Lieberman mentioned this—we have learned how to use the auditors. We view these folks as additional, independent, clearly independent, but additional people on the team to say what we are doing right or wrong because they view things from a different prospective. So, it has really been a total effort, including the GAO. That may not be often you hear that over here from a DOD person, but it is true. We have opened the door to everything we do, to whomever wants to come in, and

consequently, because we do appreciate the perspective from people when they see things from another viewpoint. So, I hope my, Dr. Hamre, our mission today was—we are not arrogant; I don't mean it that way at all, but we are confident that we can ride through any calendar disruption and conduct any operation the Nation may call upon us.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. I just want to clarify one point in the answer. We have heard so often that there is a danger of polluting our fixed computers that are Y2K compliant. Is there any danger that the non-critical mission plans and systems in the Department of Defense would interact with the critical mission systems which are compliant, and is that a problem?

Admiral WILLARD. Sir, it is a good question. Frankly, the non-mission-critical systems are undergoing the same rigorous testing and remediation processes that our critical mission systems did, and as well, they are part of the architectures that we are testing in our operations evaluation process. So, first of all, they are being remediated. Second, they are being captured in these large-scale integration tests that we are doing.

I think, to answer Mr. Turner's question in the glass half full sense, when you consider the relative successes that we are seeing through the small number of operations evaluations that we have completed thus far, I think our level of confidence is rising that this rigorous process that we apply to each individual system is a good one, and that together the systems will test satisfactorily. That should give us a good deal of confidence, even of the systems that are outside the bounds of these critical thin lines and architectures that the commanders in chief, for example, are testing.

Mr. HORN. So, you have analyzed those systems that are just regular business systems, or whatever; they can't get into your other systems that are compliant with the year 2000?

Admiral JOHNSON. If I could, sir—in the Constellation Battle Group systems integration tests that we are doing right now, we identified approximately 30 mission support systems that we thought were necessary for the functionality of that battle group, and included them in our testing. What we are finding is that we have good program managers. We told them what to do; they went out and did it, and they defined their interfaces; they tested those interfaces, and then as we put those systems together, in fact, they are performing the way we expect. We are finding that the kinds of problems we have found in the last week on CONNIE, a display on a COTS system, actually, that was certified to us by a supplier, read 1900 instead of 2000. It still worked, just had a display error. Those are the kinds of things that we are finding.

We are finding the systems operate. We may have a display functionality wrong or a day functionality wrong, but in terms of actually supporting the war-fighter, the systems work.

Mr. HORN. Any of the other services want to comment on this, the separation of non-critical mission systems that are not compliant or have not even been looked at because you are focusing correctly on the mission-critical systems? The Air Force?

General AMBROSE. Well, although the Air Force tracks a little over 400 mission-critical systems, we are looking at about 3,400

total systems. And, although all of them aren't as far along as the mission-critical systems, all of them will be Y2K compliant by January 1, 2000. So, we are confident that those systems won't corrupt the mission-critical systems.

Mr. HORN. The Army, Ms. Browning.

Ms. BROWNING. The Army tracks approximately 700 mission-essential systems, and we are tracking them quite closely. One of the things that we are doing both for our mission-critical and non-mission-critical, when we test them, we have to test all the interfaces, so if a mission-critical system interfaces with a non-mission-critical system, that is part of the test. So your concern about its corrupting one another, we have already accounted for that. And our main concern is the operational function that it is supporting, regardless of whether the system is mission-critical or not.

The test we did at White Sands, the test we have done at Fort Bragg and at Fort Sill, include both mission-critical and non-mission-critical in the threads that we are testing. In fact, our non-mission-critical systems, if you will, are probably ahead of our mission-critical systems in compliancy because they are, frankly, less complex and have less interfaces. So, we are very confident of those. But right now, we see no potential for corruption since our testing rules require that all the interfaces be done during the test.

Mr. HORN. Thank you. Colonel McHale, the Marines?

Colonel MCHALE. As I mentioned earlier, the majority of our systems are operated and maintained by the other services, and we are confident that they are tracking the right thing and we are tracking them as they track those systems.

Mr. HORN. So, you see no danger of pollution out of your other systems that are not critical?

Colonel MCHALE. And in the definition of mission-critical that was taken into account when we defined the system as mission-critical, and as Ms. Browning said, the interfaces are being tested in all the operational evaluation scenarios.

Mr. HORN. We thank you. And now I yield to the gentlewoman, the co-chairman of the Working Group Task Force, whatever we are called now, Mrs. Morella.

