



Department of Defense
Status of Year 2000 Efforts

11th Quarterly Progress Report

Submitted to
Office of Management and Budget

November 15, 1999

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000307 108

DTIC QUALITY INSPECTED 3

DoD 11th Quarterly Report to OMB

Table of Contents

EXECUTIVE SUMMARY	iii
INTRODUCTION	2
COMPONENTS OF DoD YEAR 2000 (Y2K) PROGRAM	2
SENIOR LEADERSHIP INVOLVEMENT	2
I PROGRESS ON MISSION CRITICAL SYSTEMS.....	3
STATUS OF MISSION CRITICAL SYSTEMS	3
II OTHER PROGRESS.....	4
STATUS OF NON-MISSION CRITICAL SYSTEMS	5
STATUS OF DATA EXCHANGES	6
STATUS OF TELECOMMUNICATIONS.....	6
<i>Communication Systems Y2K Compliance Status</i>	<i>7</i>
<i>Communication Testing Overview</i>	<i>7</i>
<i>Communications Contingency Planning Operations</i>	<i>7</i>
<i>Functional End to End tests</i>	<i>8</i>
<i>Readiness Assessment Network (RAN).....</i>	<i>8</i>
<i>Public Switched Telecommunications Network (PSTN).....</i>	<i>8</i>
<i>Public Switched Telecommunications Network (PSTN)/Commercial Testing</i>	<i>9</i>
<i>Summary of DOD Communications Status</i>	<i>9</i>
<i>Defense Megacenters</i>	<i>10</i>
STATUS OF BUILDINGS.....	11
<i>Individual Buildings and Facilities: Service/Defense Agency Data.....</i>	<i>11</i>
STATUS OF BIOMEDICAL EQUIPMENT AND LABORATORY DEVICES.....	13
STATUS OF ADMINISTRATIVE AND OTHER EMBEDDED DEVICES	14
ADDITIONAL INFORMATION DEMONSTRATING DOD PROGRESS.....	16
IV HIGH IMPACT PLANS.....	17
SUMMARY OF DoD HIGH IMPACT PROGRAM STATUS	17
<i>Military Hospitals.....</i>	<i>17</i>
<i>DoD Retiree and Annuitant Pay.....</i>	<i>18</i>
V CHANGE MANAGEMENT AND VERIFICATION EFFORTS	19
STATUS OF DoD CHANGE MANAGEMENT AND VERIFICATION EFFORTS	19
<i>The DoDIG and Military Inspectors General</i>	<i>19</i>
<i>The General Accounting Office.....</i>	<i>20</i>
<i>Enterprise-wide Tools for Computer Software Code Testing.....</i>	<i>20</i>
VII BUSINESS CONTINUITY AND CONTINGENCY PLANS (BCCPS)	20
STATUS OF DoD BCCP	20
<i>Contingency Planning Oversight and Tracking</i>	<i>21</i>
STATUS OF DoD CONTINUITY OF OPERATIONS PLANNING.....	23
<i>Business Impact Analysis</i>	<i>23</i>
HOST NATION SUPPORT	25
U.S. - RUSSIAN COOPERATIVE EFFORTS.....	26
YEAR 2000 TRANSITION PERIOD/DAY ONE.....	27
LEADERSHIP PREPARATION FOR DECISION-MAKING	28
<i>CJCS Contingency Assessments</i>	<i>29</i>
<i>Table Top Exercises</i>	<i>29</i>
INFORMING THE DEPARTMENT OF DEFENSE COMMUNITY AND THE PUBLIC.....	30
VIII OTHER MANAGEMENT INFORMATION	31

DoD 11th Quarterly Report to OMB

COST ESTIMATES	31
EMERGENCY FUNDS.....	32
COST ESTIMATE CHANGES	32
KEY PERSONNEL AVAILABILITY.....	32
CONCLUSION	33
LIST OF APPENDICES	35

Appendix A	Mission Critical Systems/Mission Critical Systems to be Completed
Appendix B	Non-Mission Critical Systems/Non- Mission Critical Systems to be Completed
Appendix C	Total Systems
Appendix D	Data Interfaces
Appendix E	Embedded Devices
Appendix F	DoD Y2K Community Conversations Memo of August 18, 1999
Appendix G	DoD Limitation On Configuration Changes to Y2K-Compliant Systems of August 20,1999
Appendix H	Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
Appendix I	Security Policy for DoD Y2K Information of October 6, 1999
Appendix J	Federal High Impact Programs: DoD Military Hospitals
Appendix K	Federal High Impact Programs: DoD Retiree/Annuitant Pay
Appendix L	Independent Validation and Government-Wide Systems
Appendix M	DoD Business Continuity and Contingency Planning (BCCP) Report (Updated)
Appendix N	Cost Estimates for DoD Components
Appendix O	Summary of DoD Y2K Program and November 1999 Status

Executive Summary

DoD has made great progress since the last quarterly report (Tab C):

- **99.5% of mission critical systems are complete**, and only 8 remain to field.
- **98.6% of non-mission critical systems are complete**, and only 39 remain to field.
- All nuclear systems are **100% complete**.
- All communications systems are **100% complete**.
- All 351 logical domains in the DISA Defense Megacenters are **100% complete**.
- All DLA systems are **100% complete** and supplies for mission critical items are assured.
- All 637 DoD installations are **100% complete**.
- Both DoD Federal High Impact Programs are **100% complete**.
- **99.9% of 4.2 million embedded devices are complete** and the remaining pose no hazard.

DoD Mission Critical Systems Accounting

DoD systems represent approximately one third of all systems in the Federal government. A complete recapitulation of mission critical numbers is presented below. The 10th OMB Quarterly Report, with data as of 30 June 1999, reported that DoD had 2,414 mission critical systems using OMB accounting guidelines. Since then, the following changes have occurred:

2,414	Total DoD Mission Critical Systems on June 30, 1999:
- 41	Duplicate systems corrected when all Intelligence mission critical systems were folded into the unclassified OSD database to allow for complete tracking in one database.
- 2	Two Intelligence Systems that were scheduled to be terminated or replaced that have been reclassified to non-mission critical.
- 2	Two systems reclassified as Developmental Systems – new capability to be delivered after January 1, 2000.
= 2,369	Total DoD Mission Critical Systems on September 30, 1999
- 6	Army Mission Critical systems identified as duplicates during an audit of the database and recommended for deletion by the DoD IG.
<u>+ 4</u>	USAF developmental systems added.
= 2,367	Total Mission Critical Systems on November 8, 1999

OMB reporting includes all mission critical systems including those that will not be on the books on 1 January 2000. DoD is managing towards an active inventory of 2,101 systems that represent the active inventory to defend this nation. DoD is also managing systems in three other categories:

- Developmental systems—those systems with new capability that will be delivered after January 2000.
 - Replacement systems – those systems that will be taken out of the inventory and be replaced by one or more of the systems of the 2,101 prior to 1 January 2000.
 - Terminated systems – those systems that will be turned off by 1 January 2000.
- Thus, the accounting below shows how we reconciled the OMB and DoD numbers.

2,367	Total DoD Mission Critical Systems – OMB Accounting
- 44	Developmental systems
- 95	Replacement strategy systems
<u>- 127</u>	Termination strategy systems
= 2,101	Total Mission Critical Systems DoD will have operational on January 1, 2000

Appendix A lists each late system, an explanation, and an estimated date of completion. As of November 9, 1999, the DoD has completed all but 13 mission critical systems:

- 8 of the 2,101 systems left to complete
- 4 of the 95 left to replace
- 1 of the 127 left to terminate.

Status of Department of Defense Year 2000 Efforts: **Quarterly Progress Report**

Introduction

The information technology challenge for the Department of Defense (DoD) is the same as that facing all Federal agencies and departments. What sets DoD apart from other agencies is size and significance. The Department of Defense is the largest organization in the nation. It has over three million people – active, Guard, Reserve, and civilian employees – spread all over the world at 637 military installations and many other locations. To administer to this community it takes roughly 10,000 separate computer systems involving 1.5 million individual computers. Of these, over 2,000 systems are mission critical systems that must work for DoD to successfully execute its myriad missions. Over one-third of all mission critical computer systems in the Federal government are in the Department of Defense.

Components of DoD Year 2000 (Y2K) Program

There are four major components of the DoD Year 2000 (Y2K) Program: Systems Compliance – making sure all individual systems are Year 2000 compliant in accordance with the OMB five-phase process; Operational Evaluation/Testing – to buy increased assurance that our systems work in the real world; Contingency Planning – taking prudent precautions in case systems or capabilities become unavailable due to Year 2000 related problems; and Transition Period Operations – managing the remaining challenges and reporting and responding to Year 2000 related events.

Senior Leadership Involvement

The Department of Defense has undertaken an enormous effort to ensure Y2K readiness. A year ago in August 1998, Secretary Cohen directed DoD's leadership to treat the Y2K issue as a major threat to military readiness. The unified military commands were asked to ensure Y2K testing was included in joint warfighting and operational readiness exercises. The Services and Defense Agencies were instructed to fix their systems, certify interfaces, and ensure vendors were held responsible for Y2K compliance of products. Finally, officials on the Secretary's staff were told to ensure functioning of specific business processes, such as financial transactions, health activities, supply lines, and the like.

I Progress on Mission Critical Systems

Status of Mission Critical Systems

DoD is managing towards an active inventory of 2,101 mission critical systems that represent the active inventory to defend this nation. These are included in OMB reporting. The status of mission critical systems on November 17, 1999 is summarized in the chart below.

2,101	Total Mission Critical Systems DoD will have operational on January 1, 2000
+ 44	Developmental systems
+ 95	Replacement strategy systems
+127	Termination strategy systems
2,367	Total DoD Mission Critical Systems – OMB Accounting

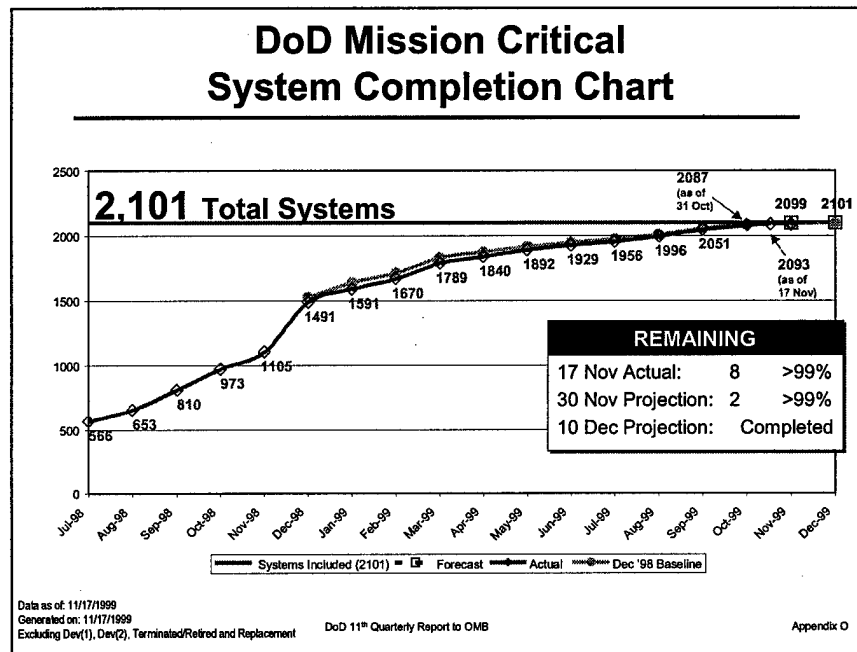
On January 1, 2000, DoD will have 2,101 mission critical systems in operation. The table below shows DoD status against both sets of systems. As of November 9, 1999, the data cut off for this report, the Department of Defense had 8 active mission critical systems to complete, and retained 5 systems slated for replacement or termination until mid-December to provide greater capability.

Category of Mission Critical Systems	Total Number	Remaining	Percentage Compliant
All Systems	2,367	13	99.5%
Developmental	-44	NA	
To be Replaced	-95	-4	95.8%
To be Terminated	-127	-1	99.2%
In Operation on January 1, 2000	2,101	8	99.6%

The DoD uses the group of 2,101 systems to track Y2K progress in monthly Y2K Steering Committee meetings chaired by the Deputy Secretary of Defense. A graphical portrayal of DoD's progress on systems compliance is shown below.

DoD 11th Quarterly Report to OMB

The status of mission critical systems (OMB Accounting) is summarized below.



Mission Critical Systems	Number Compliant	Number to be Replaced	Number to be Repaired	Number to be Retired
2,367	2,354 (99.5%)	4	8	1

Information on mission critical systems, including a list and description of the mission critical systems to be completed, is at Appendix A. Senior leadership actively manages the progress of these mission critical systems. The senior Service leaders receive daily reports. Principal Staff Assistants direct the progress of these efforts on a weekly basis. The Deputy Secretary of Defense chairs a monthly Year 2000 meeting to address issues that cut across several organizations within the DoD or require DoD collaboration with other Federal agencies, and with military counterparts among our Allies and Partners.

II Other Progress

- A. Provide a description of progress to make non-mission critical systems compliant, including measures that demonstrate that progress.

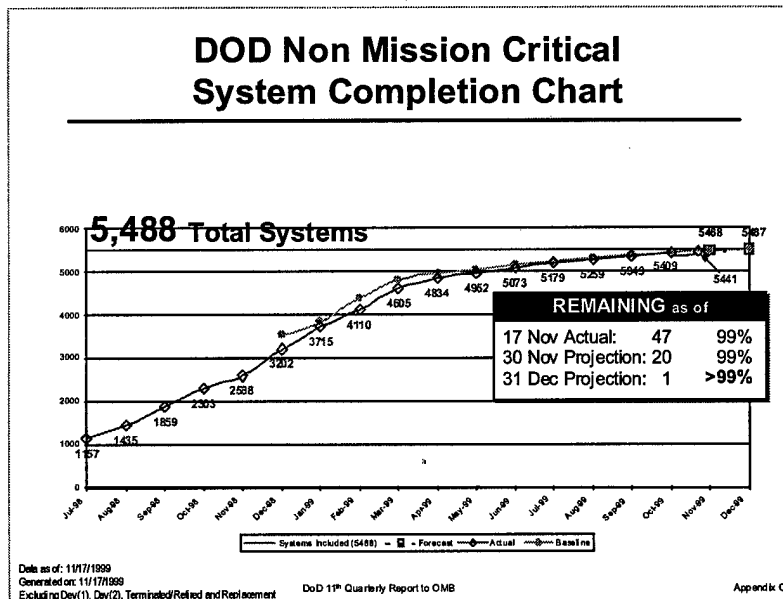
Status of Non-Mission Critical Systems

DoD is managing towards an active inventory of 5,488 non-mission critical systems that represent the active inventory to defend this nation. These are included in OMB reporting. The status of non-mission critical systems on November 17, 1999 is summarized in the chart below.

5,488	Total Non-mission Critical Systems DoD will have operational on January 1, 2000
+ 190	Developmental systems
+ 412	Replacement strategy systems
+1,177	Termination strategy systems
7,267	Total DoD Non-mission Critical Systems – OMB Accounting

The DoD tracks 5,488 non-mission critical systems that will be in operation on January 1, 2000 to chart Y2K progress in monthly Y2K Steering Committee meetings chaired by the Deputy Secretary of Defense. A graphical portrayal of DoD's progress on non-mission critical systems compliance is shown below.

The status of non-mission critical systems (OMB Accounting) on November 17, 1999 is summarized in the chart below.



Non-Mission Critical Systems	Number Compliant	Number to be Replaced	Number to be Repaired	Number to be Retired
7,267	7,166 (98.6%)	41	39	21

DoD 11th Quarterly Report to OMB

A detailed spreadsheet and a list of each non-mission critical system remaining to complete are at Appendix B. Summary data on the total of all DoD systems is at Appendix C.

One non-mission critical system used to measure the length of engine stator blades after engine teardown at the Engine Regional Repair Center, Laughlin Air Force Base, Texas, will not be ready until June 2000. This new system replaces the functionality of an older system. The DoD leadership is well aware of this schedule and supports the management decisions regarding this system. There is absolutely no mission impact.

- B. Provide a description of progress to make data exchanges compliant with all entities external to your agency.**

Status of Data Exchanges

DoD has led a sustained effort to identify, describe, and conclude memoranda of agreement (MOAs) with data exchange partners. DoD has included interface information as part of its contractual requirements with suppliers and in other legal contracts. Detailed information on DoD data interfaces is found at Appendix D.

In addition to the information on data exchanges in the DoD Y2K database, GSA maintains a database of data exchanges among Federal, State, and local government systems. The DoD data exchanges in the GSA database are primarily financial systems. After a lengthy effort on the part of the Defense Finance and Accounting Service, all DoD data exchanges with the States in the GSA database are **100 percent complete**. All are "Federal Ready," and they have been tested with the States. Moreover, the data exchanges have been successfully re-tested using the recent "S" format change issued by the Social Security Administration. This is a significant achievement.

- C. Provide a summary description of progress in assuring that telecommunications systems used by your agency are compliant, regardless of whether they are owned or managed by you, by GSA, or by some other entity. Indicate when you expect that these telecommunications systems will be compliant and describe any difficulties you are encountering in keeping to your schedule.**

Status of Telecommunications

The main purpose of DOD communications is to ensure the functions of critical voice, data, messaging, imagery, and video services are available as required to support the primary missions of the DOD Services and Agencies. The functional area of communications includes long-haul communications systems, base communications systems, strategic, and deployed/afloat tactical communications systems.

DoD 11th Quarterly Report to OMB

Communications systems are the key enablers that allow operational forces to complete their missions. Each CINC has specific communications requirements, as numerous organizations continuously and simultaneously perform multiple missions that rely on communications systems.

Communication Systems Y2K Compliance Status

There have been a total of 481 Communications Systems that have been reported into the OSD Y2K Database. Out of the 481, 286 are mission critical and 195 are non-mission critical. **All communications systems are 100% complete.** System compliance processes are based on strategies described in the Department of Defense Year 2000 Management Plan as well as action and management plans developed by the individual Services and Agencies. These define the processes, responsibilities, and actions necessary to ensure continued operations during Year 2000 (Y2K) transition periods.

Communication Testing Overview

Communication systems' testing was done at three levels. First, the Services, and Agencies completed integration testing of strings of network and systems needed to perform mission tasks. An example of service level testing were the Battle Group System Integration Test (BGSIT) tests performed by the Navy that included the key communication systems. The second type of testing consisted of an extensive series of functional end to end tests of enterprise-wide communication systems. These enterprise communications include systems that are used by the CINCs and Services to communicate across CINC, Service, Agency, and geographic boundaries. Enterprise systems included the various components of the DISN and related satellite systems. The third type of testing was the CINC sponsored OPEVALs and the Joint Users Switch Exercise (JUSE). The CINCs identified critical "Thin Line" communication systems as part of the Major Theater of War systems need to perform critical wartime/crisis mission functions.

Communications Contingency Planning Operations

System Contingency Plans provide processes and procedures for restoring functionality to a disrupted system or component thought to be Y2K compliant. System contingency planning is the Program Manager's (i. e., Executive Agent's) responsibility. System Contingency Plans map directly to at least one Operational Contingency Plan (OCP) to ensure that in the event the system experiences a Y2K disruption, an alternative system or procedure is available in order to continue the mission until the disrupted system is restored. Contingency Planning is a risk management strategy to handle the occurrence of problems caused by the Y2K year end and leap year date changes. Given the complexities of these systems, their interfaces, and the immovable Y2K deadline, error free compliance of all systems may not occur. Y2K OCPs provide alternative

DoD 11th Quarterly Report to OMB

communication systems or procedures to continue missions/functions, in the event of degradation.

