



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



JUN 16 1999

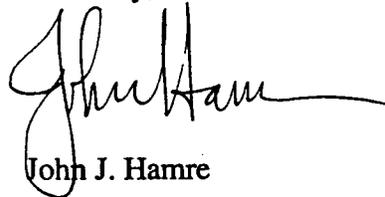
Mr. Jacob J. Lew
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Lew:

Enclosed is the Department of Defense (DoD) Business Continuity and Contingency Plan requested by Office of Management and Budget (OMB) memorandum M-99-16, "Business Continuity and Contingency Planning for the Year 2000," May 13, 1999.

The DoD high level plan for business continuity and contingency planning outlines the management approach to Year 2000. It reviews evaluation and testing of mission capabilities, and discusses the continuity and contingency planning in detail. It summarizes DoD Year 2000 date transition period planning, leadership preparation activities, and consequence management planning in accordance with the guidance in the General Accounting Office publication, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning" (August 1998).

Sincerely,



John J. Hamre

Enclosure

U09151 199



Department of Defense
High-Level Plan

**Business Continuity and
Contingency Planning**

Submitted to

Office of Management and Budget

June 15, 1999

Table of Contents

| | |
|---|----|
| Introduction | 1 |
| DoD's 1998 Focus – Fixing Systems..... | 1 |
| Management Focus..... | 1 |
| DoD Year 2000 Management Plan..... | 1 |
| Effective Senior Management Oversight | 2 |
| CEO Involvement | 2 |
| Accurate Reporting Mechanisms..... | 2 |
| DoD's Leadership Focus for 1999 – Ensuring Mission Capability | 2 |
| Evaluation and Testing of Capabilities | 3 |
| Operational Readiness Evaluations..... | 3 |
| Functional End-to-End Evaluations..... | 4 |
| Integration Testing | 5 |
| DoD Y2K Continuity and Contingency Planning | 5 |
| Business Impact Analysis..... | 6 |
| Core Functions..... | 6 |
| Planning Assumptions..... | 7 |
| General Planning Assumptions..... | 7 |
| CONUS | 7 |
| OCONUS | 7 |
| Site-Specific Planning Assumptions..... | 7 |
| Other Risks to DoD Operations..... | 7 |
| Domestic Infrastructure Disruptions..... | 7 |
| Host Nation Infrastructure Support Disruptions..... | 7 |
| NATO/Allied Systems Interoperability Disruptions..... | 8 |
| Contingency Planning Oversight and Tracking..... | 8 |
| System Contingency Plans..... | 8 |
| Operational Contingency Plans | 8 |
| Year 2000 Transition Period..... | 8 |
| Leadership Preparation for Decision-Making | 9 |
| Table Top Exercises | 9 |
| POSITIVE RESPONSE Y2K..... | 10 |
| Consequence Management Planning..... | 11 |
| Conclusion..... | 12 |

List of Figures

Figure 1 – DoD Combatant Command Operational Evaluation Activities in 19994

Figure 2 – DoD Functional End-to-End Evaluations in 19994

Figure 3 - Overall Year 2000 Table Top Exercise (TTE) Concept 10

Figure 4 - Chairman of the Joint Chiefs of Staff Contingency Assessment #1 Results..... 11

Figure 5 - DoD Operational Readiness and Consequence Management Priorities 11

Introduction

This document describes the overall strategy and process for ensuring the readiness of key programs and functions across the Department of Defense (DoD). It summarizes guidance already issued, planning already conducted, and future preparations for the Year 2000 transition. It reiterates essential elements of the four major documents guiding DoD efforts on the Year 2000 problem:

- DoD Year 2000 Management Plan, version 2.0, December 1998.
- Secretary of Defense memorandum, "Year 2000 Compliance", August 7, 1998.
- Deputy Secretary of Defense memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities", August 24, 1998.
- Deputy Secretary of Defense memorandum, "DoD Year 2000 (Y2K) Support to Civil Authorities", February 22, 1999.

The Department's business continuity and contingency planning (BCCP) efforts are only a part of its overall Y2K preparations. To place them in perspective, this document reviews the overall DoD management strategy for Y2K including the initial focus on fixing systems and the current focus on ensuring mission capabilities, briefly summarizes DoD's wide spectrum of testing activities, and then discusses the various facets of DoD BCCP efforts in detail.

