Statement of

JOHN J. HAMRE
DEPUTY SECRETARY OF DEFENSE

Before the

Committee on Armed Services
United States Senate

On

PROGRESS TOWARD YEAR 2000 COMPLIANCE

February 24, 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.

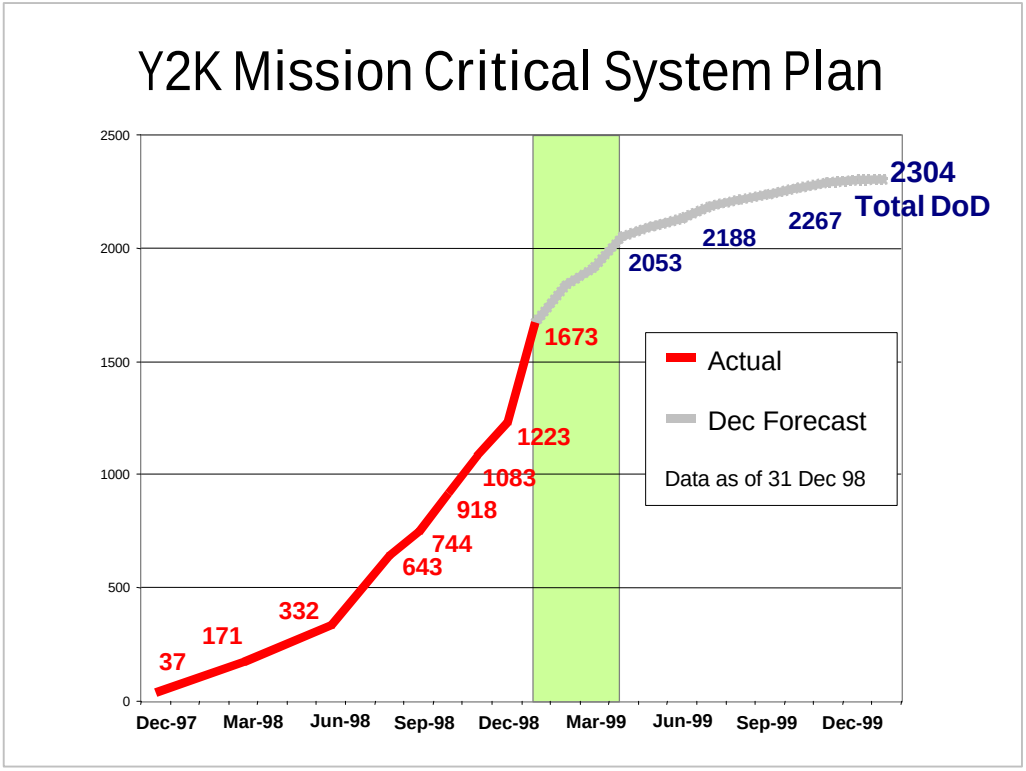

Figure 1 DoD Y2K Compliance Forecasts and Results

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.