Functional End to End tests

DISA conducted extensive end to end tests of enterprise wide communication systems at the Joint Interoperability Test Center (JITC), plus numerous tests done in conjunction with CINC OPEVALs. The largest functional end to end test for communications was the JUSE. JUSE tested a vast array of communication systems including the Nonsecure and Secure Internet Protocol Router Network (NIPRNET/SIPRNET), Defense Red Switch Network (DRSN), DSCS satellite system, Defense Message system (DMS), Automated Digital Network (AUTODIN), and interfaces to the to Public Switched Telephone Network (PSTN). JUSE encompassed over 30 total force organizations utilizing over 600 people for a period of 26 days on a 24/7 basis interfacing to 54 separate systems. The JUSE 99-Y2K network architecture was designed to represent what would be found in support of a Joint Task Force/Joint Special Operations Task Force.

Readiness Assessment Network (RAN)

Enterprise-wide communication networks support thousands of operational users all over the world. However, it is difficult and risky to roll the clocks on part of the network while other users are still operating in the current year mode. To address this problem, ASD(C3I) established a Readiness Assessment Network (RAN) to support communication testing. This concept of a RAN protects the operational networks/databases and provides the most accurate replication of the DISN components of each thin-line. It allows components to roll dates synchronized with the other thin-line components being evaluated and tested. The RAN consisted of operational systems that were disconnected from the network as well as hardware and software that were identical to operational systems in the field. The Joint Interoperability Test Center (JITC) was the key location for the government unique systems, and Telcordia was the key location for the public network portion. The RAN supported functional end to end testing and selected OPEVALs.

Public Switched Telecommunications Network (PSTN)

DOD relies heavily on the public telecommunication transport infrastructure to provide much of the terrestrial connectivity for both tactical and administrative communications, including Government Emergency Telecommunications Service (GETS). GETS is a service provided to the government by the telecommunication industry to give priority telecommunications capability in the event of emergency. The DOD approach to public switched network (PSTN) Y2K testing had three parts. First, DOD participated and monitored ongoing PSTN testing being done by industry. Second,

DoD 11th Quarterly Report to OMB

DOD replicated part of the PSTN at Telcordia to test the interface between the PSTN and government unique telecommunications systems. Finally, DOD has conducted a risk analysis of telecommunication services for DOD forces and bases overseas.

Public Switched Telecommunications Network (PSTN)/Commercial Testing

Numerous public telecommunication providers have developed tests to ensure the availability of the public telecommunications network in the Year 2000. The National Reliability and Interoperability Council (NRIC), and the Alliance for Telecommunications Industry Solutions (ATIS) are commercial telecommunication provider organizations that have conducted public telecommunication Y2K testing. DOD representatives observed some of these tests and participated in others as DOD systems successfully completed all functions. DOD and the Manager of the National Communication System participated in the Federal Sector Group meetings and assessed our role in the functional testing. Industry conducted extensive testing across the PSTN in CONUS and overseas interconnections including testing GETS functionality.

Public Switched Telecommunications Network (PSTN) to DOD Interface

The RAN described earlier was also used to test the interface between military unique systems with the PSTN, as well as the use of the PSTN as a transport system for DOD data. No Y2K anomalies were found with the DOD to PSTN or PSTN transport part of the testing.

Public Switched Telecommunications Network (PSTN) Overseas

DOD depends on host nation telecommunication systems for some of its communications on and off base at overseas locations. However, DOD is not able to test overseas public infrastructure. Therefore, ASD (C3I) conducted a study of the risks associated with providing telecommunications to the DOD in 28 countries around the world that have a large DOD presence. The risk analysis looked at the Y2K remediation efforts in these countries and determined which countries presented a risk of Y2K related telecommunications failures. The results of the risk analysis were provided to the CINCs to use in preparation of contingency plans.

Summary of DOD Communications Status

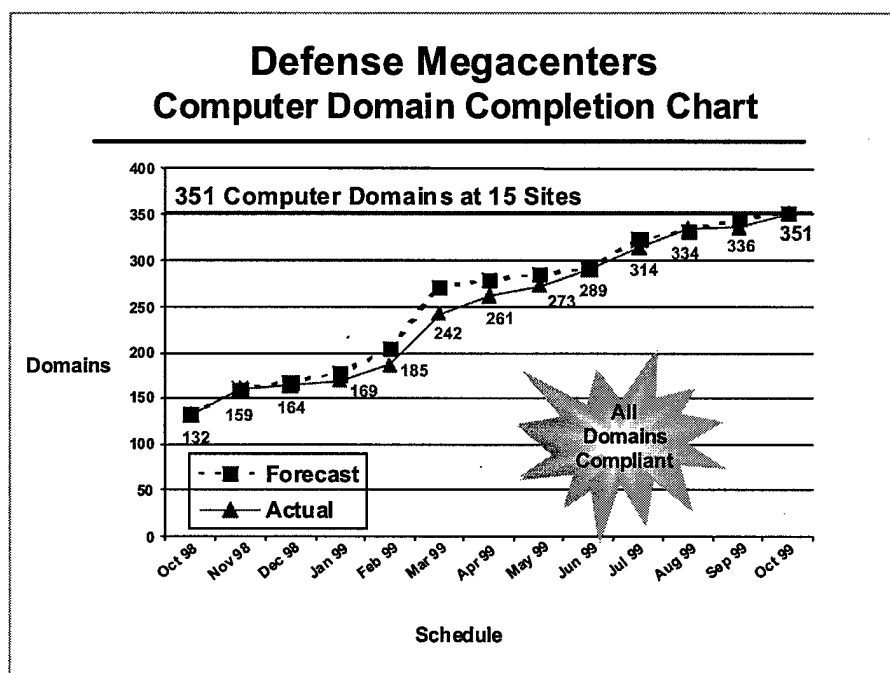
The Department of Defense is very confident that its systems will perform as designed during and after the rollover. In addition, contingency plans are in place and ready to go for mission critical systems in the event of a failure. Furthermore, Military communication planning always provides for built in redundancy and back up communication paths for key missions. Network operation centers such as DISA's

DoD 11th Quarterly Report to OMB

Global Network Operations Center (GNOSC) operate on a 7 by 24 basis, react to communication outages on a routine basis, and are well equipped to handle any unforeseen telecommunications problems that may occur. The GNOSC is tied in to CINC and National Command Centers to respond to any local or global communications problems.

Defense Megacenters

The Defense Information System Agency (DISA) Defense Megacenters (DMCs) are centralized computer centers located throughout the United States which provide all tiers of computer processing capability for the Department's Services and Agencies, including processing most of the Department's business functions. As of October 31, 1999, all of the 351 computer domains at the 15 DISA computer centers have been completed and are now Y2K compliant. This is a significant achievement because DISA was faced with the twin challenges of Quadrennial Defense Review-directed workload consolidation, migration and downsizing plus remediation and coordination with its Service and Agency customers to achieve this massive Y2K compliance effort.



- D. Provide a summary description of efforts to assure that buildings and related systems, such as heating, air conditioning, and security systems are compliant, regardless of whether they are owned or managed by you, by GSA, or by some other entity. Indicate when you expect buildings and related systems that your agency uses will be compliant and describe any difficulties you are encountering in keeping to your schedule.

Status of Buildings

The Department of Defense is responsible for 637 installations worldwide. All are now compliant. This achievement was the result of a global effort to ascertain, remediate, and test a challenging variety of infrastructure systems. Most of these installations are comparable to small towns and incorporate buildings housing industrial, commercial, and residential functions within their perimeters. Additionally, DoD has many independent buildings. Given the quantity, diversity, and global reach of DoD-occupied real estate, DoD used a multi-pronged approach for oversight of its Year 2000 compliance, involving the GSA and Washington Headquarters Service (WHS) Real Estate and Facilities Division (RE&F), the Office of the Under Secretary of Defense (Acquisition & Technology) (Installations), the Major Commands of the Services, the Defense Agencies, and the CINCs. The efforts of these organizations are discussed below.

Individual Buildings and Facilities: Service/Defense Agency Data

The National Capital Region

DoD also operates from many separate facilities, particularly in the National Capital Region (NCR). DoD occupies 148 buildings in the National Capital Region, under a variety of contracts and responsible organizations. DoD has relied upon the General Services Administration efforts, and commercial building information, to certify the separate buildings as compliant. The types and status of these buildings are summarized below.

The National Capital Region

Buildings in NCR Area	Responsible Organization	Compliance
Govt Owned RE&F Mgd	WHS	5 of 5
Govt Owned GSA Mgd	GSA	12 of 12
Leased Buildings	Army Corps of Engineers	5 of 5
Leased Buildings	WHS	29 of 29
Leased Buildings	GSA	66 of 96
	Total	118 of 148

- All government-owned DoD buildings are Y2K compliant.
- All leased buildings managed by the Army Corps of Engineers are Y2K ready.
- All leased buildings for which Washington Headquarters Service is responsible in the National Capital Region are "Y2K ready."

DoD 11th Quarterly Report to OMB

- The building lessors have been advised by their legal counsel not to certify the buildings as "Y2K compliant," but instead typically use the term "Y2K ready." The connotation is that the buildings can be operated manually, and that the lessors have contingency plans. Their legal obligation is to provide a functioning building.
- There are 30 leased buildings still listed as non-compliant in the database. These buildings are managed by GSA but include DoD tenants. DoD has contacted GSA to determine if there will be any operational impact on DoD tenants and prepare accordingly.

The Pentagon

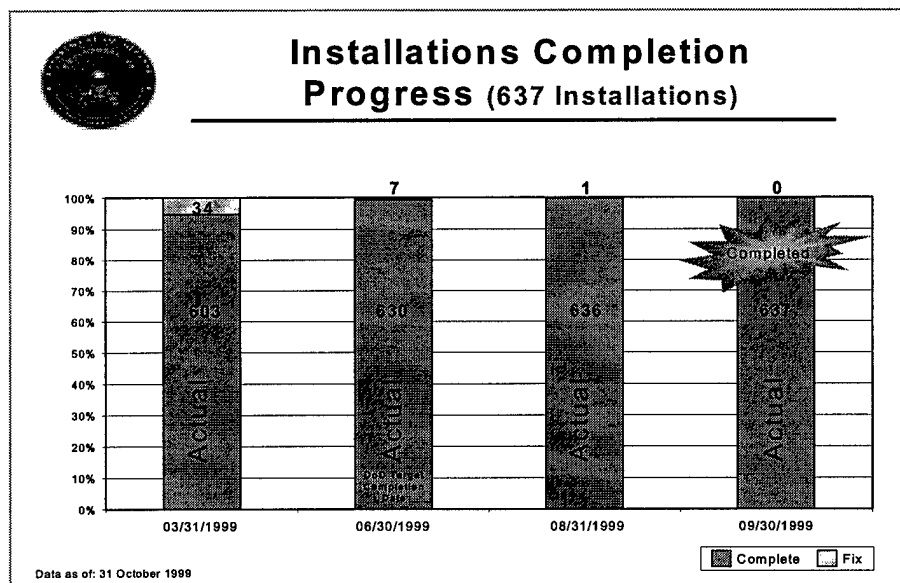
The Pentagon is Y2K compliant now and will be ready on January 1, 2000. All systems are Y2K compliant, and most major infrastructure systems also have backup systems available. The Pentagon has a backup power feed line and backup generators for command centers, the sewage station, and life and safety lights. The Pentagon air conditioning is Y2K compliant, and the building has back up generators for boilers if required. Alarms and smoke detectors are compliant. A new Y2K compliant police radio system is installed and tested. Additionally, the new telephone system is Y2K compliant. The last subsystem, the Operator Attended Switchboard, has been installed, and operator training is underway at this time. Secure telephone units are Y2K compliant, and Bell Atlantic has certified that their support is Y2K compliant.

DoD Installations

The DoD has assets at 637 installations and facilities worldwide of varying size. Most installations are comparable to small towns or cities containing industrial, commercial and residential buildings and related infrastructure. Using a five-metric standard, the Military Departments worked through their Major Commands with their installation commanders to fix and test the major "inside-the-gate" infrastructures. The Services and DLA have certified all installations as Y2K compliant.

Most military installations are not self-sufficient. Although many installations have backup generators for outages of limited duration, they rely primarily on local utilities. The DoD has made significant progress to confirm the Y2K status of local utilities, on which its installations depend and to ensure contingency plans account for temporary, localized outages in locations where compliance has not yet been confirmed. DoD has worked closely with the "outside-the-fence" utilities that supply energy and water to installations. The United States energy generation and distribution grid infrastructures have been fixed and tested. They have declared themselves to be ready by January 1, 2000.

However, the ability to perform our missions overseas was questioned because less was known about foreign utility infrastructure. Significant work was done overseas to ensure that the Commanders-In Chief (CINCs) could operate effectively. The host nation support status for overseas installations has been examined closely by a federal government International Working Group (IWG). Based on its efforts, the IWG has increased the CINCs and overseas base commanders' level of confidence to receive host nation support.



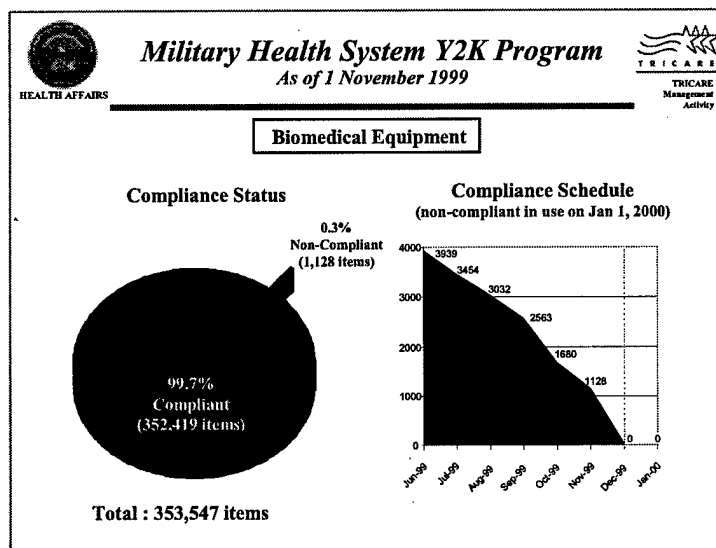
- E. Provide a summary description of progress to assure that other systems or equipment, including biomedical equipment and laboratory devices and any other products or devices using embedded chips that your agency uses are compliant. Describe any difficulties you are encountering in ensuring that such equipment is compliant.**

Status of Biomedical Equipment and Laboratory Devices

The Military Health System (MHS) has met all of its milestones toward Y2K readiness. As part of its effort to ensure that military beneficiaries receive world class healthcare at home and abroad, a comprehensive review of all 353,547 items of biomedical equipment and laboratory devices utilized throughout the MHS was undertaken. As of November 1, 1999, over 99.7 percent of biomedical equipment and laboratory devices were Y2K compliant. All biomedical equipment and laboratory devices that will be required on January 1, 2000 have been fixed. The remaining non-compliant devices have been retained for additional capability until November 30, 1999, when they must be turned in for appropriate disposal.

DoD 11th Quarterly Report to OMB

The Military Treatment Facility (MTF) commanders have certified that sites will complete remediation by November 30, 1999. Contingency plans are in place for all biomedical devices. Each MTF has trained qualified personnel to execute their contingency plans in the event of an unanticipated failure.



Compliant	Non-compliant	Total
352,419	1,128*	353,547

*** Please note:** Some non-compliant biomedical equipment has been retained in use for additional capability until November 30, 1999, the DoD deadline for disposal of non-compliant biomedical equipment. As of December 1, 1999, all non-compliant biomedical equipment will be terminated and disposed of properly.

More detailed information on embedded devices may be found at Appendix E.

Status of Administrative and Other Embedded Devices

DoD has a record number of 4,221,565 embedded devices and has replaced everything that is significant and required to accomplish DoD's mission, resulting in 99.9% compliance. The remaining non-compliant devices have no operational impact and pose no safety hazard; therefore they have been deliberately retained as a matter of sound management practice and good stewardship of the taxpayer funds. For example,

DoD 11th Quarterly Report to OMB

Army Recruiting Command correctly decided not to replace the 2,020 non-compliant fax machines located at recruiting stations. The machines still work but simply print the wrong date on the header. Many organizations decided to retain stand alone PCs that aren't compliant, but whose function is not affected by having an incorrect system date and terminate them in accordance with scheduled modernization.

Items commonly containing embedded devices are summarized in the "Embedded Devices spreadsheet found in Appendix E. These embedded devices are divided into three major categories: personal computers, communications hardware, and facilities and others. The items in each major category are described below.

Personal Computers

Most are 486 model personal computers or laptops.

Communications Hardware

All of the mission critical and mission essential communication hardware has been replaced. A few items that have been determined to have no operational impact have been deliberately retained in the inventory as a matter of sound management practice and good stewardship of the taxpayer funds.

Facilities and Others

Items with embedded devices listed under the "Facilities and Others" column of Appendix E include things such as copiers, bar code readers, cash registers, scanners, video recorders, fax machines, telephones, mail sorters, truck scales, and parking access control. Again, utility and safety were the criteria for any decision to retain an item with a non-Y2K compliant embedded device. All retained devices are fully operational and safe but may require manual re-setting of the correct date. The remaining non-compliant devices have no operational impact and pose no safety hazard; therefore they have been deliberately retained as a matter of sound management practice and good stewardship of the taxpayer funds.

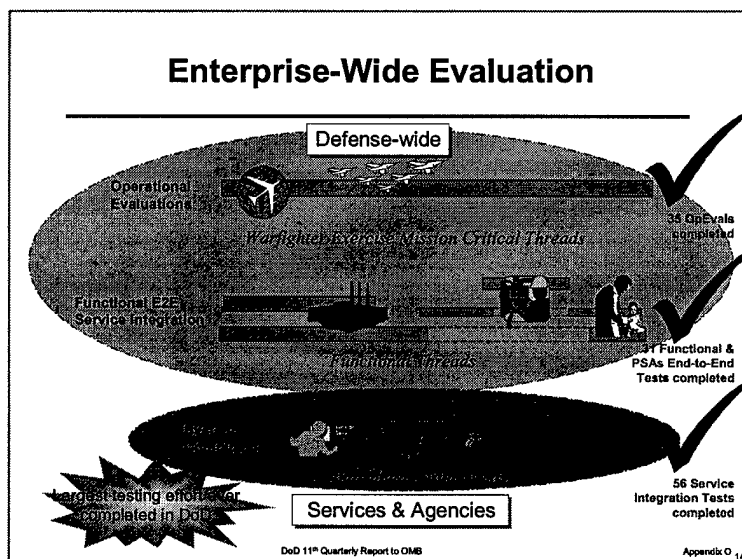
The number of non-compliant devices reported by the Department of Defense reflects the cumulative best judgement of every DoD Installation Commander given the level of mission risk and resources available. While DoD constituents continue to work to achieve 100% compliance, the number of non-compliant devices which remain represents negligible risk to DoD overall mission accomplishment. All DoD installations are Y2K compliant, meaning that every Installation Commander has fixed Y2K vulnerable devices/systems where necessary, tested them where practical, and conducted installation-wide Y2K testing of essential base services required to support key missions. Installation testing also included exercising contingency plans and continuity of operations plans to validate their executability and appropriateness. In addition, every Major Command has certified that all subordinate activities (in addition to installations) have completed the prescribed Y2K remediation process and certified they are mission ready. When taken in full context, DoD must trust the best judgement of those in command.