Mrs. MORELLA. Well, it is ongoing. Thank you, Mr. Chairman.

I want to thank you all for your testimony, and the fact that it reflects to us a commitment, and a commitment is what is really necessary, I think, in compliance with this incredible challenge.

I go back to what Mr. Lieberman said in his testimony and orally, that the most daunting aspect of Y2K is testing. And, I think we have heard that in different ramifications throughout—the idea of, is it the right testing? Are we circumventing doing it the right way in order to save time and to save money, inadvertently sometimes, the whole magnitude of testing? I am just wondering if you have any comments on it?

I would like to also mention an article that came out in DOD Computing. It refers to an IG report that is entitled, "Management of the Defense Special Weapons Agency Year 2000 Program," and the IG audit has found that the weapons agency didn't complete independent testing of three mission-critical systems before classifying them as ready. The articles goes on about the agency tested one mission-critical system, the Nuclear Management Infor-

mation System, and two have 10 non-mission-critical systems, but the IG said the agency classified all 13 as 2000 ready. And it goes on in that vein. This indicates something about the problem with testing, and I would like to hear comments from you about how do we attack this problem? What are we doing? Do you agree that this is an enormous challenge? Maybe, should I start with you Mr. Lieberman, the IG?

Mr. LIEBERMAN. Fine. That audit report was issued the day before Thanksgiving, so it was November, and it reflected the situation in that particular agency as of a few weeks before that. Those particular systems, by the way, are back on track. The last two of them will be——

Mrs. MORELLA. Mr. Inspector General, this actually had been published, though, on January 25th.

Mr. LIEBERMAN. The press article, yes. All of the systems discussed in the audit report will be implemented by the end of this month, as a matter of fact. However, we had a lot of problems initially with the managers of systems prematurely certifying that they had fixed and validated the fix on their systems. I think that the problem is behind us. The Department went back and looked at all the systems that we had not late last year, and quite a few were moved backward in terms of the reporting. That is, they were decertified. One of the reasons why the percentage of completed systems had apparently dropped, and I would say that was to the good, because it was a more accurate representation of where we really were. We are now past the point where, for most systems, we are talking about individual system level testing and certification anymore. Now we are talking about group tests, end-to-end tests, or system-of-systems tests.

Once again, I think you are absolutely right, we have to fight against any tendency to replace numbers of tests for rigor of testing, and there is a difference there. We have to do something to make sure that all these tests have the proper technical support while they are being run. An awful lot of things are happening at the same. The crunch is going to come, particularly, in the May, June, July timeframe, when the functional end-to-end tests kick in. Right now, we are just doing a few of these operational evaluations, so there is still a limited demand for technical expertise. But it is going to be tough to support all these tests adequately at the same time.

And the last thing I would say is that those commands that were most ready to do good testing went first. So, we would agree, NORAD did a fine job. Generally, the Space Command and the Strategic Command are way ahead of the other unified commands. So, they went first, did a good job, as would be expected, and had good results.

There are other commands that have different kinds of challenges, and I think the overseas commands, the big combatant commands, particularly, the Pacific Command, European Command, Central Command, are going to have a much more difficult time, for no other reason than they have real-world operational considerations that are going to distract them constantly. So, that still remains a big challenge. I am happy with my characterization of it as the most daunting challenge.

Mrs. MORELLA. Let's take note of that. Would anyone else like to comment on it? All right, Mr. Brock and then Secretary Money.

Mr. BROCK. Yes, I think there is another issue. Testing is going to be daunting, and Mr. Lieberman is right that the two initial CINCs that did the testing had somewhat of an advantage over some of the others because they also controlled more of their own systems they used. And so, they didn't have as many interfaces or dependencies on systems outside their control. But, nevertheless, we did find the guidance for those processes to be very rigorous. And I want to repeat that, that we were very pleased with the guidance.

Other tests that are coming out, as I have also mentioned in my statement, for some of the functional areas have not been defined yet. And that is our concern. These tests probably aren't as rigorous or require the same level of rigor found in operational tests, but by the fact that they aren't defined and some of them aren't scheduled, makes us wonder when they will be squeezed in.

Second, there is a whole issue which we really haven't addressed today, and that is the need to develop contingency plans or business continuity plans. The vast number of mission threads or thin lines or business processes that we have been talking about today, for the most part, still need to be developed, and also need to be tested. And so, the Department has a fair amount of work to do in a relatively short period of time.

Mrs. MORELLA. Try to follow that Secretary Money.