The scope and complexity of the Y2K problem for the DoD is unparalleled in the federal government. The Department has over one-third of the mission critical systems in the federal government and most of the embedded chips. As of the 9th Quarterly Report to the Office of Management and Budget (OMB), submitted on May 17, 1999, DoD has approximately 6,700 systems, of which 30 percent (2,038) are active mission critical systems. The Department also operates 637 military installations around the world and in the United States, which are like small towns, and rely on supporting infrastructure systems also vulnerable to Year 2000 problems. Due to DoD's extensive reliance on information technology systems, the initial management focus for Year 2000 preparedness was on assessing and fixing systems.

DoD's 1998 Focus – Fixing Systems

As the Deputy Secretary of Defense testified in February 1999, DoD spent much of 1998 getting a management structure and strategy in place to focus its efforts on Year 2000.

Management Focus

The Department's management efforts last year were focused on four key enablers: publishing a DoD Management Plan for Year 2000, implementing effective management oversight, making Year 2000 a Chief Executive Officer (CEO) problem rather than a Chief Information Officer (CIO) problem, and getting accurate reporting mechanisms in place.

DoD Year 2000 Management Plan

The Department developed and published a Year 2000 management plan that specified component responsibilities and outlined how to achieve Year 2000 compliance for systems consistent with the five-phase OMB process. The Department also made some key decisions about how to track "systems" at the Departmental level as well as how to categorize systems (as

either Mission Critical, Mission Essential, or Non-Mission Critical). The initial categorization was done by information technology specialists on CIO staffs and provided a screening and prioritization mechanism for DoD. Through the last quarter of 1998, the list was reviewed and scrubbed by CEO staffs and became a much more reliable management tool.

Effective Senior Management Oversight

Every month the Deputy Secretary of Defense chairs a DoD Year 2000 Steering Committee meeting to review progress toward achieving readiness for Year 2000. 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 means to reinforce that Year 2000 is a CEO problem, not a CIO problem.

CEO Involvement

The key event in energizing the Department was publication of Secretary Cohen's memorandum, "Year 2000 Compliance," August 7, 1998. This document firmly fixed responsibility for ensuring DoD's capability to continue operations, regardless of the Year 2000 problem, on the shoulders of the Department's CEO leadership. In addition, the Deputy Secretary of Defense issued a memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," August 24, 1998, further specifying 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 the Department's ability to track progress in these areas was implementation of a common DoD database of systems.

Accurate Reporting Mechanisms

The Department worked hard to establish a stable baseline and list of systems against which to measure progress. The Department significantly improved its ability to track Year 2000 compliance from a single authoritative database. The DoD Y2K database has been used since January, 1999, as the source of systems compliance reporting for internal management reviews and for reporting to external agencies such as OMB and Congress. The Department is expanding the database effort to incorporate the ability to capture the results of testing and evaluation efforts taking place this year and to assess system contingency planning results.

DoD's Leadership Focus for 1999 – Ensuring Mission Capability

In early January of this year, senior DoD leaders held a daylong meeting to review the results of our efforts to fix systems in 1998. Another meeting was held on April 13, 1999, to review DoD progress toward meeting the OMB deadline of March 31, 1999, for mission critical systems. There are still important efforts necessary to achieve Year 2000 compliance for all DoD systems. The Department's management efforts in 1999, however, are shifting to end-to-end evaluations of functional capabilities, contingency plan preparation and testing, and preparing for operations in the period surrounding Year 2000 transition.

Evaluation and Testing of Capabilities

The DoD efforts this year are principally focused on improving confidence in the Department's ability to continue to execute the National Military Strategy. The Department has already completed initial testing of most individual systems and their immediate interfaces. In 1999, DoD is concentrating on complex, real-world end-to-end testing of DoD "business functions" and Warfighter missions – the things that DoD does in carrying out the national military strategy.

During 1999, DoD 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" of systems that 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 (OSD), and the Commanders in Chief (CINCs) of Unified Commands.

The DoD evaluation and testing efforts are extremely complex with many events occurring nearly simultaneously. The Services will be conducting integration testing of functional or mission threads. Principal Staff Assistants on the OSD staff will organize and conduct end-to-end evaluations of functional capabilities. Finally, the CINCs, and the Warfighters, have each selected among their own unique missions to devise real-world operational evaluations to exercise various warfighting missions. 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 synchronization of the entire evaluation plan.