F. Please include any additional information that demonstrates your agency's progress.

Additional Information Demonstrating DoD Progress

DoD has been very proactive in issuing policies intended to support the transition period for Y2K Operations.

- The Secretary of Defense signed a policy memorandum, "DoD Year 2000 Community Conversations," to provide information and assistance regarding Y2K compliance efforts to military members, their families and neighboring civilian communities surrounding the DoD installations (Appendix F).
- DoD issued a critical policy statement, "Limitation on Configuration Changes to Y2K-Compliant Systems," on August 20, 1999 to prevent jeopardizing systems' compliance by further modifications. This policy gave the final decision making power to the CINCs to ensure that operational needs were weighed against other risks. (Appendix G).
- Y2K is closely linked to Information Assurance, and the Year 2000 rollover might be perceived by cyber terrorists as a period of increased vulnerability. As part of a multi-step program to increase the readiness posture for Information Warfare, the Assistant Secretary of Defense (C3I) formulated a policy to increase the security of the DoD unclassified network (Appendix H).
- Finally, the Under Secretary of Defense (Policy) clarified guidelines specifically for sensitive Year 2000 information (Appendix I).



DoD 11th Quarterly Report to OMB

- In addition, DoD has conducted 122 successful End-to-End tests demonstrating the Department's ability to conduct its mission.

IV High Impact Plans.

- A. For each of the 43 high impact programs for which your agency is the lead, as listed in Attachment C, provide:

Summary of DoD High Impact Program Status

Two Department of Defense programs are listed as Federal High Impact Programs: Military Hospitals and Retiree/Annuitant Pay.

 Federal High Impact Programs 100% Complete 		
CRITERIA	MILITARY HOSPITALS	RETIREE - ANNUITANT PAY
System Compliance	✓ 100% complete	✓ 100% complete
End-to-End Testing	✓ 100% complete	✓ 100% complete
Contingency Planning	✓ 100% complete ✓ All contingency plans tested	✓ 100% complete ✓ All contingency plans tested
Data Exchanges	✓ 100% complete	✓ 100% complete
Informing the Public	✓ 100% on track ✓ Recent Press Release (30 Sept)	✓ 100% on track ✓ Mail out to all retirees and annuitants ✓ Recent Press release (14 Oct)

Military Hospitals

The Military Health System (MHS) and its military hospitals have met all of the milestones toward Year 2000 readiness. The MHS's Year 2000 Program has overseen the validation of all systems and development of contingency plans. We are confident that military beneficiaries will receive world class health care at home and abroad through the transition to the Year 2000. A summary of the major MHS Y2K milestones and readiness is provided below. Appendix J provides a comprehensive table identifying accomplished MHS Y2K milestone activities and continuing communications initiatives.

- All MHS systems are Y2K compliant.
- All hospital computer networks are Y2K compliant.
- All systems have contingency plans in place. An independent validation and verification contractor has reviewed and approved each plan.

DoD 11th Quarterly Report to OMB

- End-to-end testing of MHS mission critical functions is complete. These tests included extensive interface testing with MHS managed care as well as medical supply partners. Both GAO and the DoD IG have audited the MHS end-to-end process and have produced favorable reports on the effectiveness of the tests.
- All military hospitals and clinics have continuity of operations plans in place.
- All MHS Managed Care Support Contractor partners have provided letters of assurance that they will continue to provide all services throughout the transition to the Year 2000.
- Over 50 articles, news releases, interviews, posters, and pamphlets have been published to assure our beneficiaries and the public that the MHS is ready for Y2K.
- The status of the Military Hospitals is detailed in Appendix J.

DoD Retiree and Annuitant Pay

DoD is dedicated to ensure that every retiree and annuitant will receive accurate, efficient, and courteous service before, during, and after January 1, 2000. The Defense Finance and Accounting Service (DFAS) has taken the following measures to ensure that retirees and annuitants will receive the same standard of pay in the Year 2000:

Systems Compliance – 100% complete.

- The Retiree/Annuitant System (DRAS) is certified 100% compliant.

Contingency Plans – 100% complete.

- The systems have extensive and detailed contingency plans, and those plans have been exercised at each location by September 30, 1999.
- Contingency Plans for DRAS-APS and RCP are established and have been tested.

End-to-End Testing – 100% complete.

- The systems have completed end-to-end testing with independent verification of all testing on or before September 30, 1999.

Interface Agreements – 100% complete.

- All DFAS interface agreements have been signed.

Interface Testing – 100% complete.

- Multiple interface testing has been completed with all critical interface partners such as the Federal Reserve Banks, IRS, Social Security, Services, and other DoD Agencies.

Independent Verification and Validation – 100% complete.

- DRAS-RCP, Retiree application was certified as Y2K compliant on April 9, 1999.

DoD 11th Quarterly Report to OMB

- An independent validation and verification contractor has reviewed and approved each plan.
- Both GAO and the DoDIG have audited the end-to-end process and have produced favorable reports on the effectiveness of the tests.

Informing our Beneficiaries – 100% complete.

- In addition to informative articles in base newspapers, on Armed Forces Radio/Television, and posted on installations, DFAS has a well-regarded website.
- It has issued several press releases and a mailing of individual notices to all retirees and annuitants with their annual statements.

The status of program to ensure prompt and reliable payment to all DoD retirees and annuitants is specified in Appendix K.

V Change Management and Verification Efforts

- A. Describe how and to what extent internal performance reports, (i.e., compliance of systems repaired and replaced) are independently verified. Provide a brief description of activities to assure independent verification that systems are fixed and to assure that information reported is accurate. Also identify who is providing verification services (for example, Inspectors General or contractors).**

Status of DoD Change Management and Verification Efforts

The DoD Y2K management plan provides guidance on independent verification and validation (IV&V) of system Y2K compliance. A mix of independent contractors, Inspectors General, other internal audit agencies, and the Government Accounting Office conducted these IV&V efforts. In addition to the IV&V conducted as part of Y2K systems compliance, operational testing is also audited, as described in subsection C below. Another aspect of IV&V activities is the independent screening of computer software using enterprise-wide tools, as described in the 9th Quarterly Report. Systems validation efforts are detailed at Appendix L.

The DoDIG and Military Inspectors General

The Office of the Assistant Inspector General for Auditing, DoD, in accordance with an informal partnership with the Chief Information Officer, provides substantial support to the effective oversight of the DoD Y2K program. Since its initial Y2K audit efforts in 1997, the DoDIG has completed 136 Y2K audits and has 39 audits ongoing. To provide that level of support, the DoDIG devoted over 180 staff years, or more than 30 percent of its audit staff, to Y2K audits during FY 1999. Staff costs for Y2K audits during FY 1998 and FY 1999 exceeded \$16 million.

DoD 11th Quarterly Report to OMB

The Service Inspectors General similarly provide independent assessments of DoD Y2K compliance management and implementation. The Services have made Year 2000 efforts a special inspection item.

The General Accounting Office

GAO auditors have played a similar function in advising the senior leadership where they might improve their efforts. The DoD has followed GAO's guides and templates for each phase of remediation as well as GAO guides for contingency planning and the most recent GAO publication on Day One Planning.

Enterprise-wide Tools for Computer Software Code Testing

The Department has purchased tools to aid in Y2K renovation and testing that have proven to be not only cost effective, but also a critical part of the DoD risk mitigation effort. These tools are industrial-strength quality assurance and test support software useful in Y2K compliance testing, code analysis, regression testing, and code quality assessment. As a risk reduction measure, the military departments Intelligence Community, and Defense Agencies are screening large amounts of these computer codes with multiple tools. This has turned out to be a very effective final screening effort.

VII Business Continuity and Contingency Plans (BCCPs)

Provide information on progress in developing and testing BCCPs in your agency. Include:

- A. Assurance that local and regional offices have developed and tested business continuity and contingency plans in coordination with headquarters. Also provide the total number of such offices which require BCCPs and the number that have such plans in place.**

Status of DoD BCCP

The DoD does contingency planning all the time for military operations and for its business functions. Consequently, the Department was well prepared for the BCCP requirements generated by the Year 2000 problem. More detailed information may be found in the updated DoD BCCP at Appendix M. The mission critical systems in DoD have system contingency plans in place and are being rehearsed and refined and reviewed by external and internal auditors. The Chairman of the Joint Chiefs of Staff conducted a series of "Contingency Assessments" to determine whether key warfighting tasks could be accomplished if key systems became unavailable. These exercises involved all facets of the Department and were a critical element in evaluating the feasibility of contingency plans for major warfighting support functions. The Department conducted a series of Table Top Exercises for senior leaders, including participation in a National level TTE in September. The TTE prepared senior leaders for possible policy decisions that might be

DoD 11th Quarterly Report to OMB

generated by Year 2000 related problems.

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 was published by the OASD(C3I)Y2K Office to assist in the process of determining local risks, based on the infrastructure supporting each site.

Contingency Planning Oversight and Tracking

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

DoD conducted 5 Y2K Contingency Planning workshops in the past year addressing essentials of Business Continuity and Contingency Planning (BCCP) development and implementation.

- Workshop 1 was used to determine the adequacy, scope and content of DoD Y2K Operational Contingency Plans. The workshop outlined for DoD Contingency Planners the essentials needed in a good System or Operational Contingency Plan.
- Workshop 2 addressed critical infrastructure assumptions necessary to bound BCCP resources and responsibilities. The workshop focused on both CONUS and OCONUS infrastructure assessments needed to define a realistic worst case scenario for which to build and exercise contingency plans.
- Workshop 3 addressed oversight responsibilities—Due Diligence—from the Secretary of Defense to the private in the foxhole. The DoD IG Audit team participated in workshop 3 providing their audit approach for Y2K plans.
- Workshop 4 in the CONUS series addressed Date Transition Strategy and Personal Preparedness during a collaborative GroupWare session. DoD Components were given the opportunity to share their Best Practices and Lessons Learned so those plans needing completion could be finalized and exercised having had the benefit of others' experiences. This "Homestretch" workshop (WS4) emphasized remaining contingency planning necessary to maximize our readiness for the Y2K rollover event.
- An OCONUS BCCP awareness workshop was held at a combined NATO/SFOR Operations meeting where the DoD provided templates to our

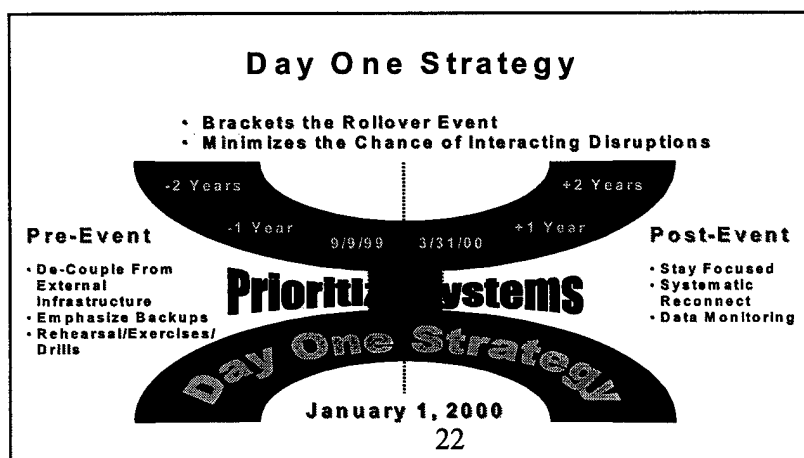
DoD 11th Quarterly Report to OMB

allies and coalition forces to assist in preparing mission critical risk assessments and impact analysis in order to enhance their BCCP process. BCCP materials were presented from the viewpoint of a NATO Planner in order to rate the level of vulnerability and consequences if a disruption were to occur. The ultimate benefit to NATO planning was increased awareness and readiness and an approach for mapping interdependencies.

In addition to BCCP workshops for contingency planners, BCCP presentations were made an integral part of two highly successful 3-day Y2K technical conferences sponsored by the DoD Y2K Office and the National Defense Industrial Association. Numerous other BCCP presentations were given throughout the year in response to requests for support. These varied from internal DoD organizations like the DISA Central Design Activity to external presentations to Mr. Joseph Connor, Under Secretary General of the United Nations.

During the summer months of 1999, parallel to and in support of the President's Council on Year 2000 Conversion, DoD launched a program of Community Conversations to promote awareness of local issues and encourage proactive contingency planning. The Department of Defense implemented this concept across all Services with a continuing effort planned through the end of 1999 to raise community awareness for day one planning and personal preparedness. Major installations have hosted many events engaging civic leaders and the general populace in open dialogue. The materials and guidance provided by OASD (C3I) promulgated a common and consistent message across the Services to coincide with that of the President's Council. Materials for Community Conversations and other Y2K BCCP items of interest can be downloaded from the DoD Y2K Contingency Planning web site located at http://www.c3i.osd.mil/org/cio/y2k/y2k_con_plan/index.html.

In conjunction with DoD's Community Conversations a "Personal Preparedness for Y2K" brochure was developed to address Y2K planning factors for military and civilian personnel. Having read and completed the brochure's enclosed checklist, deployed military personnel will feel confident that their families will be able to cope with any disruptions, however unlikely, enabling them to focus their full attention on the nation's military strategy. DoD has distributed 500,000 personal preparedness brochures at Commissaries, Post Exchanges, and has prepared a personal preparedness message insert for Leave and Earning Statements.



B. Describe how your agency is coordinating its BCCP with its Continuity of Operations (COOP) planning efforts.

Status of DoD Continuity of Operations Planning

The DoD approach to BCCP is to provide centralized policy guidance with DoD components developing appropriate plans based on that guidance and executing them appropriately. While some planning assumptions have changed for individual plans, the overall BCCP guidance remains valid and accurate as published earlier. With respect to Day One planning and activities, DoD is well tested and positioned in terms of preparation, monitoring and response activities as outlined in GAO publication, "Y2K Computing Challenge: Day One Planning and Operations Guide" (October 1999). The updated DoD BCCP at Appendix M addresses Day One Planning.

Business Impact Analysis

Impact Analysis was performed using operational risk analysis procedures standard for all DoD planning processes. Extremely long and complex information chains characterize most DoD missions. 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; and
- **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.

DoD 11th Quarterly Report to OMB

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

DoD 11th Quarterly Report to OMB

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 was planned and conducted 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.

During the past several months, the OSD Y2K Outreach Office has coordinated Department of Defense (DoD) efforts in two principal areas of international Y2K work. One area focused on determining the ability of host nations to provide critical infrastructure support services during the Y2K transition to DoD and other U.S. Government (USG) facilities and operations. The other area was dedicated toward continued work on a comprehensive five-pillar program with Russia to address mutual Y2K related national security concerns.

Host Nation Support

The OSD Y2K Outreach program was designed to supplement the extensive work of the Joint Staff, Service components, and defense organizations to address Y2K issues and ensure DoD could continue operations during the Y2K transition period. In many cases the emphasis for these prior efforts was placed on determining the installation's internal ability to manage Y2K challenges and did not necessarily address the capabilities of the host nations to provide continued support to overseas operating locations and missions.

The Y2K Outreach office expanded the overall DoD focus to "look beyond the fence" thus determining if and to what extent host nations could continue important support services during the Y2K transition period. The ultimate goal of the expanded efforts was to provide the CINCs and Service components the information they needed to determine vulnerabilities and conduct effective planning for continuity of operations and contingencies. Host nation sectors of primary concern included energy, telecommunications, water, wastewater, transportation, air traffic control services, medical services, and safety and security.

OSD Y2K Outreach worked closely with JCS, the Services, and CINC Y2K offices to determine which installations and support sectors required additional investigation to support planning efforts. The main geographic areas of interest for these efforts were Europe, South West Asia, and the Pacific/Asia. Specific locations were selected for assessment and teams were formed to visit the locations and meet with U.S. and host nation representatives. Each of the visits required extensive coordination with the State Department, embassies, CINC Y2K offices, DoD commands and components, and other U.S. Government (USG) organizations to schedule meetings and visits within

the host nations. Each team was tailored to meet specific tasks and information requirements.

Information developed during the visits, continued research, coordination of information associated with other USG agency efforts, and additional details provided by operating locations in host countries provided a much better account of what to expect during the transition. In addition, the extensive level of coordination led to additional sources of information and increased the awareness of various issues among all participants. The combined contributions of all USG agencies provided a much better assessment of what DoD and other USG agencies could expect during the transition in overseas operating locations. Specific attention was paid to NATO/SHAPE; OSD Y2K Outreach established working relationships with the SHAPE Y2K PMO, and provided appropriate technical expertise as SHAPE developed its Y2K management plans.

U.S. - Russian Cooperative Efforts

The U.S. and Russia have continued to work on mutual Y2K related national security concerns in five areas. The areas include Y2K Technology Management, Missile Warning, Nuclear Command and Control, Nuclear Stockpile Security, and Special Communications Links. Each effort has a lead agency in charge with overall coordination conducted by the OSD Y2K Outreach Office.

Y2K Management. The OSD Y2K Outreach Office is the lead agency responsible for the Y2K technology management effort. The purpose of the initiative is to exchange Y2K management program information, general status, and management experiences to provide mutual assistance in managing the problem, as well as understand each other's management plans and progress. Several meetings in Moscow the past few months permitted the two countries to exchange ideas on how to best manage the transition period. Russia decided to take an approach similar to the U.S. to meet its Y2K challenges. U.S. Y2K experts traveled to Moscow during an August session to address specific Russian requests for assistance and provide additional technical expertise.

Missile Warning. OSD Policy and the Joint Staff are lead agencies for the missile warning initiative. The purpose of the effort is to reduce the risk of misunderstandings from missile early warning systems. Other participants include OSD/C3I, SPACECOM/NORAD, and the Air Force. Work has continued to establish the Center for Year 2000 Strategic Stability (CY2KSS) in Colorado Springs, CO and ensure it is operational for the transition period. The CY2KSS will be manned by U.S. and Russian participants who will jointly monitor missile early warning status and ensure there is no misunderstanding by either country.

Nuclear Command and Control. U.S. Strategic Command (USSTRATCOM) is the lead for Nuclear Forces Command and Control initiative. There are two purposes. The first is to exchange Nuclear specific Y2K management program information, general status, and management experience to assist each other in managing the problem, as well

DoD 11th Quarterly Report to OMB

as understand each other's management plans and progress. The second is to discuss our plans for managing Y2K when it arrives to prevent misunderstandings during the Y2K transition. Other participants include OSD (Policy, C3I, Public Affairs, and functional experts), Joint Staff, SPACECOM/NORAD, and Service Components. The participants have been working with Russian Strategic Rocket Forces representatives to address mutual concerns and remedies.

Nuclear Stockpile Security. The Defense Threat Reduction Agency (DTRA) is the lead agency for this initiative. The purpose is to ensure control, security, and accountability of Russian nuclear materials, including stockpiles, weapons labs, and associated technology, during the Y2K transition. Other participants include OSD (Policy, C3I, and functional experts), Joint Staff, CINCSTRAT, and Service Components. The participants have been working with Russian Ministry of Defense (MoD) counterparts on specific action areas. Russia has identified the location of 50 monitoring centers to meet security requirements and DTRA is working with MoD to establish and equip the centers for Y2K transition period operations.