Mr. HORN. Mr. Money. She has asked my questions, so take your time.

Mr. MONEY. Back to the article. The article suggested that there was a fraudulent entry, and so forth. When that was published, the Deputy Secretary and myself, we called every service, every Defense agency, into the room and the high-level people in each of those services, like the vice chiefs and/or agencies attested to that their reporting, in fact, is accurate and not fraudulent. There was a misinterpretation, by the way, in the test plan. We requested that there be an independent signoff, not just the program manager or whoever was on the particular program. I believe we are past that. By no means do I want to minimize the testing that we performed.

I see a very important date, somewhere around the end of March, March 31st, because we will have had the operational test, at least one series of those. We will learn a lot from that. I don't expect that every one of these will fly through with no hiccups and no problems. In fact, we will focus on some where those may be.

Let me use an example of a few months ago; we had a test down at White Sands Missile Range, an end-to-end, and it flunked; it failed miserably. Went back and fixed the systems, had another one, roughly, I think it was about 3 months later—this is about 3 months ago—and it flew. We were even doing telemedicine to some remote village. So, we will go through that.

Relative to the functional testing, those were addressed later. A lot of the non-mission-critical area falls into there. But there are, to varying degrees, contingency plans. Let me give you an example.

When Dr. Hamre talked about the DFAS going through the fed, going to various banks, when that is exercised, if we see any prob-

lem with that, we will then go back and buy check stocks so we can issue checks the old way versus electronic funds transfer. Frankly, I am holding onto that. That is $4 million I would rather spend somewhere else. We will make that decision roughly the end of June. That is time enough to get the checks in place, and so forth. So, we are working through those. By no means do I want to sit here and claim that we have this whipped, that we have thought of every aspect.

One of you asked me earlier, what do I worry about? It is what we haven't thought of. You don't know what you don't know, what is going to come back and bite us in that way. But through the various tests and the extensiveness that we are trying to address those, we hope to uncover, discover, if you will, what is out there that we need to fix.

Mr. HORN. Any other questions on that or other people?

Mrs. MORELLA. I think Admiral Willard wanted to comment on that.

Admiral WILLARD. Mrs. Morella, I would comment that, with regard to magnitude of testing, that there was a methodology applied to determining what would be tested, for example, in the operational evaluations. And that methodology dealt with determining the missions of each of our unified commanders and the tasks that supported those missions and picking the most critical tasks. There is no shortcut being applied to the architecture that supports that task. So, it wasn't arbitrary. On the contrary, it was very methodical.

With regard to the points that Mr. Lieberman made on the paucity of technical expertise, that is a challenge that we continually face. By and large, when we have date functions in systems, we require the systems expert from the program manager of that system to be present to assist us in rolling clocks forward and rolling clocks back and restoring systems to 1999. It is a challenge associated with all of our evaluations, and we are spreading that expertise thin, as you can imagine. The ratio of technical expertise to systems with clocks averages about 0.75 to 1. I mean, we need nearly as many technical experts as we have systems with clocks as we step through these functional end-to-end tests and operations evaluations. So, scheduling those individuals is crucial.

On the point that was made regarding the fact that the CINCs that are farthest along are conducting their operations and evaluations earliest is true. And we are doing that because our data base captures the lessons learned and results of those evaluations, and in turn, they are spread about the other CINCs. So, those CINCs that are challenged the most, that are overseas, that are busy in other areas of the world, or that have chosen the most difficult tasks to OPEVAL, have the benefit of these earlier evaluations, successes and failures to draw on. So, we are sharing lessons learned across them all, and we hope that by the time we get to the most difficult and most challenged unified commands, that they would have absorbed a great many of the lessons from the earlier evaluations. So that too, I think, is being done very methodically.

And then my last point would be this: Again, back to the magnitude of testing, I think as the Services comment, you will find that the rigor with which they are testing is generally through very

time-tested methodologies to test their various systems. They are not inventing a lot of new things. In the case of CINC OPEVALs and picking architectures according to task, that was relatively new to us. But many of the integration tests are leveraging off of very rigorous integration tests that we have performed on our weapons systems, and other systems for many, many years with success.

Admiral JOHNSON. I would like to quickly address a couple of things, sir. One of them is the concern about shortchanging testing. A huge quantity of testing is completed by the program managers in their validations. That is complete for about 91 percent of the Navy systems right now. And now we are in the fielding business. What our experience in operational evaluations has found is that the testing was rigorous because we aren't finding problems in our operational validations.