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 the evaluation program. Finally, the GAO and the OMB provide a review by external auditors.

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

Operational Readiness Evaluations

The DoD is using the Department's Warfighters, the CINCs, to evaluate operational readiness to conduct operations unaffected by the Year 2000 problem. The Fiscal Year 1999 Defense Authorization and Appropriations Acts require DoD to conduct at least 25 operational evaluations, with each Unified Command conducting at least 2 exercises. The Department will meet those requirements, as shown in the figure below.

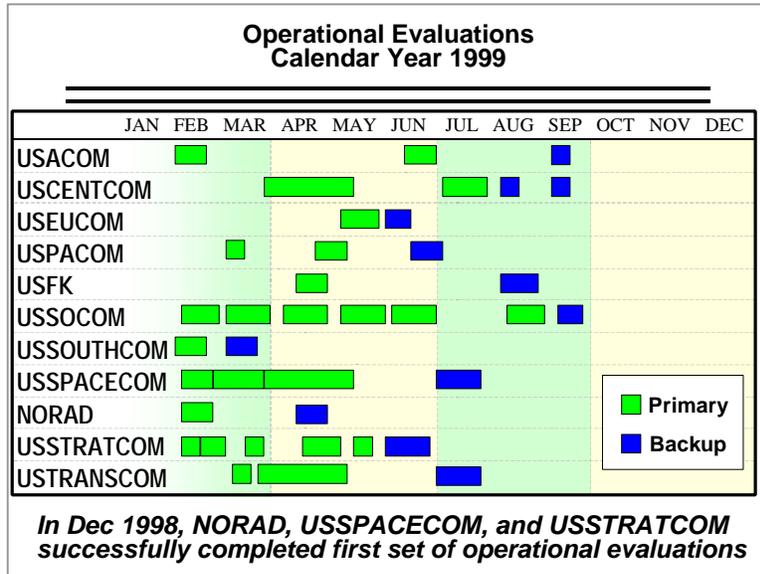


Figure 1 – DoD Combatant Command Operational Evaluation Activities in 1999

The DoD approach to assessing operational readiness has been to validate the complete warfighting process, from “sensor-to-shooter” using the significant dates specified by the GAO Testing Guide. Initial results confirm that this kind of evaluation is essential to providing the additional assurance that systems will remain operational over the Year 2000 transition.

Functional End-to-End Evaluations

The Department is using the DoD Business Process Managers – the Principal Staff Assistants (Functional Proponents) – to evaluate its ability to continue core support functions despite Year 2000. Each functional process owner: logistics, finance, communications, intelligence, personnel, medical and others will conduct end-to-end evaluations of core business functions as shown in the figure below.

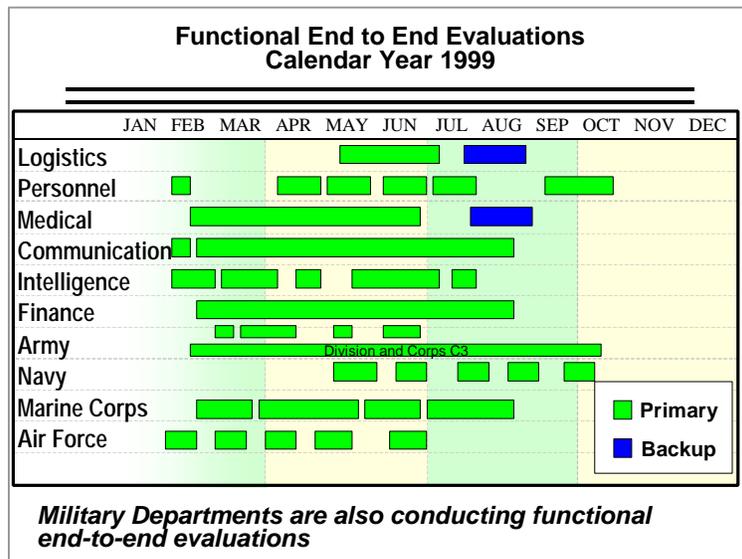


Figure 2 – DoD Functional End-to-End Evaluations in 1999

In some functional areas, particularly logistics, the Services are conducting end-to-end evaluations of their internal functional systems before 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.