Special Communication Links. The Defense Information Systems Agency (DISA) is the lead agency for the Special Communications Links initiative. The purpose is to ensure reliable communications between U.S. and Russian national political and military leaders during the Y2K transition. Other participants include OSD (Policy, C3I, Public Affairs, and functional experts), Joint Staff, CINCSTRAT, and Service Components. Extensive work has been conducted the past few months to assess existing communications links, upgrade various segments to ensure full Y2K compliance, and install additional redundancy and capability for the transition period.

Year 2000 Transition Period/Day One

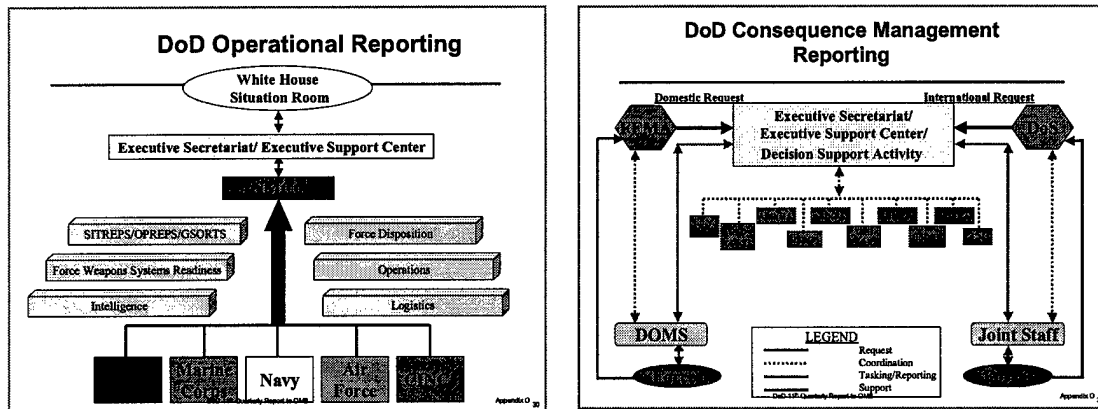
The Department has designated the period September 1, 1999, through March 31, 2000, as the "Y2K Date Transition Period." This period encompasses possible events occurring from the 9/9/99 date and from the February 29, 2000, leap year date. To prepare for the unprecedented nature of possible Y2K problems,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

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 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 has:

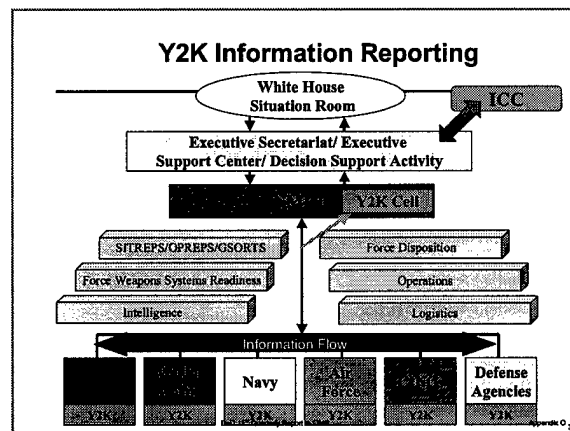
- Acted to ensure the maintenance of the department's operational readiness and the preeminence of the Department's national security responsibilities.

DoD 11th Quarterly Report to OMB

- Developed a strategy to ensure that DoD resources are applied in the most effective and efficient manner possible.



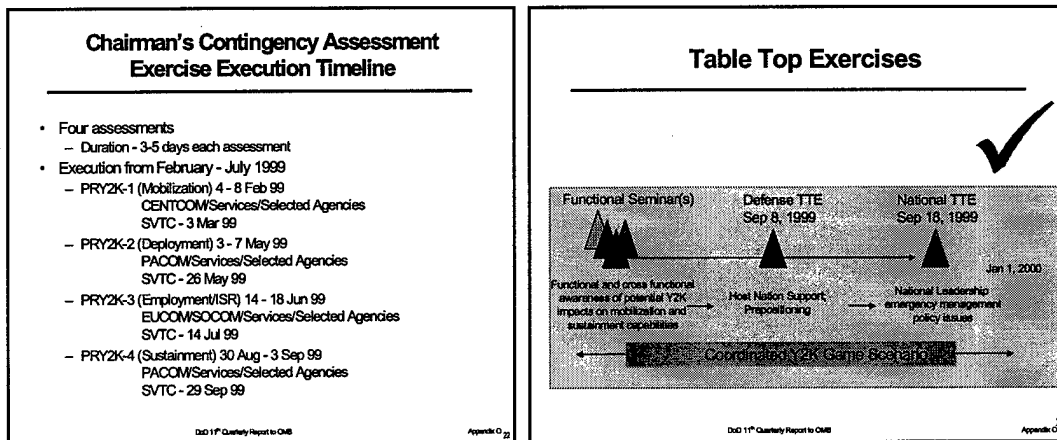
- Developed the Y2K Decision Support Activity (DSA) to monitor critical Defense infrastructures, public broadcasts, and the Internet to provide early-warning and infrastructure reliability and decision-support information to the Executive Secretariat, the Department's leadership, and the Information Coordination Center.
- Developed specific Y2K training materials to ensure everyone involved in MSCA knows the specific methods for dealing with Year 2000-related requests.
- Established an information flow to accurately receive, track, and respond to requests for MSCA from FEMA and Foreign Disaster Assistance requests from Department of State.



Leadership Preparation for Decision-Making

Throughout 1999, DoD conducted a series of events to prepare senior leadership

for possible decisions required by Y2K contingencies and evaluated the Department's operational contingency plans. There were two major activities in preparing DoD leadership for dealing with Y2K: Chairman of the Joint Chiefs of Staff (CJCS) Contingency Assessments and TableTop Exercises.



CJCS Contingency Assessments

The CJCS conducted Exercise POSITIVE RESPONSE Year 2000 (PRY2K). PRY2K was a series of four command post exercises scheduled from February to September 1999 and was the first national level exercise conducted under conditions of multiple Y2K mission critical system failures. The PRY2K assessed the ability of DoD to respond with timely decisions in a Y2K degraded environment and focused on the strategic national tasks of mobilization, deployment, employment, intelligence-surveillance-reconnaissance (ISR), and sustainment. This series of exercises was 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 was 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 assessed the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K. Finally, senior members of the warfighting community shared lessons learned and other vital information via secure videoteleconference (SVTC). The Secretary of Defense, CJCS, Service Chiefs, and CINCs participated in the SVTC following each exercise with a goal of recommending a strategy to the National Command Authorities to mitigate the impact of mission critical systems failure.

Table Top Exercises

In addition to the CJCS Contingency Assessments, the Department announced its plan for preparing the DoD leadership for the impact of Y2K on national security in a December 8, 1998, memorandum titled, "Participation in Department of Defense and National Level Y2K 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 Y2K failures. These activities

DoD 11th Quarterly Report to OMB

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 is shown in the figure below.

- A set of three functionally oriented one-day policy seminars held in November and December 1998 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 1999. 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 Y2K Coordinator, and congressional staffers.
- A DoD Defense/National Security game conducted on September 8, 1999 and completed before the national level exercise. The DoD game focused on policy and crisis management in response to a national security emergency. The DoD senior leadership fully participated, including the Deputy Secretary of Defense, the Vice-Chairman of the Joint Chiefs of Staff, the Service Under Secretaries, the DoD CIO, selected Principal Staff Assistants and the Directors of specified Defense Agencies. The State Department and FEMA also participated in the exercise.
- This activity led up to a National-level Y2K Table Top Exercise on September 18, 1999. This White House Y2K office inter-agency exercise was supported jointly by DoD and FEMA.

Informing the Department of Defense Community and the Public

The Department of Defense has executed a complex, comprehensive program to inform its many audiences: the active duty military members, their families, retirees beneficiaries, as well as other areas of the government, commercial vendors and suppliers, as well as the general public, both within the United States and throughout the world.

The Department of Defense devised and executed a decentralized public affairs effort, driven largely by the Military Departments and the Defense Agencies. Some of their achievements include:

- Produced and distributed over one million Y2K Personal Preparedness pamphlets to the DoD community throughout the globe.
- Published hundreds of articles in specialized newspapers and magazines to target specialized audiences and address their concerns.

DoD 11th Quarterly Report to OMB

- Produced countless video, television, and radio public service announcements and informational programming for use in training, and aired on the Armed Forces Radio and Television branch of the Armed Forces Information Service.
- Created and operated numerous websites to provide more specialized and detailed information on Year 2000 programs.
- The Department of the Navy produced a creative and cost effective "Virtual Town Hall" meeting to reach all sailors and marines despite their arduous OPTEMPO. The Virtual Town Hall meeting involved the President's Special Assistant for Year 2000 Conversion, the Under Secretary of the Navy, the Vice Chief of Naval Operations, the Assistant Commandant of the Marine Corps, and other officials who presented a prepared program then responded to extemporaneous questions via satellite from DON members all over the globe. The tape was later sent to all Navy and Marine Corps units for use in training.
- Over 200 DoD Installations engaged in "Community Conversations" with their surrounding civilian communities to share information regarding Year 2000 efforts.
- The Military Health System produced informational inserts for pharmacy bags and Y2K videotapes aired in waiting rooms.
- The Defense Commissary Agency produced an exceptional public service campaign to inform and assist its public, particularly those assigned to installations outside the United States.
- The Defense Finance and Accounting Service (DFAS) also produced a Y2K statement for Leave and Earnings Statements as well as many other media efforts.

As a result of this cooperative information effort, DoD members and their beneficiaries are among the most informed on Year 2000 efforts.

VIII Other Management Information

- A. Report your estimates of costs associated with year 2000 remediation including both information technology costs as well as costs associated with non-IT systems. Report totals in millions of dollars. (For amounts under \$10 million, report to tenths of a million.).**

Cost Estimates

Cost estimates are detailed at Appendix N.

- B. Please identify any costs within these estimates that are not covered by base funds and/or emergency funds that have already been released.**

Emergency Funds

The Department received \$1.1 billion in Emergency Supplemental funds for Y2K in Fiscal Year 1999. All funding has been spent.

- C. If there have been dramatic changes in cost, please explain.**

Cost Estimate Changes

The Department's estimate of Y2K costs has remained relatively unchanged from the 10th report. The reported figure for FY 99 decreased due to a refinement of the requirements and associated costing. Other changes are considered minor and reflect normal accounting adjustments.

The Office of the Assistant Inspector General for Auditing, DoD, in accordance with an informal partnership with the Chief Information Officer, provides substantial support to the effective oversight of the DoD Y2K program. Since its initial Y2K audit efforts in 1997, the DoDIG has completed 136 Y2K audits and has 39 audits ongoing. To provide that level of support, the DoDIG devoted over 180 staff years, or more than 30 percent of its audit staff, to Y2K audits during FY 1999. Staff costs for Y2K audits during FY 1998 and FY 1999 exceeded \$16 million.

- D. Describe any concerns with availability of key personnel, including ensuring that key staff will be available during the weeks before and after the transition to the year 2000.**

Key Personnel Availability

DoD has no problems with key staff availability for Y2K. DoD is a 7 x 24 business under normal circumstances and it is well prepared to staff all of its operations centers and execute recall of other personnel if necessary. Organizational Y2K "command posts," existing operations centers, and facility special action teams have been designated. Operational forces will use proven mechanisms for reporting and responding to changes in capability or readiness. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Y2K Decision Support Activity (DSA) will monitor the readiness of DoD business functions. The business units of the DoD (e.g. Defense Logistics Agency, Defense Finance and Accounting Service) will report status and outages of mission critical systems to the DSA if and when they occur. Each Defense Agency and the major organizations of the services have established help desks and action teams to quickly respond to any system-related problems, while Continuity of Operations Plans ensure that core DoD missions will continue.

- E. Describe any problems that are affecting progress.**

DoD 11th Quarterly Report to OMB

The Y2K 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 Y2K-related problems.

The Department's collective efforts in dealing with the Year 2000 problem have had several positive impacts on IT management. The DoD is treating the Year 2000 problem as if it were a cyber attack directed at the very core of its military capability -- at the ability to obtain, process, and control information that allows American forces to dominate the battlefield. Securing systems for the Year 2000 has also afforded numerous lessons that will translate well to efforts in securing critical information infrastructure in the years well beyond the Year 2000.

Assessment efforts for Y2K have led to the best ever accounting of DoD systems and status. The information management structure now in place meets the requirements of the Clinger-Cohen Act. There is more senior level awareness and appreciation for information technology than ever before, to include an acute awareness that government needs to keep pace with industry. The enormous effort and awareness of IT generated by the Year 2000 problem has resulted in significant progress across the board in information superiority.

Conclusion

The Department of Defense is prepared to execute its national security responsibilities before, on, and after January 1, 2000. The Department's operational contingency plans have been developed and executed within a solid management structure. All Year 2000 efforts received the personal attention of the Department's senior leadership. Finally, these efforts have been rigorously scrutinized by independent auditors, including the Department's Inspectors General and the General Accounting Office.

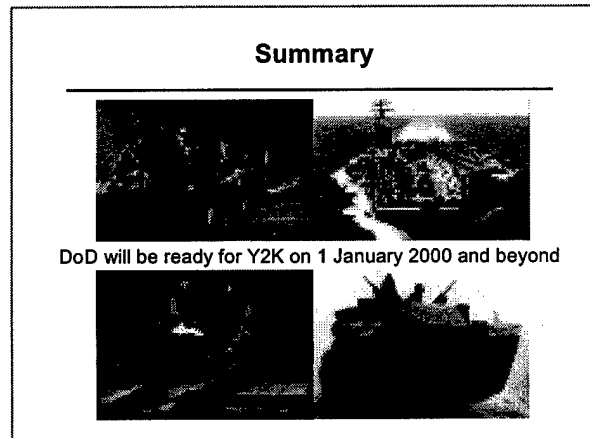
- The DoD components have gone to commendable lengths to prepare both their systems and their personnel for the transition with informational messages in a variety of media.
- A system configuration management policy for Y2K to minimize changes has been promulgated, with documented procedures to obtain necessary waivers.
- Infrastructure risk assessments have been performed by Defense Logistics Agency and by the commands responsible for coordinating and providing utilities and critical infrastructure services to DoD facilities.
- Y2K "Posture Levels" have been established by the Joint Staff and implemented by the Services, Commanders in Chief of the Combatant

DoD 11th Quarterly Report to OMB

Commands, and key Defense Agencies. These posture levels provide planning and action assumptions for DoD components and a means to synchronize actions in anticipation of or response to any disruptions occurring during the date transition.

- DoD has conducted 122 End-to-End tests to demonstrate the Department's ability to conduct its mission.

A summary of the DoD Y2K Program and status as of November 9, 1999 is included at Appendix O.



List of Appendices

- Appendix A Mission Critical Systems/Mission Critical Systems to be Completed
- Appendix B Non-Mission Critical Systems/Non- Mission Critical Systems to be Completed
- Appendix C Total Systems
- Appendix D Data Interfaces
- Appendix E Embedded Devices
- Appendix F DoD Y2K Community Conversations Memo of August 18, 1999
- Appendix G DoD Limitation On Configuration Changes to Y2K-Compliant Systems of August 20,1999
- Appendix H Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
- Appendix I Security Policy for DoD Y2K Information of October 6, 1999
- Appendix J Federal High Impact Programs: DoD Military Hospitals
- Appendix K Federal High Impact Programs: DoD Retiree/Annuitant Pay
- Appendix L Independent Validation and Government-Wide Systems
- Appendix M Updated DoD Day One Planning and BCCP Report
- Appendix N Cost Estimates for DoD Components
- Appendix O Summary of DoD Y2K Program and November 1999 Status

Department of Defense
11th Quarterly Report to OMB
MISSION CRITICAL SYSTEMS

MISSION CRITICAL SYSTEMS														
Component	Total Systems	Strategy				Remediations Strategy by Phase					Systems to Complete			
		No Remediation	Development 1 and 2	Replacement	Termination	Assessment	Renovation	Validation	Implementation	Completion	Replacement	Termination	Remediation	No Rem Req
ARMY	409	220	14	11	4	0	0	0	2	158	1	0	2	0
DON	679	488	1	7	8	0	0	0	0	175	0	0	0	0
USAF	441	260	11	12	24	0	0	0	0	134	1	0	0	0
JS	40	5	0	5	1	0	0	0	2	27	1	0	2	0
SOCOM	31	4	3	0	0	0	0	0	1	23	0	0	1	0
USI	438	82	0	30	75	0	0	0	2	249	1	1	2	0
DIA	0	0	0	0	0	0	0	0	0	0	0	0	0	0
USD(A&T)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BMDO	10	0	10	0	0	0	0	0	0	0	0	0	0	0
DARPA	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DLA	33	2	0	0	0	0	0	0	0	0	0	0	0	0
DTRA	7	0	0	1	0	0	0	0	0	31	0	0	0	0
DFAS	63	0	0	19	2	0	0	0	0	6	0	0	0	0
DCAA	0	0	0	0	0	0	0	0	0	42	0	0	0	0
USD(P&R)	2	0	0	0	0	0	0	0	0	2	0	0	0	0
DeCA	4	0	0	0	0	0	0	0	1	3	0	0	1	0
OASD/HA	12	2	0	0	1	0	0	0	0	9	0	0	0	0
DSCA	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSS	2	2	0	0	0	0	0	0	0	0	0	0	0	0
DISA	113	7	5	4	2	0	0	0	0	95	0	0	0	0
AFIS	0	0	0	0	0	0	0	0	0	0	0	0	0	0
WHS	83	28	0	6	10	0	0	0	0	39	0	0	0	0
DODIG	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total	2367	1100	44	95	127	0	0	0	8	993	4	1	8	0