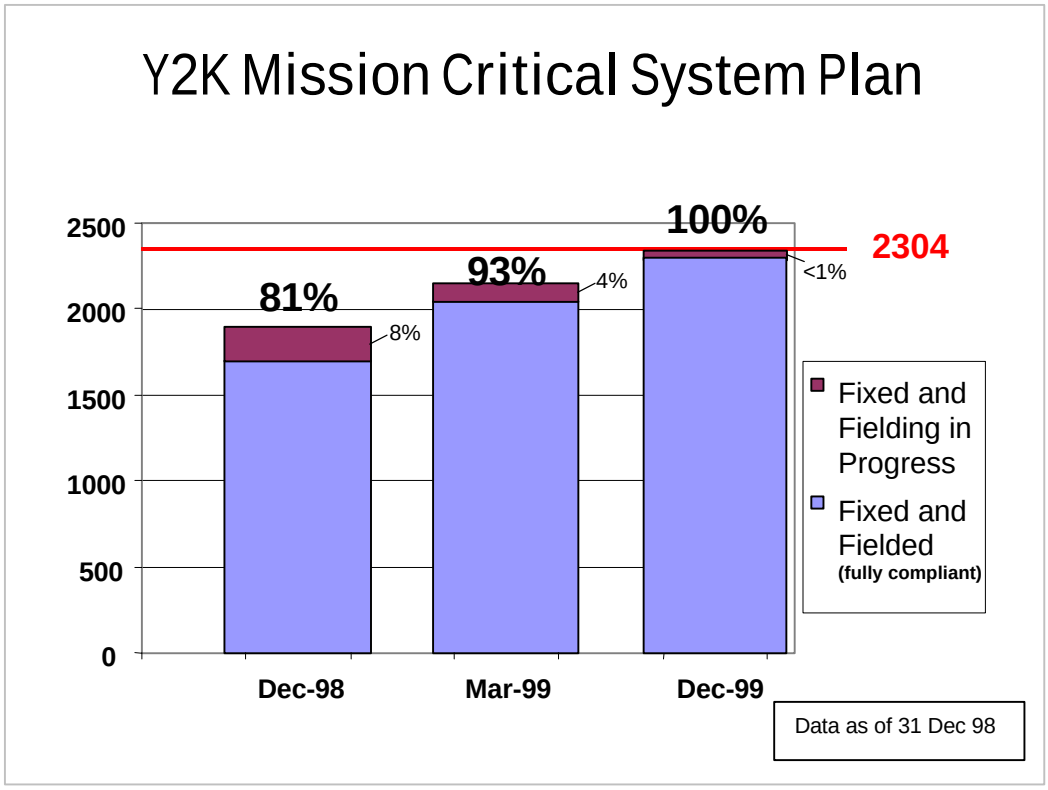

Figure 2 DoD Status at Key Milestones

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

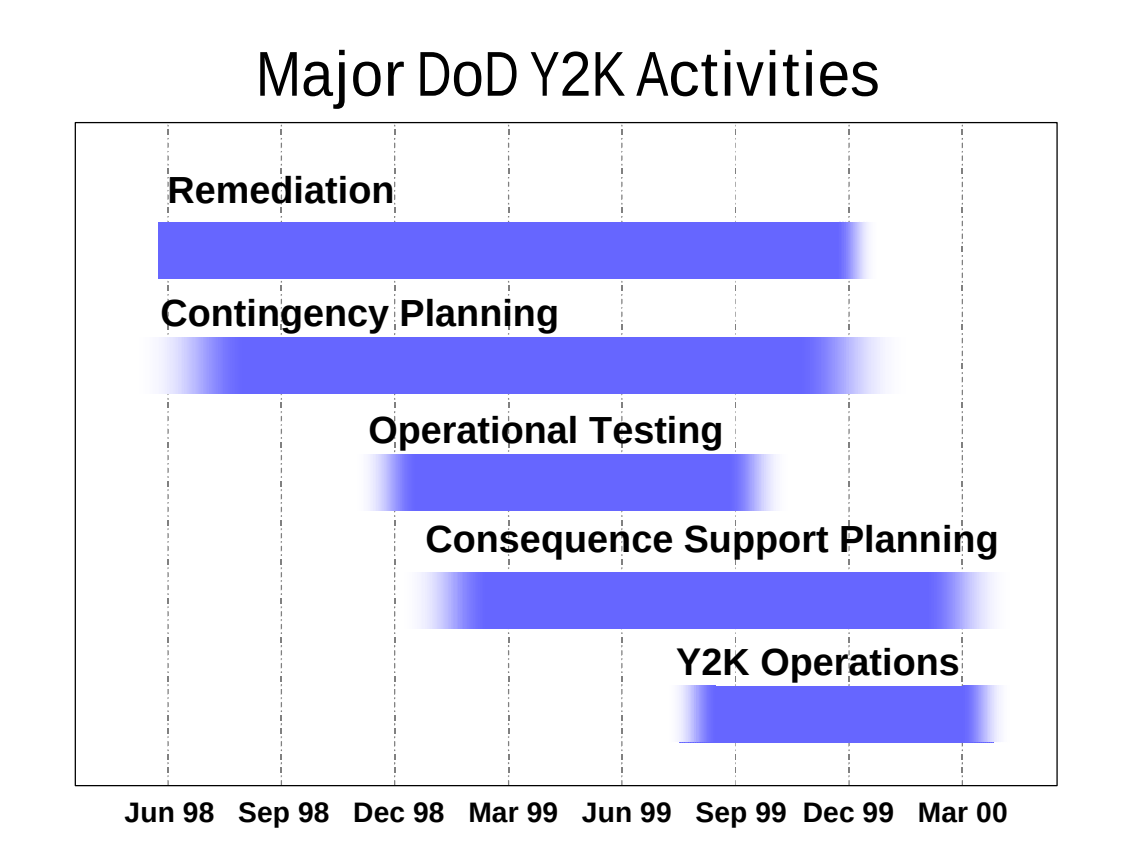

Figure 3 - Major DoD Y2K Activities in 1999

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 General Accounting Office and the Office of Management and Budget 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."