Integration Testing

Service integration testing will fix responsibility with the Department's system owners – the Military Departments – to ensure continued functioning of other key processes that allow for Title 10 functions of organizing, training, and equipping forces. This testing is over and above the five-phase OMB process each individual system must complete to be certified as Year 2000 compliant.

Service 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 end-to-end testing. These tests are the third method DoD is using to ensure departmental compliance with the evaluation requirements contained in the Fiscal Year 1999 Defense Authorization and Appropriations Acts. Those Acts require that “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 DoD maintains the hard won confidence in 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, DoD has the largest and most comprehensive evaluation plan in the Department's history, and is continuing to work on refining plans to improve the overall evaluation of core DoD functions. This plan will significantly improve the level of confidence in DoD's ability to carry on operations despite Year 2000. While these extensive efforts will mitigate risk, the interconnectedness of everything guarantees that Year 2000 will have an impact on DoD. To deal with this reality, DoD must focus on realistic continuity of operations and contingency planning.

DoD Y2K Continuity and Contingency Planning

Like all U.S. Government Agencies, DoD is using Contingency Planning to ensure continuity of critical functions in the event of unforeseen disruptions to DoD and Government Systems or the supporting infrastructure. Y2K Contingency Planning within DoD takes on different forms and uses different names than other agencies, but is built on the same foundation as the GAO recommended approach to Business Continuity and Contingency Planning.

Information requirements, methods and techniques to be used in developing all contingency plans are outlined in the DoD Year 2000 Management Plan. Amplifying guidance has been promulgated by each of the DoD Components. A DoD Commander's Y2K Preparedness Handbook has been published by the OASD(C3I)Y2K Office to assist in the process of determining local risks, based on the infrastructure supporting each site.

The two primary types of Y2K continuity and contingency plans within DoD are:

- System Contingency Plans – which document the planned actions associated with a timely restoration of a system to full functionality following a Y2K-related disruption to the hardware and software associated with the system. Within DoD, System Contingency Plans are required for all date-aware mission-critical systems and strongly recommended for most other systems. The status of system contingency plans for mission-critical systems is being tracked in the DoD Y2K Database.
- Operational Contingency Plans – which document the planned actions associated with maintaining a pre-designated minimum level of capability during any disruptions to the supporting systems or infrastructure. Operational Contingency Plans may be written in support of a single system or application, in support of a single mission or function, or in support of the full range of missions or functions performed by a DoD entity. When the planning is in support of a single system or application, the system contingency planning information and the operational contingency planning information are often combined in a single plan.) Operational Contingency Plans may be known in some DoD Components as Continuity of Operations Plans, Operational Continuity Plans or Business Continuity Plans.

Business Impact Analysis

Impact Analysis is performed using operational risk analysis procedures standard for all DoD planning processes. Most DoD missions are characterized by extremely long and complex information chains. To ensure that these chains were thoroughly examined, the Joint Chiefs of Staff, each of the Unified Commands, the Services and most DoD Agencies used a technique called *Thin Line of Systems Analysis* to determine the critical paths by which information flowed during the execution of their primary missions. Identifying the *thin lines* served to ensure that all mission-critical systems were identified for each DoD mission/function. Systems comprising these *thin lines* were all involved in end-to-end testing to ensure that all elements were fully Y2K compliant.

Core Functions

The Department of Defense is a very complex organization. Under its present organization, there are three primary allocations of responsibility. These may be described as follows:

- Warfighting, which is the responsibility of the Joint Chiefs and the Unified Commands
- Organize, Train and Equip, which are the Title X responsibilities of the Services.
- Support Functions (Logistics, Personnel, Health/Medical, Communications, Intelligence) which are the responsibilities of designated Principal Staff Assistants (PSAs) within the Office of the Secretary of Defense.

The DoD commands are assigned missions from various higher authorities. These missions can be analyzed and linked to elements from the applicable Service or Joint Mission Essential Task List (METL). The missions and METLs of each DoD command correspond to the core functions of that command.

Planning Assumptions

There are two major categories of planning assumptions: general assumptions applicable across DoD, and site specific assumptions applicable to a unique location.

General Planning Assumptions

DoD Operations occur worldwide and thus the general planning assumptions are separated into CONUS and OCONUS locations.