Department of Defense
11th Quarterly Report to OMB
Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column In Repair To Replace	Contingency Plan Complete Yes No	Date Available	Reason system won't be implemented on time	Completion Date
ARMY M1A2	Abrams M1A2 Tank System	Heavy Combat Vehicle; Tracked.	X	X	1-Nov-98	A non-operational software error with the clock set-up page on the commander's display was corrected in March of 1999. The Version 2.5.2 software change package was shipped to the field on 11/2/99. Estimate that all of the 627 affected tanks will load the Version 2.5.2 software change package by 12/15/99. This problem is only cosmetic. It does not affect the operational capability of the tank.	15-Dec-99
RCAS RPAM	Retirement Point Accounting Management	Retirement Point Accounting Management (RPAM) for the Army National Guard. The application replaces the ARNG RPAS and will function on the RCAS upon completion.	X	X	28-Jul-99	RPAM is implemented at all sites with only the issue of data migration remaining. Estimated completion of data migration is 12/15/99.	15-Dec-99
RPAS-ARNG	Retirement Points Accounting System - Army National Guard	RPAS is a computer-supported retirement point accounting system that operates at the field operating level located in each of the 50 States and 4 Territories. RPAS supports the areas of retirement point accounting, personnel management, information retrieval, and external interfaces.		X	13-May-98	This system was never planned to be Y2K compliant because of replacement by RCAS RPAM.	15-Dec-99
DFCS DIBS 2000	DeCA Interactive Business System	Started in January 1997 to make the DIBS system Y2K compliant. DIBS is DeCA's core business system. It supports a variety of functions (ordering, receiving, shelf stock replacement, physical inventory and control operations).	X	X	10-Feb-99	Deployment of DIBS 2000 to all regions takes approximately one year. Deployment is scheduled to begin 9/1/98. The system will be fully implemented and Y2K compliant by 11/30/99.	30-Nov-99
JS JFCOM	LIMS	Information Management System	X	X	1-May-98	LIMS is migrating COTS packages. JFCOM HQ complete. Final migration at Suffolk, Va. Location will complete in NOV 99.	19-Nov-99
JFCOM	LDMX FEED	AMHS		X	1-Jan-98	Y2K compliant AMHS software wasn't delivered as scheduled. DISA is currently fielding compliant version.	30-Nov-99
SOCOM	PRIVATEER	Provides a permanent, integrated threat warning capability onboard Cyclone class Coastal Patrol Combatants and Mark V SOF craft.	X	X	1-Jan-99	Awaiting vendor delivery. Implementation is dependent on individual platforms (Cyclone class Personal Computers and Mark V Special Operations Forces support vessels) becoming available for installation.	20-Nov-99
PACOM	PASS-K	Pacom ADP Server Site - Korea			1-Jan-00	Fielding delay due to PERSTEMPO (Ulchi Focus Lens (UFL) exercise).	17-Nov-99
USAF WCCS v1.2	Wing Command and Control System	Command and Control		X	1-Jan-98	This system was scheduled to be replaced by TBMCs. Since TBMCs will no longer be implemented before 1 Jan 2000, work-arounds for WCCS are now being fielded. WCCS will be decommissioned on 30 Nov 99.	30-Nov-99
USI ISSE Guard	ISSE Guard	Guard processor controlling information exchange between networks operating at different classification levels.	X	X	1-Jan-99	All installations completed but two. Last two locations have an alternative process available; ISSE Guard is not considered a mission critical functionality at those locations. Installs are scheduled to be completed by 15 Nov 99.	15-Nov-99

Department of Defense
11th Quarterly Report to OMB
Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency/ Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	In	To	Yes	No		
DAWN	Defense Attache Worldwide Network	Worldwide communications and information support network for defense attaches.	X			X		System is 92% complete for worldwide implementation. Remaining system installations remain on schedule for 30 Nov 99 completion, per the program schedule developed in 1998.	30-Nov-99
DELF2426	DELF2426	A specialized intelligence system			X	X		System is being replaced at two locations. Replacement system is currently being installed. The user acceptance test is scheduled for completion by 29 Nov 99. Because of differences in functionality between the old and new system, one site has received permission to continue operating the old system (DELF2426) until the end of the year.	27-Dec-99
DESM1153	DESM1153	A specialized intelligence processing system			X		X	System is being retired. Functionality has been taken over by a different system; the user is finishing an FY99 processing backlog with the older system before it is retired. Out of service date is projected for 15 Nov 99.	15-Nov-99

Department of Defense
11th Quarterly Report to OMB
NON MISSION CRITICAL SYSTEMS

NON MISSION CRITICAL SYSTEMS														
Component	Total Systems	Strategy				Remediations Strategy by Phase				Systems to Complete				No Rem Req
		No Remediation	Development 1 and 2	Replacement	Termination	Remediation	Assessment	Renovation	Validation	Implementation	Completion	Replacement	Termination	Remediation
ARMY	752	326	29	92	44	258	0	0	0	3	258	6	3	3
DON	1848	1107	0	77	286	374	0	1	0	3	374	0	0	4
USAF	2990	1593	127	52	606	312	0	7	7	5	593	7	7	19
JS	80	36	4	12	9	19	0	0	0	0	19	1	1	0
SOCOM	2	1	1	0	0	0	0	0	0	0	0	0	0	0
USI	1055	48	2	123	183	689	0	1	4	4	690	23	10	9
DIA	0	0	0	0	0	0	0	0	0	0	0	0	0	0
USD(A&T)	25	0	12	9	0	4	0	0	0	0	4	0	0	0
BMDO	143	70	9	0	0	64	0	0	0	0	64	0	0	0
DARPA	1	0	0	0	0	1	0	0	0	0	1	0	0	0
DLA	80	2	1	10	16	51	0	0	0	0	51	0	0	0
DTRA	17	2	0	0	0	15	0	0	0	0	15	0	0	0
DFAS	71	2	0	11	14	44	0	0	0	0	44	1	0	0
DCAA	1	1	0	0	0	0	0	0	0	0	0	0	0	0
USD(P&R)	2	1	0	0	0	1	0	0	0	0	1	0	0	0
DeCA	6	0	0	6	0	0	0	0	0	0	0	2	0	0
OASD/HA	75	8	1	4	14	49	0	0	0	0	48	0	0	0
DSCA	6	0	1	0	0	5	0	0	0	0	5	0	0	0
DSS	22	7	2	7	1	12	0	2	0	2	1	0	0	4
DISA	29	1	1	0	0	27	0	0	0	0	27	0	0	0
AFIS	18	13	0	2	0	3	0	0	0	0	3	1	0	0
WHS	23	11	0	0	2	10	0	0	0	0	10	0	0	0
DODIG	21	0	0	7	2	12	0	0	0	0	12	0	0	0
Total	7267	3229	190	412	1177	2259	0	11	11	17	2220	41	21	39
														8

NON MISSION CRITICAL SYSTEMS

APPENDIX B

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete			Reason system won't be implemented on time	Completion Date
			In	To	Repair	Yes	No	Date Available		
AFIS	VIS-MEDIA INVENTORY MANAGEMENT SYSTEM (OBMS)		X			X		1-Nov-99	CONTRACTING DELAY. EXISTING SYSTEM WAS ORIGINALLY SCHEDULED FOR REPLACEMENT IN JAN-FEB 2000. RATHER THAN SPEND \$27,000 TO TEST THE EXISTING SYSTEM FOR Y2K COMPLIANCE, CONTRACT WAS MODIFIED TO REPLACE THE SYSTEM PRIOR TO 1/1/00. NEW SYSTEM HAS BEEN TESTED AND CERTIFIED Y2K COMPLIANT AND IS IN FINAL INSTALLATION PROCESS.	15-Dec-99
ARMY										
IGNET	Inspector General Network System	The IGNET is an automated information network that supports IG case data collection, data analysis, communications and administrative requirements of IGs worldwide.	X			X		30-Sep-99	As of 11/15/99, the hardware at all 250 sites has been upgraded. Compliant version of software will be implemented at all field locations by 12/03/99.	3-Dec-99
HOMES 3	Housing Office Management System	HOMES 3 will replace current HOUSING programs being used by Army Housing Offices. It allows those offices to manage the housing inventory and government-owned furnishings on Army installations.		X		X		1-Sep-98	This system slipped because of a test failure. This test failure required that the system be revisited, fixed, and new acceptance testing be completed. As of 11/08/99, this system has been implemented at 98% of its 102 scheduled sites (100 of 102).	10-Dec-99
ALPMS	Army Lodging Property Management System (ALPMS)	The Geac/UX system will become the property management system which replaces the non-Y2K HOMES Lodging at Army Lodging operations.		X			X	15-Dec-99	Shipping, funding coordination with the Army Lodging sites, and site readiness caused progress delay. As of 10/27/99, 57 of the 60 (95%) sites are completed.	6-Dec-99
HOMES LODGING V8.0	Housing Operations Management System Lodging Version 8.0	HOMES Lodging is non-Y2K, and is being replaced by the Army Lodging Property Management System (ALPMS). The COTS system is provided by Geac Computers, Inc. Geac has provided Y2K compliant documentation.					X	15-Dec-99	Due to replacement system (ALPMS) fielding schedule. As of 10/27/99, 57 of the 60 (95%) sites have been replaced by ALPMS.	30-Nov-99
SIDPERS-ARNG (HOL)	Standard Installation/Division Personnel System-ARNG (Headqu	SIDPERS (HOL) Headquarters Operating Level provides a variety of personnel, organization and authorization data reports and extracts to the Headquarters, field levels, DOD and DA agencies.				X		14-May-98	This is a single site fielding and is currently undergoing conversion to TAPDB-ARNG as of 10/18/99.	30-Nov-99
MPMIS SMS	Military Police Management Information System Security Manag	It is a software application used by physical security inspectors to conduct risk analysis, perform inspections, evaluate mission essential vulnerable areas, track civilian police and security guard programs.				X		15-Jun-98	Due to changes in security methods and practices, this system has become obsolete and will be retired on 11/30/99.	30-Nov-99
HOMES 2 A&T/CHRRS	Housing Operations Management System Assignments & Terminati	System is used by Army Housing offices. It will be replaced by HOMES 3.				X		1-Sep-98	Due to replacement system (Homes 3) fielding schedule. As of 11/08/99, this system has been implemented at 98% of its 102 scheduled sites (100 of 102).	10-Dec-99
HOMES 2 FURNISHINGS	Housing Operations Management System Furnishings (HOMES 2 FU	System is used by Army Housing offices. It will be replaced by HOMES 3.				X		1-Sep-98	Due to replacement system (Homes 3) fielding schedule. As of 11/08/99, this system has been implemented at 98% of its 102 scheduled sites (100 of 102).	10-Dec-99
HOMES 2 SA (3B2)	Housing Operations Management System System Administration (	System is used by Army Housing offices. It will be replaced by HOMES 3.				X		1-Sep-98	Due to replacement system (Homes 3) fielding schedule. As of 11/08/99, this system has been implemented at 98% of its 102 scheduled sites (100 of 102).	10-Dec-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column	Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	Replace	Yes	No	Date Available
HOMES 2 SA (HP)	Housing Operations Management System Administration (	System is used by Army Housing offices. It will be replaced by HOMES 3.			X		1-Sep-98
DRREAL	Desktop Resource for Real Estate	DrReal is a GUI based application used to track real estate information at the state level. The data is then forwarded to NGB for approval and consolidation. DrReal data is used to produce reports showing the number, facility type and funding of real estate throughout the National Guard.			X		25-Sep-98
WLN	Warlord Notebook	Command unique INTEL system that consists of prototype software hosted on a unit procured laptop. Maintenance of this prototype system is a unit responsibility.			X		4-Nov-99
DFAS COINS	Contractor Invoice Service	COINS enables defense contractors whose invoices are paid from MOCAS at DFAS-CO to electronically inquire about the status of their invoices.	X			X	1-Jan-98
DFAS AN/SQ-34A(V)	AIRCRAFT CARRIER TACTICAL SUPPORT CENTER TACTICAL SUBSYSTEM	THE AN/SQ-34A(V) AIRCRAFT CARRIER TACTICAL SUPPORT CENTER (CV-TSC) IS INSTALLED IN ALL CV/CVNs AND PROVIDES THE CAPABILITY TO COLLECT, PROCESS, ANALYZE AND DISPLAY ACOUSTIC AND TACTICAL INFORMATION.	X		X		1-Jan-98
QDB	SYMIS QUERY DATABASE	PROVIDES END-USER QUERY ACCESS TO SHIPYARD INFORMATION.	X		X		1-Jan-98
IANTN	INTER AMERICAN NAVAL TELECOMMUNICATIONS NETWORKS	IANTN OPERATES A DEMAND ASSIGNED MULTIPLE ACCESS (DAMA) SYSTEM WITH A HUB SITE IN PUERTO RICO AND 12 REMOTE SITES THROUGHOUT CENTRAL AND SOUTH AMERICA.	X		X		1-Jan-98
AN/KSQ-1/PLRS	AMPHIBIOUS ASSAULT DIRECTION SYSTEM (AADS) AN/KSQ-1/PLRS	THE AN/KSQ-1 PROVIDES THE COMMANDER, AMPHIBIOUS TASK FORCE THE CAPABILITY TO IDENTIFY, TRACK COMMUNICATE WITH AND CONTROL AMPHIBIOUS LANDING CRAFT THROUGH TRANSIT ASHORE, OFFLOAD AND RETURN TO SHIP.	X		X		1-Jan-98
DSS							

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column In Repair Replace	Contingency Plan Complete Yes No	Date Available	Reason system won't be implemented on time	Completion Date
ISS	INDUSTRIAL SECURITY SYSTEM	AUTOMATED SYSTEM TO TRACK GOVERNMENT CONTRACTOR FACILITY CLEARANCE INFORMATION UNDER THE DEFENSE INDUSTRIAL SECURITY PROGRAM (DISP).		X	1-Nov-99	System remains in validation. New Project Management Office assigned System is in testing at the Air Force testing site at Gunter Air Force Base	15-Dec-99
FINCEN02	CCMS TREASURY FINCEN			X	1-Nov-99	System still in validation. Unit testing being conducted at Air Force testing facility at Gunter Air Force Base. Completion date is Dec 15, 1999	15-Dec-99
FCMS	File Control Management System	Used to request dossiers from various DoD repositories		X	1-Nov-99	System in validation phase. Currently being tested (unit) at Gunter Air Force Base. Will be completed on Dec 15, 1999.	15-Dec-99
FAM	Field Agent Management				1-Jan-01	This is a replacement system - due to inability of contractor to deliver in timely manner the legacy system was renovated to make compliant	1-Jan-01
FIMS01	Field Information Management System			X	1-Nov-99	System was changed from replacement to remediation when unable to develop replacement system in timely manner	15-Dec-99
RTS01	Reject Tracking System	System is used to record and track paper personnel security forms that are rejected and returned		X	1-Nov-99	System is being unit tested at Gunter Air Force Base by our newly assigned Project Management Office	15-Dec-99
ACM	CCMS Credit	Application queries the three major credit bureaus databases		X	1-Nov-99	System is being unit tested by the newly assigned Air Force Project Management Office (being tested at Gunter Air Force Base)	15-Dec-99
DeCA	DeCA Interim Business System						
DIBS retiring	DIBS	DIBS is an improved version of the District Oriented Store System (DOSS) used by the Army in Europe. Designed to replace the various service specific systems inherited by DeCA, DIBS supports a variety of functions ordering, receiving, shelf stock replace		X	1-Jan-98	DIBS is being replaced by the DeCA Interactive Business System (DIBS 2000).	30-Nov-99
FDS	Frequent Delivery Systems	Combined into DIBS 2000. FDS/DSD placed orders, tracks the receipt of deliveries, totals the amount owed for products received, supports the reconciliation of deliveries, initiates payments to vendors and maintains files of resale items provided by more		X	1-Jan-98	FDS is being replaced by DIBS 2000.	30-Nov-99
JS							
CENTCOM (NMC)	DVTC	DVTC- Desktop Video Teleconferencing System	X	X	1-Jun-99	Awaiting new hardware.	17-Dec-99
SPACECOM (NMC)	ARENA	ARENA Mapping Tool	X	X	1-Jan-99	In development	15-Jul-00
USAF							
NACTS	Nellis Air Combat Training System	Scientific and Engineering	X	X	1-Jan-98	Category III, Mission Impaired system. A development system replacing RFMDS. Following development schedule. No mission impact.	30-Nov-99
ECSII / D136N	J85 Engine Compressor Stator (ECSII) Program	Human Resources		X	1-Jan-98	Category II, Mission Essential system. System used to measure the length of engine stator blades after engine tear-down at the Engine Regional Repair Center, Laughlin AFB, TX. This new version replaces the functionality of an older version. No mission impact. Since this new version will not be deployed until after Jan 2000, existing system is being certified.	30-Jun-00