The operational testing is being run by operational commanders. They are defining the scope of testing, and they are calling upon the SYSCOM commanders and other technical experts to provide the support they need in order to satisfy them that the systems that are being deployed, in our deployed units, are in fact, going to work and provide them the capability they need.

Another comment, and I am shifting to a separate subject, and that is on the area of contingency planning. We think we are very, very far along in the area of contingency planning. We have worked with our operational commands and our shore establishments to develop a contingency planning guide which we published last November. Our operators already have casualty procedures and operating procedures in place to deal with system failures. They do that on a daily basis. We have backup and redundant systems.

And what we are doing is exercising those capabilities they already have and their operational capabilities to shift to backup systems or backup methods in the event of a system failure, and we are exercising those procedures in our operational evaluations. We already have disaster preparedness plans at our bases. We are looking at those in terms of year 2000, and making sure that those disaster preparedness plans reflect the year 2000 aspect of it, and will be ready to be implemented, if necessary. So we think the contingency planning aspect of that is much farther along than a lot of people think. And we are exercising all of those contingency plans and continuity operational plans in our operational evaluations.

Mr. HORN. Admiral, as you have mentioned, contingency plans, and before General Ambrose does, I am reminded with Mr. Money's comment, they are going to go back to just writing out checks. There is even an earlier contingency plan the Navy practiced, which was just pay it out in cash and sign for it, which was what the Senate did when I came there in the 1960's. They had some Navy officer, who is now comptroller of the Senate, to just passing it out in cash. And I remember one basic commander, General Ambrose, who paid the whole base in $2 bills. And believe me, community relations went up with the Air Force when they saw thousands of $2 bills out there.

But go ahead.

General AMBROSE. Until about 4 months ago, I was the Commander of Offutt Air Force Base in Omaha, NE, and fortunately, we have had such a tremendous relationship with downtown, I didn't need to do the $2 bill thing, but it will be a good hip pocket thing to hold.

I would just like to point out, just a couple of days ago, our auditors presented a report to me on a phase validation we asked them to do. Basically, we asked them to go back and take a look at a sample of the systems that we have certified, across all criticalities, not just mission-critical, and take a look at the process, and the exit criteria for going through each step of the process, and make sure we did that right. And they went out and looked at 267 systems, most of which were chosen at random, and they reported no testing discrepancies of any kind, and in fact, only a couple of minor discrepancies of any kind, not a statistically significant number.

In terms of OPEVALs, and especially the end-to-end tests, we are spending a lot of time right now making sure that when we test, the quantity and the quality are both what they should be, and that we are testing the right processes and the right systems. And realistically, you can't test every possible way that you will use even your mission-critical systems. So, what you must do is ask how do we use these in the preponderance of our operations and that is what we will test.

Now, we are ready for the unexpected things that occur, because we have told our program managers and, more importantly, we have told our commanders that you need to take a look at all that you do from the standpoint of what is it that you can't stand to shut down, and then have another way to do that thing. And that is how, I think, the entire Department is approaching Y2K. So, if the computers work, and we think they will, great. If they don't work, we will continue to do business because we have another way to do it.

Mrs. MORELLA. If I just might mention one thing—with our very distinguished military here, and Inspector General, and GAO representative, I am reminded—I have mentioned this once before at a hearing—of Admiral Grace Hopper. Remember the first woman admiral? She is the one who devised COBOL. Don't you wonder what she is thinking now, from where she is up with St. Peter as she looks down on the need for people who are skilled in using COBOL and in remedying this problem that she was a little part of?

And I thank you. Thank you, Mr. Chairman.

Mr. HORN. Ms. Browning.

Ms. BROWNING. Mrs. Morella, I would like to answer two of your questions, one, whether we are testing the right stuff——

Mrs. MORELLA. Thank you.

Ms. BROWNING [continuing]. And two, about the veracity of our certification? And by the way, I am sure Grace Hopper is laughing in her grave; I would think that.

What I would like to give you—I don't know if you want to enter this into the record, but as to whether we are testing the right stuff, the Army looked at its major battlefield functional areas, how it does business. We have over 100, what we call, mission threads.

We have boiled that down to 24 critical mission threads. This was done not by the techs; this was done by the war fighters. So, these are the threads; these 24 critical ones are the ones that we are testing. And we are testing them at the division, at the corps; they are being tested in the OPEVALs, in the end-to-end tests.