CONUS

For purposes of preparing DoD business continuity and contingency plans, DoD Components should assume that electric power, natural gas, water service, waste treatment, financial services, transportation, public voice and data communications, the Internet, mail service, and the mass media will be available domestically, although it is possible that there will be localized disruptions in some areas. Each Command preparing an operational contingency plan shall make a determination as to the degree to which the general assumption applies to the sites(s) covered by that particular plan.

OCONUS

In Non-U.S. locations, DoD follows the general planning assumptions of the State Department, which, in cooperation with other agencies, is gathering Y2K information on a country-specific basis. The State Department has designated the Head of Mission in each country to be the U.S. lead on Y2K issues there, and agencies with interests overseas should work with the State Department to understand the risks to their operations and to develop appropriate assumptions.

Site-Specific Planning Assumptions

The Commander / Director responsible for each DoD site or facility is responsible for determining the appropriate site-specific planning assumptions for that location. This entails due diligence in seeking out the Y2K status of local suppliers of critical services and supplies to that site in support of its core functions.

Other Risks to DoD Operations

The principal external risks to DoD Operations may be separated into three categories: Domestic Infrastructure Disruptions; Host Nation Infrastructure Support Disruptions; U.S. and NATO/Allied Systems Interoperability Disruptions.

Domestic Infrastructure Disruptions

Domestic infrastructure disruptions are addressed during the normal contingency planning process. DoD planners make full use of the extensive information available through the internet and the large number of DoD Y2K-related websites.

Host Nation Infrastructure Support Disruptions

Regional Discussions with Host Nations for OCONUS installations have been used to ensure that Y2K planning assumptions are valid, as discussed previously. In addition, the

OASD(C3I)Y2K Office has representatives working directly with NATO to facilitate the process of information exchange among NATO planners. Since the most critical status updates are those to be collected in the final months before the Date Transition Event, this process will grow in emphasis during 1999.

NATO/Allied Systems Interoperability Disruptions

Interoperability Testing has been planned to ensure systems interoperability with Allied and NATO systems. The operational contingency plans developed by Joint and Allied Commands will address procedures to be followed in case of unforeseen disruptions.

Contingency Planning Oversight and Tracking

Oversight and tracking for contingency plans differs based on the type of contingency plan: system or operational.

System Contingency Plans

These plans, a responsibility of Chief Information Officers and Program Managers, are centrally tracked as to its status for all mission-critical systems. Oversight responsibilities with respect to Plan viability and completeness fall primarily on the CIO or Program Manager. Many system plans also received additional oversight during the Operational Readiness Assessments, other testing and during DoD IG and Service IG visits and inspections. The OASD(C3I)Y2K office reviews all test reports and IG reports involving contingency plans and advises the cognizant staff as to its recommendations.

Operational Contingency Plans

In keeping with DoD's management strategy of centralized policy development, decentralized planning and execution, the Joint Chiefs, the PSAs and the Services are each responsible for determining the elements which must do Operational Contingency Planning in that organization. In general, all units with a Director or Commanding Officer are required to develop these plans. Tracking and Oversight responsibilities remain with the organization and the status of operational contingency plans is not captured in the DoD Y2K Database. DoD IG and Component IG offices provide an additional level of oversight.

Year 2000 Transition Period

The Department has designated the period September 1, 1999, through March 31, 2000, as the "Y2K Date Transition Period." This period encompasses possible events occurring from the 9/9/99 date and from the February 29, 2000, leap year date. To prepare for the unprecedented nature of possible Year 2000 problems, DoD is developing procedures to ensure its ability to identify, report, and respond effectively to Year 2000-related events.

As indicated in the earlier response on national security responsibilities, DoD formed a Year 2000 Consequence Management Integrated Process Team (IPT). The IPT consisted of representatives from all elements of the Department, including the Services, Joint Staff, OSD Principal Staff Assistants, and the Director of Military Support (DOMS). The IPT reviewed current guidance, processes, and procedures for providing domestic Military Support to Civil Authorities (MSCA). The IPT also reviewed the organizational structure, processes, and procedures necessary to respond to requests for foreign disaster assistance.