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency/ Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	Replace	In To	Yes	No		
ANG AIRS	ANG AIRLIFT INFORMATION AND REPORTING SYSTEM	Command and Control	X			X		Category III, Mission Impaired system. System is Y2K compliant and fielded. Working the certification package for signature with completion by 15 Nov 99. No mission impact.	15-Nov-99
AMMES (MOD)	Automated Material Management and Engineering Syst	Logistics					X	Category III, Mission Impaired. System will be decommissioned on 30 November 1999 per Hq AF waiver. Function outsourced beginning Jan 2000.	30-Nov-99
BRDSUP/E080	Board Support	Personnel and Readiness	X			X		Category II, Mission Essential system. System provides information on applicants to officer selection boards. Certification is now required due to delay of replacement system. Y2K patch is being installed. Certification will follow. The Officer accession process will continue. Although labor intensive, manual processing is the temporary work-around.	30-Nov-99
CADET- ED/E017	Cadet Education and Training Computing	Human Resources				X		Category III, Mission Impaired system. Replacement for High Wind Alert System at the US Air Force Academy. Legacy system will continue to function with workarounds until replacement is procured. Contract goes out for bids after site survey team completes analysis. No mission impact. ¹	4-Dec-99
OPS- ATLANTIS/D272	OPS Atlantis	Human Resources				X		Category II, Mission Essential. Wargaming system is running in parallel with newly developed replacement system until data conversion is complete. No mission impact.	30-Nov-99
EMS/D288	Education Management System	Human Resources					X	Category II, Mission Essential system. The Education Management System is a new development which replaces the functionality of two systems that could not be made Y2K compliant. Provides basic student management capabilities to the Officer Training School and the AF ROTC cadet program. Certification efforts are underway. No mission impact.	30-Nov-99
OPS ATLANTIS II/D277	Enhancement to Operation ATLANTIS Wargame Program	Human Resources		X		X		Category II, Mission Essential. The new version of this unclassified wargaming tool used to teach company grade officers enrolled in the Air Force Squadron Officer School replaces the functionality of an older version. It has been certified and is in implementation phase. Given the time/effort required to transition data from the old system to the new system, as a backup, efforts are nearing completion to certify the older version. No mission impact, does not process dates, additionally, the old version is being certified as a work-around.	30-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	In To	Replace	Yes	No		
ILS/R028	Integrated Library System	Information Management					X	Category IV - non-mission essential system. Base library system designed to support multiple, general purpose library operations, such as automated book checkout, at numerous AETC bases. Contract schedule drives completion dates. Minimal impact, manual work-arounds available.	30-Nov-99
ACES	Automated Civil Engineer System	Facilities		X		X		Category III, Mission Impaired system. This is a development system replacing an existing system that has become Y2K compliant. No impact due to existing functional capability with Y2K compliant system.	30-Nov-99
RASCAL	RASCAL-USAFE Tasking Database	Information Management					X	Category III, Mission Impaired system. A legacy database used to track administrative tasks. The compliant replacement system is in place. Legacy system will terminate once remaining active tasks are closed. No mission impact.	30-Nov-99
ALSMS	Automated Life Support Management System	Command and Control	X			X		Category II, Mission Essential system. System is still in testing for validation. Target for certification package completion is 15 Nov 99. Minimal mission impact.	30-Nov-99
RMCC - IFDAPS	Integrated Flight Data Acquisition and Processing System	Scientific and Engineering				X		Category IV - non-mission essential system. Conversion of files to ADAPS, the replacement system, and testing required. No mission impact.	1-Dec-99
RDS	Run File Development System	Scientific and Engineering				X		Category III, Mission Impaired system. Conversion of files to ADAPS, the replacement system, and testing required. No mission impact.	1-Dec-99
DATA SYSTEM (HP A900)	DMS PROTOCOL CONVERTER	Weapons				X		Category III, Mission Impaired system. A decommissioning system awaiting completion of the replacement system (DMS-DEPOT). No mission impact.	15-Dec-99
DATA SYSTEM (PN 9050)	DATA MANAGEMENT SYSTEM (DMS) ENCORE	Weapons				X		Category III, Mission Impaired system. A decommissioning system awaiting completion of the replacement system (DMS-DEPOT). No mission impact.	15-Dec-99
RESOMS	Resource Scheduling and Operational Management System	Scientific and Engineering					X	Category IV - non-mission essential system. A decommissioning system whose functionality is included in RESOMS II, tested compliant. Awaiting final certification package signature. No mission impact.	30-Nov-99
DATA SYSTEM (HP1000)	EMDAS (PAS)	Weapons				X		Category III, Mission Impaired system. A decommissioning system awaiting final implementation of the replacement system (DMS-DEPOT). Systems will run in parallel until replacement operationally acceptable. No mission impact.	20-Dec-99
RFMDS	Red Flag Measurement Debriefing System	Scientific and Engineering				X		Category III, Mission Impaired system. A decommissioning system awaiting completion of replacement system (NACTS). No mission impact.	15-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency/ Acronym	System Name	Brief Functional Description	Put X in required column				Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	In	To	Replace	Yes	No		
AWMDS UPGRADE	Air Warrior Measurement and Debriefing System Upgrade	Human Resources				X	X		Category II, Mission Essential system. Normal development schedule delays caused a slippage in the completion date. Certification package is in for final signature. No mission impact.	7-Nov-99
FDS II (ATCALS)	Flight Data System (Version II)	Command and Control					X		Category III, Mission Impaired system. Decommissioning system awaiting one site to implement FAA's FDIO (Flight Data Input/Output) system to complete package. No mission impact.	15-Nov-99
AWMDS	Air Warrior Measurement and Debriefing System	Personnel and Readiness					X		Category III, Mission Impaired system. Decommissioning system awaiting final certification and delivery of replacement development system. No mission impact.	1-Nov-99
C-20A	C-20A	Weapons		X			X		Category III, Mission Impaired. 1 aircraft completed. 2 remaining. Aircraft is scheduled to receive a new GPS. Second aircraft enters the depot 22 Nov 99 with delivery on 7 Feb 00 and the third aircraft enters depot 17 Dec 99 with delivery on 6 Mar 00. Aircraft do not fly when in depot so there is no mission impact.	17-Dec-99
C-20H	C-20H Aircraft	Weapons		X			X		Category III, Mission Impaired. 1 aircraft completed 1 remaining. Second aircraft enters depot on 15 Dec 99 with delivery on 5 Jan 00. Aircraft do not fly while in depot, no mission impact.	15-Dec-99
EMDAS-PADS	EMDAS-PERFORMANCE ASSESSMENT DATA SYSTEM	Weapons					X		Category III, Mission Impaired system. Development system following schedule. No mission impact.	23-Nov-99
DMS-DEPOT	DEPOT MANAGEMENT SYSTEM-DEPOT REPLACEMENT	Weapons				X		X	Category III, Mission Impaired system. Development system on contract schedule for final certification in Dec 99. No mission impact.	15-Dec-99
PRICE	Publishing Resources Information, Cost, and Evaluation system	Information Management		X			X		Category III, Mission Impaired. Projected upgrade to system failed to meet requirements. Implemented contingency plan to replace legacy system with commercial off the shelf products. Process of adapting commercial product and porting legacy data is technically complex and the implementation schedule is unavoidably aggressive. Workarounds exist but will impact timelines of service to AF publishing customers. This system is under close scrutiny by both the functional and the AF Y2K office. No impact to wartime operations. ¹	31-Dec-99
AFSCN OAS	Air Force Satellite Control Network Orbital Analysis System	Space and Weather		X			X		Category II, Mission Essential system. System delayed by operational issues that require further testing. The decommissioning system is running in tandem with its replacement. No mission impact.	17-Dec-99
ATLAS	Aircraft Traffic Logging Automated System	Command and Control					X		Category III, Mission Impaired system. Being replaced by ATLAS-R. No mission impact.	30-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete		Reason system won't be implemented on time	Completion Date
			Repair	Replace	To	Yes	No		
ATLAS-R	Aircraft Traffic Logging Automated System - Replacement	Command and Control		X		X		Category III, Mission Impaired system. Development system replacing ATLAS. Following development schedule. No mission impact.	30-Nov-99
SBIRS WM (MANDS)	Space Based Infrared System Warning Model (MANDS)	Space and Weather					X	Category IV - non-mission essential system. This was a decommissioning system, decision made not to effort underway. No mission impact.	27-Dec-99
B-2 GPU	B-2 Data Reduction and Analysis System	Weapons	X			X		Category III, Mission Impaired system. A data reduction and analysis system used to analyze range data. System is compliant and fielded. Awaiting final signature on certification package. No mission impact.	26-Nov-99
TB2/E050	Testbank 2.0	Human Resources				X		Category III, Mission Impaired system. System provides courseware developers with the capability to generate, store and print different types of tests. Certification package is in final coordination. No mission impact.	30-Nov-99
SIFP/E108	534th Training Squadron Student Initial Feedback Program	Human Resources				X		Category IV - non-mission essential system. This is an end-user developed/maintained system that provides end-of-course critique and report generation for students taught by the 534th Training Squadron. Certification package is in final coordination. No mission impact.	30-Nov-99
MOSECE/E106	534th Training Squadron Monthly Security Test Program	Human Resources				X		Category IV non-mission essential system. This is an end-user developed/maintained system that allows squadron members to view training materials and be tested on knowledge learned. Certification package is in final coordination. No mission impact.	30-Nov-99
ECS/D136	J85 Engine Compressor Stator	Scientific and Engineering					X	Category II, Mission Essential system. System measures the length of engine stator blades after engine teardown at the Engine Regional Repair Center, Laughlin AFB, TX. Upgraded version scheduled to replace this system Jun 00. Efforts underway to certify existing system with work-around. No mission impact, proven manual work-arounds available.	30-Nov-99
KITS	Kadena Interim Training System	Scientific and Engineering				X		Category III, Mission Impaired system. Awaiting final coordination of the certification package. No mission impact.	30-Nov-99
CACTIS	Crime and Counterintelligence, Terrorism Information System	Command and Control				X		Category II, Mission Essential system. Certification package in final coordination. No mission impact.	30-Nov-99
USI S21	Mission Support	Set of internal management support systems that support the NRO mission. Upgrading NRO network to NT based systems, requiring upgrades to all of the software applications. 3 non-mission critical applications remaining.	X			X		Tracking to original planned schedule. Completion date 6 Dec	6-Dec-99
S22	Operations Support	Set of systems that support nonmission critical aspects of the NRO mission. Three applications remaining.	X			X		Awaiting final patch delivery from vendor. ECD is 22 Nov 99.	22-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Pat X in required column			Contingency Plan Complete			Reason system won't be implemented on time	Completion Date
			Repair	Replace	To	Yes	No	Date Available		
ALE (DIA)	ALE (DIA)	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.	X				X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, ALE (DIA) will be shut down by 30 Nov 99.	30-Nov-99
DAWS	Defense Automated Warning System	System is being replaced by the Modernized Defense Intelligence Threat Data System (MDITDS). It is an intelligence database.	X				X	1-Jan-98	MDITDS is operational at all sites. Some sites are conducting parallel operations between DAWS and MDITDS until the end of November to ensure a smooth transition.	30-Nov-99
NACDF	National Area Coverage Data Files	System is being replaced by NACDF-M. It is an intelligence database.	X				X	1-Jan-98	NACDF-M has been installed. Maintaining parallel operations until the end of November to ensure a smooth transition.	30-Nov-99
PMIS-M/F	Personnel Management Information System-Mainframe	System is being replaced. It is a personnel management data system.	X				X	1-Jan-98	Replacement system is operational. Conducting parallel operations until the end of November to ensure a smooth transition.	30-Nov-99
APMIS	Automated Personnel Management Information System	System is being replaced. It is a personnel and manpower authorization management system.	X				X	1-Jan-98	Replacement system is operational. Conducting parallel operations until the end of November to ensure a smooth transition between the two systems.	30-Nov-99
PORTHOLE	PORTHOLE	An intelligence collection system.	X			X		1-Jan-98	Deployment to 2 field sites in process. ECD is 10 Dec 99.	10-Dec-99
SPECTRA	SPECTRA	An intelligence collection system	X			X		1-Jan-98	Deployment to one remaining site will occur shortly. ECD is 10 Dec 99.	10-Dec-99
JATACS	JATACS	An intelligence analysis system.	X				X	1-Jan-98	Software update only. Update tape in route to 10 sites. ECD is 30 Nov 99.	30-Nov-99
ACES	ACES	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery. ¹		X			X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, ACES will be shut down by 30 Nov 99.	30-Nov-99
ACS	ACS	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.	X				X	1-Jan-98	Status: NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, ACS will be shut down by 30 Nov 99.	30-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column		Contingency Plan Complete			Reason system won't be implemented on time	Completion Date
			In Repair	To Replace	Yes	No	Date Available		
ALE	ALE	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.		X		X	1-Jan-98	Status: NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, ALE will be shut down by 30 Nov 99.	30-Nov-99
ARGUS	Automated Remote Global Update System	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery. ¹		X		X	1-Jan-98	Status: NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, ARGUS will be shut down by 30 Nov 99.	30-Nov-99
FE/S	Feature Extraction Segment	System being replaced. Used in the creation of geospatial products (maps, charts, etc) ¹		X		X	1-Jan-98	Status: The replacement system is operational and operating satisfactorily. NIMA is temporarily retaining FE/S to complete some FY99 work tasks that were deferred due to the Kosovo operation world situations. System will be shut down by 30 Nov.	30-Nov-99
MIS	Map Index System	System being replaced by GIMDE/MDL. Used in the management of production of geospatial products (maps, charts, etc)		X	X		26-Sep-99	GIMDE / MDL have experienced development delays, slipping their schedules into CY2000. A contingency process has been activated. MIS is being kept operational until 15 Dec 99 to finalize the necessary management database for the contingency process, then the system will be terminated	30-Nov-99
NBIDI Servers	National Base of Imagery Derived Information Servers	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.		X		X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, NBIDI Servers will be shut down by 30 Nov 99.	30-Nov-99
NDDS	NIS Data Distribution Server	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery. ¹		X		X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, NDDS will be shut down by 30 Nov 99.	30-Nov-99

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency / Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete			Reason system won't be implemented on time	Completion Date
			Repair	To Replace	Yes	No	Date Available			
NES/CS	NES Comms Servers	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.		X		X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, NES/CS will be shut down by 30 Nov 99.	30-Nov-99	
NMUS	NDS Multi User System	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery. ¹		X		X	1-Jan-98	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, NMUS will be shut down by 30 Nov 99.	30-Nov-99	
Phase IV	Phase IV	System is being replaced. Payroll system.		X		X	1-Jan-98	Phase IV was kept operational due to pending decisions on transferring to another organization, workload associated with the Unisys system. Decision was made on 14 Oct 99, and this system will be shut down on 30 Nov 99.	30-Nov-99	
PM/S	Program Management Segment	System being replaced by GIMDE/MDL. Used in the management of production of geospatial products (maps, charts, etc)		X		X	1-Jan-98	GIMDE / MDL have experienced development delays, slipping their schedules into CY2000. A contingency process has been activated. PM/S is being kept operational until 15 Dec 99 to finalize the necessary management database for the contingency process, then the system will be terminated	15-Dec-99	
SP/S	Source Preparation Segment	System being replaced by GIMDE/MDL. Used in the management of production of geospatial products (maps, charts, etc).		X		X	1-Jan-98	GIMDE / MDL have experienced development delays, slipping their schedules into CY2000. A contingency process has been activated. SP/S is being kept operational until 15 Dec 99 to finalize the necessary management database for the contingency process, then the system will be terminated	15-Dec-99	
Unisys	Unisys	System being replaced. Mainframe used in the creation of create specialized geospatial products.		X		X	1-Jan-98	Replacement system is operational and performing satisfactorily. All functions were effectively transitioned with one remaining. Final decision made 14 Oct to transition last remaining function to another organization; system will retire 30 Nov 99.	30-Nov-99	

Department of Defense
11th Quarterly Report to OMB
Non Mission Critical Systems Scheduled for Completion After 1 Nov 1999

Agency/ Acronym	System Name	Brief Functional Description	Put X in required column			Contingency Plan Complete			Reason system won't be implemented on time	Completion Date
			In Repair	To Replace	Yes	No	Yes	No		
NDS	NIMA Data System	System being replaced by the National Exploitation System (NES). Used in the exploitation of national imagery.		X				X	NES activated on 31 Jul 99 and was declared operational on 26 Oct 99. NIMA will conduct parallel operations to ensure continuity of operations in case of unexpected NES problems. Since 26 Oct, NIMA has not experienced any significant NES operational issues. NIMA will review NES status on 16 Nov 99. If operations have been satisfactory, NDS will be shut down by 30 Nov 99.	30-Nov-99
USI-559	USI-559	Classified Intelligence System	X					X	System installed at one location. Remediation expected to be completed by 30 Nov 99.	30-Nov-99
USI-1032	USI-1032	Classified System	X					X	System installed at one location. Remediation expected to be completed by 30 Nov 99.	30-Nov-99
NMC001	NMC001	A distributed computing utility program, used at one location.	X					X	System is reported as completed; however, we are verifying that the installation process actually occurred as reported.	30-Nov-99
NMC004	NMC004	Classified capability	X					X	System ECD is 1 Dec 99	1-Dec-99
NMC006	NMC006	System being replaced. Personnel information system		X				X	Replacement system operational. This system will be left operational until the end of the year to allow off-site personnel to query their personnel records during nonworking hours when the replacement system is off-line.	30-Dec-99
NMC007	NMC007	System being replaced. Hardware maintenance status tracking data base. Also tracks requirements for and purchase status of personal computers.		X				X	System will be replaced by 1 Dec 99.	1-Dec-99
NMC008	NMC008	System being replaced. Classified System.		X				X	Replacement system will be operational by 15 Nov 99.	15-Nov-99
NMC005	NMC005	System Being retired. Pharmacy record management system.						X	System being retired as organization's pharmacy record system being incorporated into another organization's system. Conversion process on-going. Will complete by 10 Dec 99	10-Dec-99
Hyperchannel	Hyperchannel	System being retired. Comms system associated with the Unisys system (Unisys is being replaced).						X	Retirement held up pending workload decisions on functions in the Unisys system. Final decisions were made on 14 Oct 99. Hyperchannel will be retired by 30 Nov 99	30-Nov-99
UDB	Unit Data Base	Record keeping system						X	System will be retired 30 Nov 99	30-Nov-99
UPD	Unit Personnel Database	Personnel data system.						X	System will be retired by 30 Nov 99	30-Nov-99
TMS	TMS	Classified function						X	System will be retired by 30 Nov 99	30-Nov-99
CSOE	CSOE	A training aid						X	System will be retired by 30 Nov 99.	30-Nov-99
USI-664	USI-664	Classified system.						X	System will be retired by 30 Nov 99.	30-Nov-99
USI-671	USI-671	Classified system						X	System will be retired by 30 Nov 99.	30-Nov-99
USI-674	USI-674	Classified Capability						X	System will be retired by 30 Nov 99.	30-Nov-99
USI-974	USI-974	Classified system						X	System will be retired by 30 Nov 99.	30-Nov-99

Department of Defense
11th Quarterly Report to OMB
TOTAL SYSTEMS

TOTAL SYSTEMS															
Component	Total Systems	Strategy				Remediation	Remediations Strategy by Phase				Systems to Complete				
		No Remediation	Development 1 and 2	Replacement	Termination		Assessment	Renovation	Validation	Implementation	Completion	Replacement	Termination	Remediation	No Rem Req
ARMY	1161	546	43	103	48		0	0	0	5		7	3	5	0
DON	2527	1595	1	84	294		0	1	0	3		0	0	4	0
USAF	3431	1853	138	64	630		0	7	7	5		8	7	19	6
JS	120	41	4	17	10		0	0	0	2		2	1	2	0
SOCOM	33	5	4	0	0		0	0	0	1		0	0	1	0
USI	1493	130	2	153	258		0	1	4	6		24	11	11	0
DIA	0	0	0	0	0		0	0	0	0		0	0	0	0
USD(A&T)	25	0	12	9	0		0	0	0	0		0	0	0	0
BMDO	153	70	19	0	0		0	0	0	0		0	0	0	0
DARPA	1	0	0	0	0		0	0	0	0		0	0	0	0
DLA	113	4	1	10	16		0	0	0	0		0	0	0	0
DTRA	24	2	0	1	0		0	0	0	0		0	0	0	0
DFAS	134	2	0	30	16		0	0	0	0		1	0	0	0
DCAA	1	1	0	0	0		0	0	0	0		0	0	0	0
USD(P&R)	4	1	0	0	0		0	0	0	0		0	0	0	0
DeCA	10	0	0	6	0		0	0	0	1		0	0	1	0
OASD/HA	87	10	1	4	15		0	0	0	0		0	0	0	0
DSCA	6	0	1	0	0		0	0	0	0		0	0	0	0
DSS	24	9	2	7	1		0	2	0	2		0	0	4	2
DISA	142	8	6	4	2		0	0	0	0		0	0	0	0
AFIS	18	13	0	2	0		0	0	0	0		1	0	0	0
WHS	106	39	0	6	12		0	0	0	0		0	0	0	0
DODIG	21	0	0	7	2		0	0	0	0		0	0	0	0
Total	9634	4329	234	507	1304		0	11	11	25		45	22	47	8

TOTAL SYSTEMS

APPENDIX C

Department of Defense
11th Quarterly Report to OMB
INTERFACES

Interfaces				Total Date:		Number of Interfaces with									
	Number of Interfaces	Number Impacted by Y2K	Number Fixed	% of MOAs Completed	100% of MOAs Complete	Internal to DOD	State Agencies	Local Govt	Other Dod	Federal Govt	Private Sector	Foreign Govt	Foreign Private		
Acronym															
ARMY	5075	2105	2105	100		4596	0	0	438	14	16	11	0		
DON	4199	1718	1718	100		3436	4	0	644	43	68	4	0		
USAF	2363	1721	1721	100		2175	0	0	177	6	4	0	1		
JS	43	0	0	0		28	1	0	13	0	1	0	0		
SOCOM	93	0	0	0		12	0	0	80	0	1	0	0		
USI	0	435	404	100		0	0	0	0	0	0	0	0		
DIA	0		0	0		0	0	0	0	0	0	0	0		
USD(A&T)	0		0	0		0	0	0	0	0	0	0	0		
BMDO	147	25	25	100		81	0	0	66	0	0	0	0		
DARPA	0	0	0	0		0	0	0	0	0	0	0	0		
DLA	190	2	2	100		2	0	0	185	0	1	2	0		
DTRA	18	14	14	100		14	0	0	4	0	0	0	0		
DFAS	2374	293	293	100		983	151	94	852	159	127	3	5		
DCAA	0	0	0	0		0	0	0	0	0	0	0	0		
USD(P&R)	75	0	0	0		2	50	0	21	2	0	0	0		
DeCA	25	9	9	100		18	0	0	4	0	3	0	0		
OASD/HA	197	73	73	100		114	0	0	75	0	8	0	0		
DSCA	51	0	0	0		15	0	0	35	1	0	0	0		
DSS	81	11	8	97		30	0	0	24	15	12	0	0		
DISA	159	159	159	100		53	0	0	41	33	19	13	0		
AFIS	0	0	0	0		0	0	0	0	0	0	0	0		
WHS	37	0	0	0		1	0	0	29	7	0	0	0		
DODIG	0	0	0	0		0	0	0	0	0	0	0	0		
Total	15127	6565	6531			11560	206	94	2688	280	260	33	6		

Department of Defense
11th Quarterly Report to OMB
EMBEDDED DEVICES

Agency Acronym	Devices Controlled by Information Technology and/or by Microchip					
	PCs & Servers			Comm Hardware/Software		
	Compliant	Unknown	Non-Comp	Compliant	Unknown	Non-Comp
ARMY	460,988		12,121	58,360		226
DON	636,975	0	26,095	70,043	0	5,960
USAF	304,472	0	16,783	138,146	0	4,605
JS						
SOCOM						
USI	17,025	0	261	248	0	11
DIA						
USD(A&T)						
BMDO	1,632	0	0	22	0	13
DARPA	515			257		
DLA	117,515	0	0	14,359	0	0
DTRA	2,707	0	0	483	0	0
DFAS	30,234	0	226	542	0	146
DCAA	4,652			383		
USD(P&R)						
DeCA	5,522		0	427		0
OASD/HA	99,457	0	4,800	16,954	0	0
DSCA	518			77		
DSS						
DISA	23,282			3,125		
AFIS						
WHS	15,237	0	0	1,749	0	0
DODIG	1,726		0	4		0
Total	1,722,457	0	60,286	305,179	0	10,961
					23	32,446



DEPUTY SECRETARY OF DEFENSE

**1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010**

18 AUG 1999



**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES**

413.51

SUBJECT: DoD Year 2000 (Y2K) Community Conversations

Historically, U.S. Military Service Members, DoD Civilians, and their families have always been strongly supportive of the communities in which they live and work. The Y2K challenge provides an opportunity to again demonstrate that commitment and further strengthen those relationships.