We are also, in terms of testing the right stuff, the minimum we are doing are four critical dates. And that is true across the Defense Department. The September 9, 1999 date, the crossover, the midnight crossover on December 31, and there are two midnight crossovers on the leap year. Those are the minimum. Some tests, especially if they are complicated business systems, are testing more. But we are testing those. In addition, we have a lot of management controls on the test. The Army has been using for over a year and a half the Army Audit Agency. There are internal management consultants to Y2K from my office. They have been doing very good work for us. They are out there asking the questions on the contract compliance, on the interface agreements, et cetera, and we constantly get reports and updates from them. In addition, for our testing, we are going to use our operational tests and evaluation command, to sit with us, the technical folks, the functional folks, to do that.

Mr. HORN. Without objection, that exhibit is put in the record at this point.

Ms. BROWNING. Thank you. Also, for all of our contingency plans that we have for mission-critical systems, they not only have to have a technical piece, but also a functional piece. So, we are looking at that.

Your second question on the veracity of the certification, and this is for the certification of our individual systems, for all mission-critical systems in the Army, we require either a senior executive service or a flag officer signature on that. And we require it in two channels, both the technical or the material developer channel, as well as the functional channel.

We also, again, have those management controls. We have sent some of those back from our front offices because they haven't looked at everything. We also have the AAA working with us on that.

One final thing, if you ask how I don't sleep at night because of Y2K, I would say the thing that probably bothers me the most is the outside dependencies. I am very confident in the Defense Department, not only in the Army, but the rest of the components. It is the outside dependencies, whether they be our suppliers, whether they be foreign countries, and the more that we can do nationally to get that message out and to educate people, I think the more we minimize risks come this December.

Mr. HORN. Well, I take it you are looking at electricity, food supply——

Ms. BROWNING. Yes.

Mr. HORN [continuing]. Water, et cetera. I mean, we might face a Berlin airlift, I think, in some of these bases, but I would think it depends on how distant they are from the main source of supplies.

Ms. BROWNING. And how robust the infrastructure is around them.

Mr. HORN. Right. And that should be a worry, just in general.
Ms. BROWNING. Right.

Mr. HORN. So is the Army asking those questions on the contingency plan? Because as I get the reports from the Department, and all departments, all 24 of them, we hardly see any movement in facing up to a contingency plan. Now, maybe they are just optimistic and say, well, gee, we will finish by March 31st and we will get the testing done and all of that. Very few contingency plans. The one that you see in the domestic departments, perhaps the Department of Defense, is we will use the United States Postal Service. And the other day, we had the Postal Service in, and we said, "What is your contingency plan?" I didn't snidely say, "Is it a mailbox?" I just let that pass. But, that is one of the problems on, say, getting checks out and everything else to one's employees, which have mortgages to pay and all the rest of it. So, that is a worry, and yet, I don't see much movement on the contingency plan in its reporting.

Colonel McHale, what about the Marine situation?

Colonel MCHALE. Certainly. Ms. Browning mentioned the Army developed the critical mission threads. Coincidentally, at the same time, at a parallel independent path, the Marine Corps arrived at the same conclusion in evaluating and constructing our OPEVALs much the same way the Army did. When I heard about the Army system, I immediately suspected that we had taken a wrong turn some place because we were doing the same thing, but it verified that we were doing the right thing.

On contingency plans, the Marine Corps requires contingency plans for all our mission-critical and all our mission support systems because of that interdependency of the two systems. And we found that, in doing that, that causes us to be more rigorous about the way we were evaluating our plans. You are concerned about not having contingency plans, I believe, as the Department of Defense goes through this process of conducting the operational evaluations, conducting tabletop seminars, that that will cause us to focus again away from the system-by-system evaluation and to focus on the larger functional, and, in our case, the Marine Corps-wide plan of how we are going to operate on day one, how we are going to operate on January 1st, and those contingency plans will evolve as we get away from the system-by-system analysis.

One comment about the operational evaluations that we are conducting: I am amazed that it turns out that every Marine Corps general officer was born in Missouri and they don't want to take anybody's word for anything. So as we have developed our operational evaluation plan, we have said, these are the systems that you have to test in a minimum configuration. And we have found in all the operational evaluations that we have conducted or are planning to conduct that they are additional systems, that our Army systems or Air Force systems, that they want to be able to have—if I can use the term "warm and fuzzy" feeling about—and the Commandant has charged them at the time of this operational evaluation cycle, which will complete for us at the end of July, that each one of them needs to come back to the Commandant and say, "I can do my mission." And he is not really going to be concerned

about, well, it was an Air Force or it was a Navy system that failed.