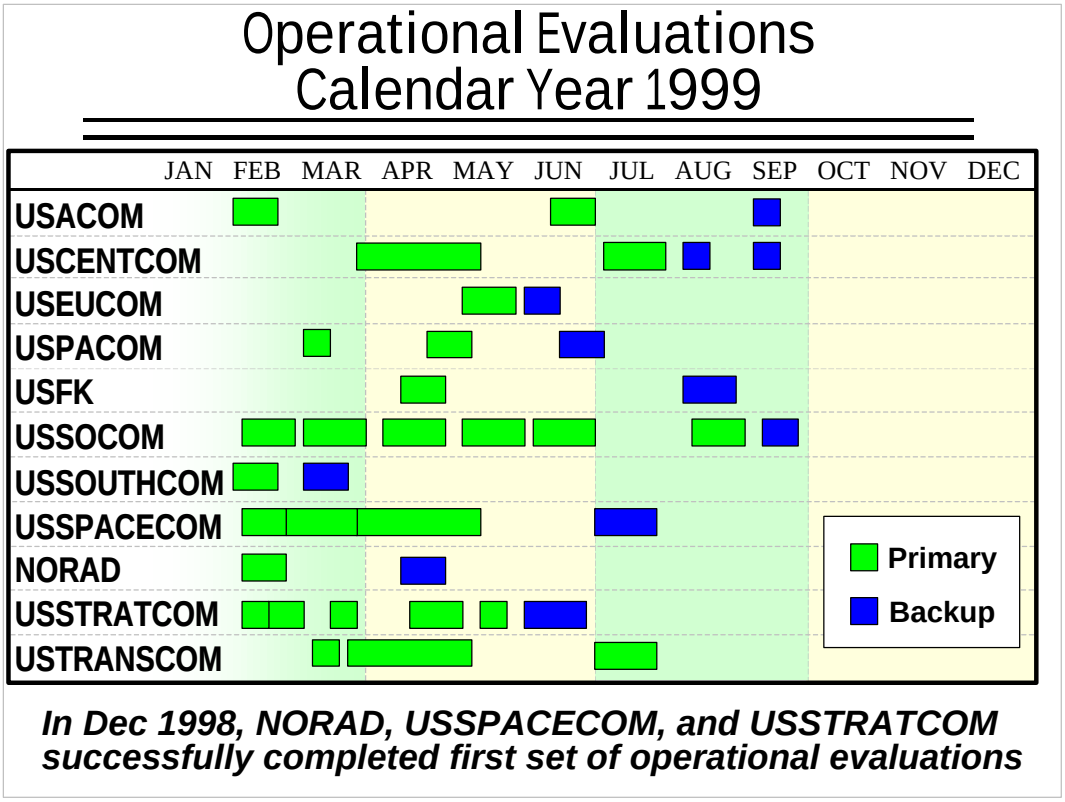

Figure 4 DoD Combatant Command Operational Evaluation Activities in 1999

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.

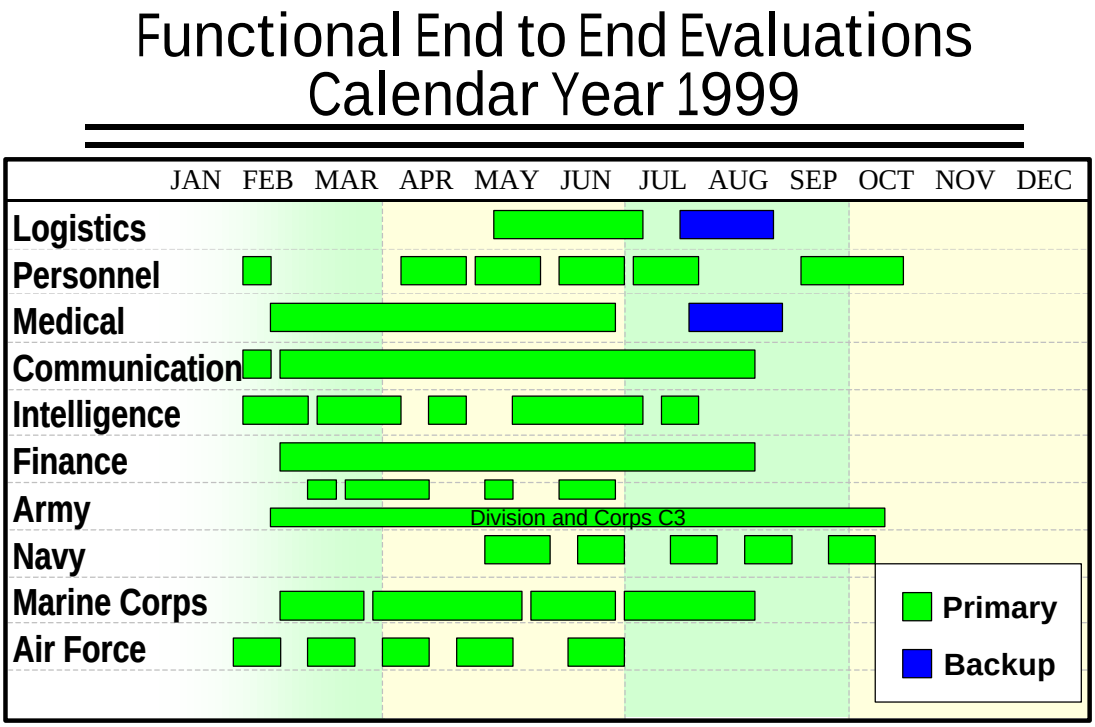

Figure 5 - DoD Functional End-to-End Evaluations in 1999

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 Chiefs of Staff for their subordinate commands and to the Principal Staff Assistants in the Office of the Secretary of Defense 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 REPONSE Y2K

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 I will defer to my colleague, the Deputy Director for Central Intelligence, on the specifics of other nation status.

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 military support to civil authorities (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 compliancy status.
- Rescheduling work held in abeyance for the more urgent goal of Y2K compliance. In summary, the opportunity cost of delaying the development of other systems in order to pay for, schedule, attain compliance, and observe the configuration freeze to ensure continued Y2K compliance, 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.