People are looking for straight talk about Y2K readiness in their own local communities. From power and phone companies to banks and water utilities, Americans want to know how the important local services upon which they rely may be affected by computers' ability to process the century date change.

I am directing that the Department actively support the President's Council on Year 2000 Conversion Community Conversations Program. Local gatherings enable citizens to hear directly from key service providers about the status of efforts to ensure that computers are ready for the date change and the work that remains to be done. They also provide an opportunity for citizens to raise questions or concerns they may have about the Y2K computer problem and enable communities to work together to identify areas where additional preparation and planning are needed. The campaign kicked off in June with several regional and local meetings held across the country.

12 Aug 99

012614 /99

I am asking the Secretary of each Military Department to support this effort and encourage major base, post, camp, and station commanders to engage and support their respective civic leaders and communities in holding Y2K Community Conversations. I understand that many military communities have already begun similar outreach efforts, and I applaud and support those proactive efforts. Accordingly, I have directed the Department's Year 2000 Office to support DoD's Y2K Community Conversations making available outreach materials, communicating with the President's Council and participating in events as requested by Commanders.

In the spirit of the American community and in the best traditions of the Armed Forces, I urge each of you to devote the time, talent, and resources necessary to make the President's Y2K Community Conversations Program a truly nation-wide success. Year 2000 Community Conversations will provide information necessary to plan for the date transition event, maximizing our readiness at home so that deployed forces can focus on exercising our national military strategy.



John J. Hamre



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



AUG 20 1999

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DEFENSE FIELD ACTIVITIES
CHIEF, NATIONAL GUARD BUREAU**

413.51

SUBJECT: Limitation on Configuration Changes to Y2K-Compliant Systems

The Department is engaged in a sustained and comprehensive program of Y2K system remediation, integration testing, functional end-to-end testing, and operational evaluations. The purpose of these efforts is to insure the Department will be fully mission capable throughout the millennium change.

The purpose of this memorandum is to ensure that configuration changes to date-dependent, mission critical systems do not add undue Y2K risk to, or undermine confidence in, system architectures that have been determined to be Y2K compliant. It provides combatant commanders (CINCs) and Principal Staff Assistants (PSAs) with visibility of, and veto authority over, configuration change proposals that may adversely impact such system architectures.

This policy pertains to any configuration changes to date-dependent, mission critical systems identified on CINC thin-line or PSA functional end-to-end architectures that would ordinarily come under the purview of a Configuration Control Board (CCB), including hardware, software, networking infrastructure, processed materials, services, and related technical documentation. The following procedures for obtaining approval for system configuration changes apply:

20 Aug 99

- Following CCB review and approval, system Program Managers (PMs) will submit proposed configuration changes, including Y2K risk analyses, schedules, and justification (e.g., warfighting, safety, environmental, contractual, legal) to affected CINCs and PSAs, through their program Executive Officer (PEO)/Designated Acquisition Commander (DAC), or equivalent.



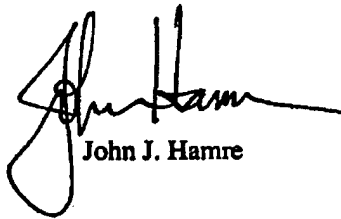
713305 /99

- CINC's and PSAs will have two weeks (minimum 10 working days) following receipt of the change proposal to approve or disapprove implementation. The intention is for the CINC/PSA to perform a quick risk/benefit assessment of the proposal and its impact on Y2K compliant system architectures. Failure to respond will be considered approval of the change.
- If there are multiple affected CINC's and consensus is not reached, the Chairman of the Joint Chiefs of Staff will resolve the differences. I will resolve the differences when a consensus cannot be reached among multiple, affected PSAs.

This process does not apply to changes needed to prevent Y2K failures or to restore system operations after failure.

Any configuration changes to tested Y2K-compliant, mission critical system architectures shall be documented in accordance with the DoD Y2K Management Plan. The DoD Inspector General will monitor and report to the DoD CIO on the efficiency and effectiveness of the above process.

This memorandum is effective 1 September 1999 through 15 March 2000.



John J. Hamre



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

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

August 22, 1999

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES**

SUBJECT: Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet)

The security of the Department of Defense's (DoD) information infrastructure is related to protection of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) against intrusion and malicious activity. Intrusion attempts are expected to increase as hackers may be tempted to masquerade their activities as Year 2000 (Y2K) bugs. Information assurance and network protection efforts hinge on identification, control and management of NIPRNet connections. Of particular interest and concern are the multitude of interconnections between the NIPRNet and the Internet. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, requires all DoD information systems, including networked computers, to comply with minimum security requirements. These security requirements pertain to any information technology (IT) system(s), regardless of the classification of the data processed.

Defense-in-Depth is the DoD approach to the protection of information systems. This memorandum describes the requirement for a significant piece of the overall DoD Defense-in-Depth strategy. However, DoD Components are cautioned that the protections described in this memorandum are only one layer of Defense-in-Depth and are not in and of themselves sufficient. Components must implement other protections per the Defense-in-Depth strategy as well. The use of firewalls or other technologies to provide higher levels of security between NIPRNet user enclaves is highly recommended.

The guidelines provided in Chairman of the Joint Chiefs of Staff memorandum CM-510-99, "Information Operations Condition" (INFOCON), March 10, 1999, require certain actions to be taken to increase the readiness posture for Information Warfare. Positive control of military connections to the Internet is required to support the setting of INFOCON conditions. This memorandum establishes the DoD policy that the only authorized access to the Internet is via the



NIPRNet. Certain situations may exist where a CINC, Service, or Agency may require a direct connection to the Internet or where near-term migration to the NIPRNet may not be feasible. Therefore, a waiver process shall be established that will consider each exception request individually and allow for the migration of systems to the NIPRNet over time.

The Defense Information Systems Agency (DISA) has established a number of NIPRNet gateways to the Internet, which will be protected and controlled by firewalls and other technologies. The level of protection provided by these, or equivalent, gateways can be increased in response to rising INFOCON conditions. All connections to the Internet, to include those that are provided by NIPRNet or those that have an OSD waiver, must meet or exceed the minimum security requirements contained in the implementation guidance to this memorandum.

Positive control of all NIPRNet-Internet connections is an absolute requirement. All connections to the NIPRNet will comply with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and be approved via the NIPRNet connection approval process. The implementation guidance accompanying this memorandum recognizes the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) as the body representing the DISN Designated Approval Authorities for security issues. Chaired by DISA and with representation from the Joint Staff, DISA, Defense Intelligence Agency, National Security Agency, Services, and the Joint Task Force - Computer Network Defense (JTF-CND), the DSAWG will set and maintain firewall policy, protocol controls, and overall minimum network security standards.

Unless specifically excluded below, Components shall terminate all direct connections to the Internet and establish connectivity to the Internet via the NIPRNet. Components shall develop a list of all direct connections with a suggested schedule for transitioning these connections by September 1, 1999. Working with DISA and ASD(C3I), Components will prepare a definitive transition plan by September 30, 1999, though implementation of portions of the plan can begin as early as feasible and agreed to. The goal is to have the transition complete and other protections in place by December 15, 1999, while avoiding operational degradation. Internet connections that cannot be terminated prior to December 15, 1999 or meeting one of the stated exclusions will need a waiver. Waiver requests shall explain how the non-NIPRNet-Internet connections meet the minimum security standards established by the DSAWG and be accompanied by a plan to transition the connection to the NIPRNet. Waiver requests and associated transition plans must be submitted to the DSAWG by October 15, 1999. The Components and DISA will brief the ASD(C3I) on progress and issues on a monthly basis beginning in August 1999. Detailed formats for reporting and waiver requests will be published in the implementation guidelines.

This directive does not apply to direct Internet connections for educational (off-duty or non-duty related) or morale, welfare, and recreational activities. These activities are not required to obtain Internet access via the NIPRNet. However, none of the Internet-connected networks, AISs, or individual computers used at these activities will be further connected to the NIPRNet. Direct connections to the Internet to support electronic commerce are permitted so long as those systems have a waiver or are not also connected to the NIPRNet.

This directive does not prohibit properly protected dial-in or dial-out modem pools, nor does it prohibit properly documented, protected connections to other networks that meet the security requirements of DoD Directive 5200.28 and this memorandum's implementation guidance. For example, interconnections between AISs where the Designated Approval Authorities for each AIS have completed a Memorandum of Agreement that details the interface security requirements are permitted. However, neither modem pools nor connections to other networks can be allowed to introduce backdoors (cross connections between the Internet and the NIPRNet) that weaken the intent of this memorandum. Connections are not permitted to interfere with the JTF-CND's visibility into and control of department connections to the Internet.

Uncontrolled Internet connections pose a significant and unacceptable threat to all DoD information systems and operations. Your continuous and active support is directed in eliminating this threat to the security and operational readiness of the Department. My point of contact in the Technical Services Directorate of the Year 2000 Program Office is Mr. Walter P. Benesch, telephone (703) 602-0983 ext. 129, email: beneschw@osd.pentagon.mil.



Arthur L. Money
Senior Civilian Official



POLICY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000



In Reply Refer to:
I-99/012944-PS

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Security Policy for DoD Y2K Information

Information that reveals the Y2K status of overseas operating locations, DoD dependence on host nation provided services, and the ability of host nations to provide services to the operating locations during the Y2K transition period must be afforded appropriate protection. Such information shall be treated in the following manner:

During collection, prior to aggregation:

- In accordance with Public Law 105-271, 112 Statute 2386, Section 4(f)(3)(A) (reprinted at 15 USC §1 note), Year 2000 Information and Readiness Disclosure Act, information that has been obtained under the auspices of a special year 2000 data gathering request is exempt from disclosure under subsection (b)(3) of section 552 of title 5, United States Code, commonly known as the "Freedom of Information Act", or FOIA, without the express written consent of the provider of the information. Such information shall be marked "For Official Use Only" and labeled on the bottom of each page.
- Information that is of a commercial or financial nature that has been obtained from a person and is deemed privileged or confidential shall be marked "For Official Use Only" and labeled on the bottom of each page. Per subsection (b)(4), "Confidential Business Information", this material is not subject to release under the FOIA.
- Information that is construed to be "working papers", where data has not been associated with the context material, shall be marked "For Official Use Only" and labeled on the bottom of each page. Per subsection (b)(5), "Internal Government Communications", this material is not subject to release under the FOIA.
- Information that reveals DoD overseas Y2K status and host nation support capabilities to DoD shall not be posted to unclassified websites.



Upon aggregation:

- This memorandum shall serve as classification authority to classify information which, when aggregated, renders an assessment of a specific military installation relative to Y2K vulnerabilities. Such assessments shall be classified **SECRET** pursuant to Executive Order 12958, paragraph 1.5(g). All information classified by this directive shall be declassified on 31 May 2000 unless deemed otherwise by competent authority.



Peter F. Verga
Deputy for Policy Support

Milestone Update for Assuring Year 2000 Readiness for Military Hospitals
Prepared for
The Office of Management and Budget (OMB)

The Military Health System and its military hospitals have met all of the milestones toward Year 2000 readiness. We are confident that military beneficiaries will receive world class healthcare at home and abroad through the transition to the Year 2000. A summary of the major MHS Y2K milestones and readiness is provided below, followed by a comprehensive table identifying accomplished MHS Y2K milestone activities and continuing communications initiatives.

- All MHS systems are Y2K compliant.
- All hospital computer networks are Y2K compliant.
- All systems have contingency plans in place. An independent validation and verification contractor has reviewed and approved each plan.
- End-to-end testing of MHS mission critical functions is complete. These tests included extensive interface testing with MHS managed care as well as medical supply partners. Both GAO and the DoD IG have audited the MHS end-to-end process and have produced favorable reports on the effectiveness of the tests.
- All military hospitals and clinics have continuity of operations plans in place.
- All PCs and Servers (386 and 486) on office LANs in use on 1 January 2000 will be compliant by 30 November 1999.
- All MHS Managed Care Support Contractor partners have provided letters of assurance that they will continue to provide all services throughout the transition to the Year 2000.
- Over 50 articles, news releases, interviews, posters, and pamphlets have been published to assure our beneficiaries and the public that the MHS is ready for Y2K.
- The MHS will continue to test, refine and verify all of its Y2K efforts right up until 31 December to ensure that nothing has been overlooked.

MHS READINESS	
CRITERIA	MILITARY HOSPITALS
System Compliance	✓ 100% Complete
End-to-end Testing	✓ 100% Complete
Contingency Planning	All Contingency Plans Tested ✓ 100% Complete
Data Exchanges	✓ 100% Complete
Informing the Public	Superb - Last Press Release (25 Oct)

Sharing Key Information on Readiness with Other Partners and the Public

Milestones	Partner/Event	Remarks
28 Feb 99	Health Care Providers	Health Care Provider letter posted on TRICARE web page – 8 March 1999 http://www.tricare.osd.mil/tricare/hcpartltr.html The letter informs health care partners that TRICARE will be ready for the Year 2000 transition and identifies key steps needed to prepare their practices for Y2K. The letter included a Y2K checklist to assess Y2K readiness. The letter was distributed to providers through prime managed care support contractor newsletters:

11th Quarterly Report to OMB

Milestones	Partner/Event	Remarks
		Anthem Alliance for Health, Inc. – 5 May 1999 Humana Military Health Services, Inc. – 5 May 1999 Tri West Healthcare Alliance – 10 May 1999 Sierra Military Health Services, Inc.- June/July 1999 Foundation Health Federal Services – 5 May 1999
29 Sept 99	Health Care Providers	Second Health Care Provider letter, signed by Dr. Sue Bailey, Assistant Secretary of Defense (Health Affairs), on 22 September 1999, posted on TRICARE web page on 29 September 1999. The letter informs health care partners that TRICARE has successfully completed Y2K preparation and testing and provides a guide of steps to take to ensure their practice is Y2K ready. The letter was distributed to prime managed care support contractors for dissemination to medical and dental care providers. Anthem Alliance, Sierra, and TriWest published the letter in their newsletters, disseminated by October 31; Foundation's newsletter went out November 8. Humana had a special mailing on October 20.
30 April 99	Managed Care Support Contractors (MCSC)	Compliance assurance and Y2K assistance site visits: Visits confirmed Y2K preparedness plans of the Managed Care Support Contractors. *Palmetto Government Benefits Administrator Columbia SC – 10-12 March 1999 Sierra Military Health Services, Inc. Baltimore MD – 17-18 March 1999 Foundation Health Federal Services Rancho Cordoba CA – 24-25 March 1999 *Wisconsin Physicians Service Madison WI – 29-30 March 1999 **Iowa Foundation Des Moines IO – 1-2 April 1999 Humana Military Health Services, Inc. Louisville KY – 7-8 April 1999 Anthem Alliance for Health, Inc. Indianapolis IN – 15-16 April 1999 Tri West Healthcare Alliance Phoenix AZ – 19-20 April 1999 *subcontractor to MCSC for claims processing **Tricare Senior Prime and Medicare claims processor
17 May 99	White House Pharmaceutical Summit	Participated in summit - 17 May 1999. Resulted in MHS pharmacy policy to reinforce standard pharmacy practices in the MHS. Detailed information is available at http://www.tricare.osd.mil/y2k/ipt/pdf/pharm2.PDF and http://www.y2k.gov/new/0614guid.htm
15 June 99	Health Policy Workshop	Dr. Sue Bailey, the Assistant Secretary of Defense

11th Quarterly Report to OMB

Milestones	Partner/Event	Remarks
		(Health Affairs) chaired the Military Health System (MHS) Year 2000 (Y2K) Table Top Exercise (TTE) held on 15 June 1999. After being presented with several simultaneous Y2K disruption scenarios surrounding 1 January 2000, the participants addressed policy, priority and resource decisions to sustain the MHS' ability to execute its mission. Military Health System and senior executive participants included: • Deputy Assistant Secretaries of Defense • Military Health System Chief Information Officer • Army, Navy, Air Force Deputy Surgeons General • Presidents and Chief Executive Officers of the Managed Care Support Contractors, and • Representatives from: the Office of the Secretary of Defense, Uniformed Services University of Health Sciences, the President's Council on Y2K Conversion, and the Department of Veterans Affairs.
Ongoing	Managed Care Support Contractors	Dissemination of Y2K readiness information to beneficiaries through MCSCs' quarterly newsletters; performed end-to-end testing with MCSCs to ensure all healthcare related systems are Y2K ready and shared lessons learned during weekly Interface Working Group meetings. Executive-level quarterly meetings to discuss the Y2K progress of TRICARE's supplemental health care services (private sector health care)
Ongoing	Health Care Sector Outreach Program	Outreach semi-monthly report – 15 October 1999 and 31 October 1999 provided to HHS to inform the Health Care Sector Outreach Program of MHS Y2K activities supporting the White House Y2K conversion team.
Ongoing	Veterans Health Administration	Conferences, meetings, information exchange
Ongoing	Department of Health and Human Services	Outreach events
Ongoing	Food and Drug Administration Biomedical Clearinghouse	Meetings and submission of updated MHS biomedical equipment database
Ongoing	Pharmaceutical industry	Participated in White House Pharmaceutical Summit– 17 May 1999 Produced the DoD Pharmacy Y2K Transition policy, signed 28 June 1999 by Dr. Sue Bailey, the Assistant Secretary of Defense (Health Affairs). The policy reconfirms the White House summit conclusions and directs providers and pharmacists to provide consistent reassurance to our beneficiaries that their prescription drugs will remain available through the Y2K transition and encourage them to refill their prescriptions on schedule, 5-7 days before their medication runs out. The DoD policy is found in the www at: http://www.tricare.osd.mil/y2k/ipt/pdf/pharm2.PDF Participated in the White House Y2K Roundtable on Consumable Medical and Surgical Supplies – 7 June 1999. Some of the topics discussed included: effects of stockpiling and hoarding, effects of artificial shortages on patient care, methods of communicating Y2K compliance

11th Quarterly Report to OMB

Milestones	Partner/Event	Remarks
		effectively, and methods of developing Y2K inventory management plans between customers and suppliers.