Based on recommendations made by the IPT, DoD is:

- Ensuring resource visibility and refining its allocation processes by identifying DoD assets that have utility in providing Military Support to Civil Authorities.
- Refining operations and reporting procedures and developing an agreed to lexicon to ensure the creation and maintenance of a “common operational picture.”
- Developing a triage strategy to ensure that DoD resources are applied in the most effective and efficient manner possible.
- Developing specific Year 2000 training materials to ensure that everyone involved in MSCA knows the specific means and methods for dealing with Year 2000-related requests.
- Refining its procedures for ensuring real-time decision support information is provided to DoD authorities to include creation of an Infrastructure Monitoring and Decision Support Activity. The Activity will monitor critical Defense systems and infrastructures, public broadcasts, and the Internet to provide infrastructure reliability and decision-support information to the Executive Support Center.

Throughout 1999, DoD will conduct a series of events to prepare senior leadership for possible decisions required by Year 2000 contingencies and to evaluate the Department’s operational contingency plans.

Leadership Preparation for Decision-Making

There are two major activities in preparing DoD leadership for dealing with Year 2000: Table Top Exercises and the CJCS-Sponsored Exercise POSITIVE RESPONSE Y2K (PRY2K).

Table Top Exercises

The Department announced its plan for preparing the DoD leadership for the impact of Year 2000 on national security in a December 8, 1998, memorandum titled, “Participation in Department of Defense and National Level Year 2000 Table Top Exercises.” This memorandum outlines exercise activities conducted at the defense and national level. The exercises expose participants to a reasonably worst case scenario induced by potential Year 2000 failures. These activities enhance participants’ understanding of potential Year 2000 impacts on national security; assist in the development of policy recommendations; provide continuing impetus to accelerate progress on fixing Year 2000 systems problems; and facilitate effective contingency planning. The four-part program, depicted in Figure 4 below, 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, including the Deputy Secretary of Defense, the State Department, the Federal Emergency Management Agency (FEMA), the President’s Year 2000 Coordinator, and congressional staffers.

- A DoD Defense/National Security game planned for August and completed before 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 the Deputy Secretary of Defense, the Vice-Chairman, Joint Chiefs of Staff, the Service Under Secretaries, the DoD CIO, 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 Year 2000 Table Top Exercise in September, which will be a White House Year 2000 office inter-agency exercise, supported jointly by DoD and FEMA.