A marine commander has to be able to do his mission regardless of what systems he has to bring to bear, and that is what he is evaluating. So, it far exceeds whatever the congressional requirements are for systems that are only Marine Corps owned and operated.

Mr. HORN. Mr. Ose, any further questions? Mrs. Morella, any further questions? Mr. Turner, any further?

Mr. TURNER. No, thank you.

Mr. HORN. I have one last question, and that is on the nuclear supply, and this is really directed at Mr. Money and Admiral Willard.

In terms of your weapons support and the use of the nuclear suppliers in the United States, has the Department of Defense asked these questions of its supplier or have they left it generally to the Department of Energy as the cabinet department supplier, if you will? Because some people are worried about some of our reactors and are there microprocessors in there that lead in one condition or the other by—let's take it, we are in Illinois. Most of their electrical power is generated by nuclear reactors. If we have blackouts, which haven't had anything to do with nuclear reactors at this point—and sometimes we don't have the slightest idea what contributed to that blackout in either the San Francisco situation, the New York situation; that was a decade ago. I am just curious, if we are looking at suppliers, it seems to me the Defense Department has a role in there, and are they worried or not?

Mr. MONEY. Yes, sir. If we start with the weapons versus the reactors generating power——

Mr. HORN. Right.

Mr. MONEY [continuing]. DOE has that responsibility. DOD overlooks that CINCSTRAT in particular.

Anything you want to add?

Admiral WILLARD. Yes, sir. There is a simple answer: By and large, the facilities that are owned by the Department of Energy [DOE] are being overseen by DOE, and the interfaces to those facilities are being checked by the Department of Energy. In those areas where an interface exists between our strategic commands and those vendors, then Strategic Command is maintaining visibility. I think Admiral Mies would assure you of that.

Mr. MONEY. When it gets to reactors, then that is a power generation and that will be a DOE reporting up through John Koskinen.

Mr. HORN. OK. We thank you. We will be pursuing that in a couple of months, and obviously, we have got a major concern on the nuclear reaction in terms of supply for civilians, as well as military indirectly, in some cases.

Let me just thank the people—and then I will have a few remarks here—thank the people that helped prepare this hearing: J. Russell George is in the door down there, staff director and chief counsel for the Subcommittee on Government Management, Information, and Technology; Matt Ryan, senior policy director, right behind me here for that subcommittee; Bonnie Heald, director of information and professional staff member; and Mason Alinger, the

clerk for the subcommittee; Richard Lucas, our faithful intern; and for the Technology Subcommittee, Richard Russell is back of Mrs. Morella, staff director; Ben Wu, professional staff; and Joe Sullivan, the clerk.

And for the minority we have Faith Weiss, the counsel, and Jean Gosa, the clerk.

And for our faithful court reporter, it is Leslie Preer.

I think you have all given some very compelling testimony this morning, and it, obviously, pleases all of us that both the Inspector General of Defense and the GAO are working together, and everybody in all the services seem to be working together. So, I commend you for that.

Let's face it, the safety of our country and other countries depend on the Department of Defense's mission-critical services, and we have been concerned, obviously, that the Defense Department seems to be behind schedule, but it could be that you are in the Preakness or something and you are waiting for the last few laps. I don't know. I have sometimes said, with the administration, when it took a long time to get them organized, that it was like the "Perils of Pauline." You know, she is strapped over the railroad, you think she is a goner, next Saturday, she is doing great. [Laughter.]

And that is when movies were 10 or 15 cents.

I appreciate Secretary Cohen and Deputy Secretary Hamre, and now, hopefully, Assistant Secretary-to-be Money, for the leadership they are providing. I think that has absolutely been essential in solving some of these problems.

But we remain concerned about the preparedness and potential vulnerability of foreign military bases, and we are delighted with the initiative the Secretary took in relation to the Russians. I happen to feel very strongly that, if we don't win the Russians in with us as part of the western democracy down the line, we would have made the biggest mistake we could make in diplomacy in the last part of this century. So, I am glad those relations were started when General Powell was chairman of the Joint Chiefs of Staff; I am glad they are going on.

And I thank all of you for testimony. It is good to know that progress has been made within the executive branch. I think we still see a lot that has to be done, and some of it relates to the national defense, and hopefully, with all of your hard work, we will get that job done. And we thank you for coming.

With that, this meeting is adjourned.

[Whereupon, at 1:12 p.m., the subcommittee was adjourned.]

○