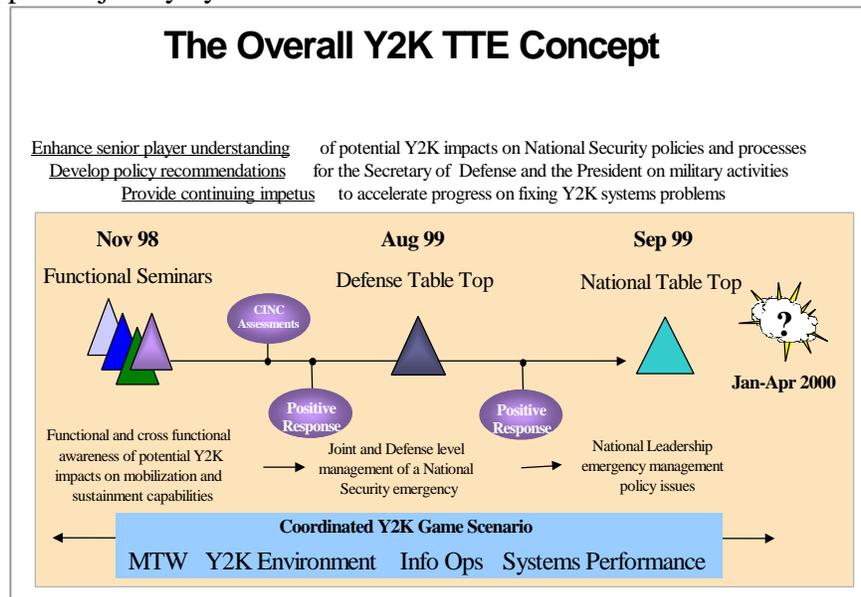


Figure 3 - Overall Year 2000 Table Top Exercise (TTE) Concept

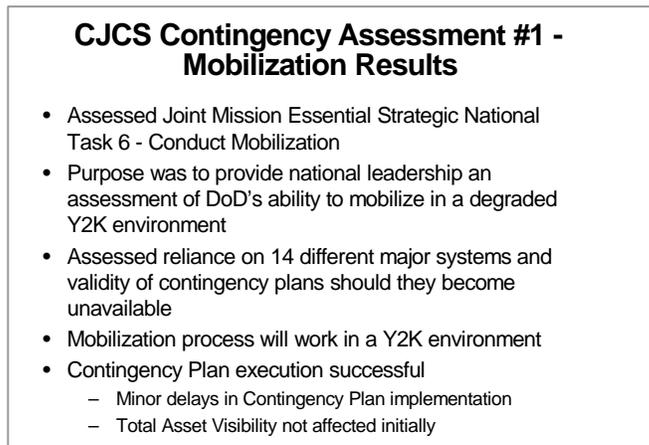
POSITIVE RESPONSE Y2K

In addition to Table Top Exercises, the 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 Year 2000 mission critical system failures. The PRY2K assesses the ability of DoD to respond with timely decisions in a Year 2000 degraded 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 Year 2000 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 Year 2000. 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 Authorities to mitigate the impact of mission critical systems failure. Results of the first contingency assessment, which dealt with mobilization, are summarized in the figure below.

Figure 4 - Chairman of the Joint Chiefs of Staff Contingency Assessment #1 Results



Consequence Management Planning

The Department of Defense has been working with other Federal agencies on consequence management and continuity of operations planning and recognizes the potential for multiple competing demands for DoD resources throughout the Year 2000 date transition period. Because of this, in January 1999, the Department conducted a high level review of its “consequence management” policies, procedures, and organizations. Actions taken after the review will ensure DoD is prepared to support a potentially increased number of requests for both domestic and international assistance, consistent with the guidance in the figure below.

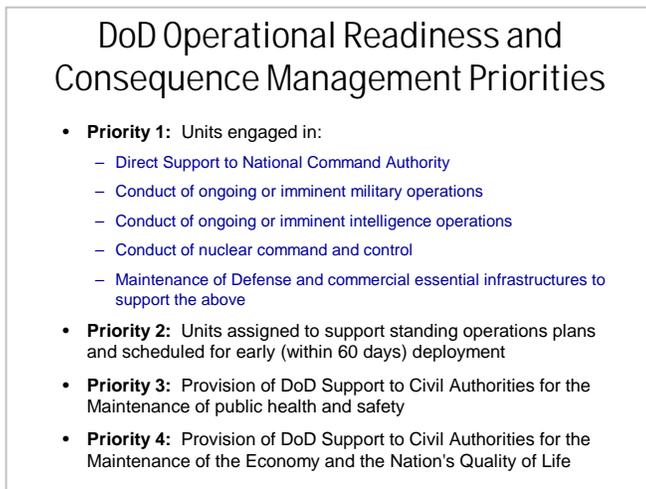


Figure 5 - DoD Operational Readiness and Consequence Management Priorities

The first priority is to ensure DoD ability to conduct ongoing or imminent support to the National Command Authority, warfighting, peacekeeping, intelligence, nuclear command and control, or critical infrastructure protection operations. Consequently, the Secretary of Defense, or his designated representative, approval is required before committing organizations and assets engaged in Priority 1 activities to support Year 2000-related requests for assistance.

Likewise, the approval of the Chairman of the Joint Chiefs of Staff, or his designated representative, is required before assets or organizations engaged in Priority 2 activities can be committed to support Year 2000 related requests for assistance.

Other units may provide support to civil authorities with first priority to maintenance of public health and safety and second priority to maintenance of the economy and the nation's quality of life.

Throughout 1999, DoD will be actively collaborating with federal agencies and organizations to further the Department's (and the Nation's) ability to develop and exercise the information flow and procedures necessary to effectively respond to Year 2000 date related events.

Conclusion

The Department of Defense will be prepared to execute its national security responsibilities before, on, and after January 1, 2000. The Department's comprehensive systems compliance efforts, operational evaluations and end-to-end testing, and systems and operational contingency plans are being developed and executed within a solid management structure. All Year 2000 efforts are receiving the personal attention of the Department's senior leadership. Finally, these efforts are being rigorously scrutinized by independent auditors, including the Department's Inspectors General and the General Accounting Office.

The Year 2000 problem is one of enormous scope and complexity for the Department of Defense, which has over one-third of the Federal Government's mission critical systems. Despite this challenge, the high percentage of systems compliance already achieved, combined with the results of end-to-end and operational evaluations already conducted and system contingency plans already tested, provides a high degree of confidence the Department will be able to execute the national military strategy unimpeded by Year 2000-related problems.