Medical Facility Readiness Assessments

Milestones	Event	Remarks
30 June 99	Medical Facility Self-Assessments	Self-assessment checklist complete
31 July 99	Medical Facility Self-Assessment Evaluation	Medical Facilities performed a self-assessment with the checklist to prepare for Y2K.
31 Aug 99	On-site Medical Facility Assessments	Assessments and assistance visits to representative DoD hospitals were conducted to assist the sites in the Y2K preparedness. Assist visits performed at following Military Treatment Facilities. The lessons learned from these visits were shared with other sites. Walter Reed - 8-11 June Ft Belvoir - 22-24 June NH Beaufort - 29 June-1 July Ft Gordon - 29 Jun-2 July Ft Rucker - 6-9 July Wuerzburg, GE - 12-16 July NH Lemoore - 12 July-16 July Heidelberg, GE - 12-16 July Landstuhl, GE - 17-23 July NH Bremerton - 19-23 July Vicenza, IT - 26-29 July NH 29 Palms - 26-29 July Ft Polk - 27-30 July Ft Huachuca - 10-13 Aug USNH Naples, IT - 10-13 Aug USNH Sigonella, IT - 16-18 Aug Ft Eustis -17-20 Aug Ft Lee - 17-20 Aug USNH Rota, SP - 20-24 Aug Ft Riley - 24-28 Aug USNH Keflavik, IC-27 Aug-1 Sep USNH Yokosuka, JA - 6-10 Sep USNH Okinawa, JA - 13-16 Sep Seoul, SK - 13-18 Sep USNH Guam - 19-22 Sep NNMC Bethesda - 28 Sep-1 Oct

Functional Readiness Assessments (FRA) (End-to-end Testing)

Milestones	Event	Remarks
30 Sep 99	Functional Readiness Assessments (Total)	100% complete All Mission Critical Threads and Sub-threads successfully tested. Dates tested = FY 2000, CY 2000,

11th Quarterly Report to OMB

Milestones	Event	Remarks
		LY 2000
30 July 99	Patient Administration FRA The patient administration processes tested are concerned with enrollment, appointment, eligibility, and claims processing and involve the following: <u>Key partners:</u> Palmetto Government Benefits Administrator Sierra Military Health Services, Inc. Foundation Health Federal Services Wisconsin Physicians Service Humana Military Health Services, Inc. Anthem Alliance for Health, Inc. Tri West Healthcare Alliance <u>DoD system:</u> Defense Eligibility and Enrollment Reporting System (DEERS) <u>MHS systems:</u> TMA-Aurora's Central Deductible and Catastrophic Cap File (CDCF) Composite Health Care System (CHCS)	100% complete All Mission Critical Threads successfully tested
30 July 99	Patient Care FRA The patient care processes tested are concerned with diagnosis, treatment, and immunizations and involve the following systems: <u>DoD system:</u> Defense Eligibility Enrollment Reporting System (DEERS) <u>MHS systems:</u> Composite Health Care System (CHCS) Defense Blood Standard System (DBSS) 16 high-volume laboratory instruments Comprehensive Clinical Evaluation Program (CCEP) Clinical Information System (CIS) Preventive Health Care Application (PHCA) Aeromedical Service Information Management System (ASIMS) Military Occupational Data System (MODS)/ Shipboard Nontactical Automated Data Processing (ADP) Program (SNAP) — Shipboard Automated Medical System (SAMS)	100% complete All Mission Critical Threads successfully tested
30 Sep 99	Medical Logistics FRA The medical logistics processes tested are concerned with the delivery of pharmaceutical and surgical supplies. Five medical supply companies comprise approximately 85% of the MHS' medical supply business. <u>Key Partners:</u> Bergen Brunswig Medical Corporation (pharmaceutical) McKesson Drug Company, Inc. (pharmaceutical) Bindley Western Drug Company, Inc. (pharmaceutical) Owens and Minor (medical surgical devices)	100% complete All Mission Critical Threads successfully tested

11th Quarterly Report to OMB

Milestones	Event	Remarks
	Durr (medical surgical devices)	

MHS Contingency and Continuity of Operations Plans

Milestones	Event	Remarks
31 Dec 98	Contingency Plans for Mission Critical Information Systems	Complete
31 Mar 99	Contingency Plans for Non-Mission Critical Information Systems	Complete
31 Aug 99	TRICARE Y2K Continuity of Operations Plan (COOP)	Version 2.0 was distributed on 11 June 1999 for review. Comments and recommendations resulting from this review and from the testing/validation of the plan at the MHS Y2K Table Top Exercise were incorporated into version 3.0. Version 3.0 released 31 August 1999. This product is ready for use during the Y2K transition.
30 Sep 99	Y2K COOP Operational Evaluations	The military hospitals capitalized on the requirement for semi-annual Joint Commission on Accreditation of Health Care Organizations (JCAHO) exercises of emergency preparedness plans. Sites completed exercising emergency preparedness plans on 30 September 1999.

Communications Initiatives to Keep the Public Informed

Milestones	Event	Remarks
March 99	Draft initial materials: fact sheets, FAQ document	Three fact sheets complete and posted on the Y2K section of the Health Affairs web page: generic Y2K, administrative services, and pharmacy.
March 99	News releases for 31 March 1999 milestone	Two press releases issued: Military Health System Nears Goals for Y2K Compliance – 5 March 1999 and MHS on Track for Y2K Compliance - 31 Mar 99
April 99	Media Interview and Resulting Article	Interview with American Forces Information Service reporter – 25 March 1999 19 April 1999 article: Military Health System Treats Y2K Symptoms, posted on the DefenseLINK web site http://www.defenselink.mil/ and linked to TRICARE home page
April 99	Complete comprehensive communications plan	Complete
April 99	Initial TRICARE Y2K newsletter prepared and	The first edition of the MHS Y2K

11th Quarterly Report to OMB

Milestones	Event	Remarks
	distributed	newsletter was approved and released in June. The newsletter is intended to inform military beneficiaries and providers of the actions being taken to fortify the MHS against any Y2K interruption. The newsletter's distribution includes the Army, Navy, and Air Force medical departments, MHS regional leaders, military hospitals, and MHS purchased care partners – the TRICARE Managed Care Support Contractors. Each of these organizations will forward the newsletters to beneficiaries and providers. To expand the reach of the newsletter, it also will be placed on the Health Affairs web site and provided to media organizations such as Armed Forces Information Service and the Army, Navy and Air Force public affairs offices.
May 99	Media Interviews & Briefings and Resulting Articles	Interview with American Forces Information Service reporter – 3 May 1999 TV spot on AFIS stations. Briefing for trade press (Service Times, US Medicine, Federal Computer Week, American Forces Information Service) 19 May 1999 Article posted to FCW web site 19 May 1999 Military Health System on Track for Y2K Compliance – 31 March 1999 Health Officials Claim Y2K Readiness – 7 June 1999, Air Force Times, Marine Corps Times
May 99	Briefing for the Military Coalition and the National Military and Veterans Alliance	Conducted 26 May 99, each representative provided binder with fact sheets, FAQ, and newsletter
June 99	Updated Materials	Five fact sheets completed and posted on the TRICARE web site: Biomedical Equipment, Facility Y2K Readiness, MHS Leadership Engaged in Planning, DEERS, and End-to-End Testing. Q&As expanded and posted on TRICARE web site.
August 99	Created Y2K posters and handouts for Military Hospitals	Posters and handouts are displayed in military hospitals and clinics worldwide and will further re-enforce beneficiary confidence in the MHS.
October 99	Posters and Handouts distributed to all military hospitals	Distributed week of 18 October 99

11th Quarterly Report to OMB

Milestones	Event	Remarks
October 99	Media Briefing	MHS Y2K Program Manager was interviewed by American Forces Press Service on 15 Oct. The interview included a Y2K update, focusing on progress to date, effectiveness of end-to-end testing of mission critical and non-mission critical systems, and the final preparations for ensuring that uninterrupted quality healthcare is available for beneficiaries worldwide. The resulting article has been distributed to Service publications and was posted on DoD's DefenseLINK web site on 26 Oct 99.
October 99	Second newsletter prepared and distributed	Second edition of the MHS Y2K newsletter was released in October and posted on the TRICARE Y2K web site on October 12. The lead article stressed that the Military pharmacy system is prepared for Y2K. The newsletter's distribution includes the Army, Navy and Air Force medical departments, MHS regional leaders, military hospitals and our purchased care partners, as well as the American Forces Information Service and the Services' public affairs offices.
October 99	Informational Video production initiated	Video designed to play on cable stations in and around military installations as well as in military hospital waiting rooms. Production underway. Completion expected in mid November
November 99	Y2K Video disseminated to military medical facilities	
Ongoing	TRICARE Y2K Web site	http://www.tricare.osd.mil/y2k/year2000.html To relay a clear Y2K message to our military beneficiaries, the MHS Y2K Project Office has redesigned the Y2K section of the Health Affairs web page. The new web pages include fact sheets on MHS Y2K preparedness, health computer systems Y2K status, and advice on filling prescriptions during the transition to the year 2000. In addition, press releases and answers to frequently asked questions are displayed on the web pages. A news advisory, sent to over 5,000 outlets, announced the update of the Y2K section of the Health Affairs

11th Quarterly Report to OMB

Milestones	Event	Remarks
		web page. A Pharmaceutical Section was added to the TRICARE Y2K web site in early October. The section carries a pharmacy fact sheet advising continued routine practices for filling prescriptions, frequently asked questions and a "to do" list, giving prudent steps to ensure beneficiaries are prepared for any medical situation. Latest update: 12 October 1999
January 2000	Media briefing on impact of Y2K date change on MHS	
January 2000	Update Briefing for The Military Coalition and National Military and Veterans Alliance	

***Milestone Update for Assuring Year 2000 Readiness for Defense Finance and
Accounting Service
Prepared for the Office of Management and Budget (OMB)***

High Impact Systems

Milestones	Partner/Event	Remarks
Completed	Defense Retiree and Annuitant Pay System	100% complete DRAS-APS, Annuitant application was certified as a Y2K compliant application on December 31, 1998
Completed	Defense Retiree and Annuitant Pay System	100% complete DRAS-RCP, Retiree application was certified as Y2K compliant on April 9, 1999
Completed	End to End Testing	100% complete DRAS-APS and RCP have completed the requirement for end to end testing
Completed	Contingency Plans	100% complete Contingency Plans for DRAS-APS and RCP are established and have been tested.

All DFAS Systems

Completed	All DFAS System Compliance	100% complete All DFAS systems are compliant by 30 September 1999. In addition, DFAS has replaced or retired 64 systems during the Year 2000 initiative.
Completed	Interface Agreements	100% complete All DFAS interface agreements have been signed. There are in excess of 1400 agreements.
Completed	End to End Testing	100% complete One End to End Test has been conducted on all 42 DFAS mission critical systems.
Completed	Additional End to End Testing	100% complete All DFAS 42 mission critical systems have completed at least one end to end test, and most have completed multiple testing. These tests involve all critical interface partners such as the Federal Reserve Banks, IRS, Social Security, Services, and other DoD Agencies. The majority of the additional tests were completed by the end of September with an independent verification and validation of the process following completion of each of the testing events. To date, DFAS has accomplished all requirements for end to end testing specified in the GAO testing Guide (one test for each mission critical system). In addition, DFAS has completed multi-scenario end to end testing. Although the requirement is to test each mission critical system only once, the DFAS strategy involves each mission critical system in multiple end to end testing scenarios. These additional testing processes enhance DFAS' level of success for Year 2000.

Completed	Contingency Plans	100% complete Contingency plans are in place for DFAS systems and critical business processes. Plans have been tested to ensure viability.
Completed	DFAS rollover	100% complete All DFAS systems and supporting networks will be backed up prior to rollover and will be available for production on January 1, 2000.

Pay Systems

Completed	Pay Application Compliance	100% complete All DFAS pay systems for civilian, military, retiree/annuitant, vendor/contractor, transportation and travel are Y2K compliant.
------------------	----------------------------	---

Public Affairs

Completed	Presentations	
1/12/1999	Consortium of Military Associations	Addressed legislative/governmental affairs members representing 25 military associations.
2/20/1999	Customer Service, Orlando	Update on retirees, annuitants, active duty and reserve service members and civilians.
3/23/1999	Customer Service, Cleveland	see above
3/25/1999	Customer Service, Columbus	see above
7/21/1999	Customer Service, Charleston	see above
7/27/1999	Customer Service, Charleston	see above
1/12/1999	Congressional	Addressed professional committee staff from the Senate Armed Services Committee
Completed/ Ongoing		100% Complete according to schedule Numerous presentations and briefings have been conducted for various groups since April 1999. Others are planned through 1999.

Media

Jan-99	Retired Officer's Association	100% complete News release (DFAS Press Release 99-10) announcing the Y2K 100 percent ready status for the Overseas Military Banking Program Contractor Bank of America. This release was issued to all the Services' publications and Stars and Stripes.
Feb-99	DFAS Magazine	100% complete News release (DFAS Press Release 99-11) announcing that DFAS has every confidence that all DoD civilian, military members and retirees will get paid after January 1, 2000. This release was issued to all the Services' publications for retirees.
Mar-99	American Forces Information Service	100% complete Interview for print and video with DFAS Director on compliance and contingency. Broadcast to overseas audience and print to all publications in DoD.
Mar-99	Military Report	100% complete Story on compliance and contingency

May-99	Afterburner, Military News Services	100% complete Ran stories on DFAS compliance covering retiree and annuitant interests.
Jun-99	Soldiers Magazine	100% complete Article on DFAS Y2K status for pay systems
Aug-99	News Release	100% complete News release (DFAS Press Release 99-10) announcing the Y2K 100 percent ready status for the Overseas Military Banking Program Contractor Bank of America. This release was issued to all the Services' publications and Stars and Stripes.
Aug-99	News Release	100% complete News release (DFAS Press Release 99-11) announcing that DFAS has every confidence that all DoD civilian, military members and retirees will get paid after January 1, 2000. This release was issued to all the Services' publications for retirees.
Oct-99	News Release	100% complete News release on Defense Retiree and Annuitant Pay System stating that all testing for compliance, end to end and contingency has been completed.

Other

Complete	Currency	100% complete DFAS in conjunction with the Department of State is ensuring that overseas banks covered under the Overseas Military Banking Contract will have sufficient U.S. and foreign currency available. The Overseas Military Banking Contract system is Y2K compliant and provides services to OCONUS military personnel and dependents, military disbursing officers, DoD civilian personnel and dependents, Defense Credit Unions, organizational clients (exchanges, commissaries, nonappropriated fund instrumentalities) and other Federal Agencies.
Complete Updated Ongoing	DFAS Website	100% complete dfas.mil/y2k/ Web site contains answers to frequently asked questions, system status, points of contact, and an article on retirees.
Plans Complete/ Operations Ongoing	Transition Operations	Plans 100% complete Operations ongoing Pre-position payroll tapes Pay contract invoices upon receipt prior to rollover Generators in place Essential and critical employees in place Orderly backup and restart of systems and networks

11th Quarterly Report to OMB
Validation and Verification Methods

Describe how and to what extent internal performance reports are independently validated.	Describe Y2K readiness of Government-wide systems your agency operates.
ARMY All systems are required to complete a Year 2000 certification checklist as proof of compliance. This certification requires coordination and signature by the systems developer, the applicable functional proponent, and for mission critical systems, the General Officer/Senior Executive Service owner. Each system owner is required to plan and implement the requisite verification process, tailored to specific system requirements. In addition, the Army Audit Agency (AAA) is conducting independent program and process reviews and audits on specified Army systems, using the Army certification checklist as the evaluation basis. In addition, AAA is evaluating and reviewing systems that have submitted signed certification checklists.	
DON All mission critical systems and all Y2K vulnerable systems undergo rigorous system and functional testing. Critical operational systems are validated in Fast Cruises, Weapons System Readiness Testing (WSRT), Marine Corps Operational Evaluations (OPEVAL), Battle Group Systems Interoperability Testing (BGSIT) and a formal Joint Staff Operations Evaluation (OPEVAL) process prior to fleet release. Most Naval mission critical systems have designated testing facilities that are independent of the developing agent or support activity. Testing of major mission critical systems is conducted using a formal, documented independent verification and validation (IV & V) process. For mission critical personnel and major training systems, contractors are performing 100% code checking. The Navy and Marine Corps use government personnel to perform routine spot checks to validate the work coming back from the contractors that performed validation. The Naval Audit Service validates test procedure methodologies and results for accuracy. The Department has established a "code checking" program using COTS computer engineering tools for code quality assessment.	

11th Quarterly Report to OMB
Validation and Verification Methods

USAF	
I. Independent Validation/Verification (IV&V) that is taking place is being accomplished by: * In-house independent test teams using software scanning tools--independent of the teams that performed development or renovation. * Air Force test teams external to the system owning organization--Air Force Operational Test & Evaluation Center (AFOTEC), is providing technical support to test directors. * Contractor test teams--Air Mobility Command hired a contractor to perform IV & V on their renovated systems. * Software code verification tools--Air Force functionals hired contractors to conduct IV & V of renovated code. II. Independent testing is being determined by program managers, commanders, and certifiers based upon accepted system risk and system mission criticality. III. System testing will, at a minimum, include those dates contained in the DoD Y2K management Plan, dated December 1998, and regression testing. 1999 has been set aside as the year in which system interoperability will be tested. IV. The Air Force Communications Agency (AFCA) Y2K Program Office at Scott AFB, IL established Certification Strike Teams. These teams provide hands-on customer focused assistance to MAJCOMS and organizations having immediate Y2K needs. These teams already visited over 150 organizations world-wide. V. The AF Audit Agency and the DoD IG continue inspections at multiple sites across the Air Force. All units recently began a Special Interest Item (SII) self inspection, under the auspices of the AF Inspection Agency. The focus of the SII is configuration assurance and management. VI. On 30 June 99, AF installation commanders completed and signed an Installation Certification checklist certifying that critical base utilities and infrastructure equipment had been assessed, fixed, and tested and that Contingency Plans and COOPs are in place to deal with unexpected failures.	Global Positioning System (GPS) is an Air Force owned Government wide system. It is being handled the same as any other Air Force system: * Required to be certified under the Air Force Certification Process. * Tracked in the Air Force Y2K database. * Interfaces, both internal and external are tracked in the database with agreements or control documents. * Help desk is available to answer questions for governmental and commercial users. * The three operational blocks of GPS satellites as well as ground support equipment and user interfaces have been tested.

11th Quarterly Report to OMB
Validation and Verification Methods

JS	Users are validating systems based on the DoD Management Plan's and the Joint Staff Action Plan's certification checklist. Systems are using additional testing and verification methodologies as required which differ from system to system. The Unified Command's methods for independent verification of Y2K compliance are obtained by a combination of one of the following: 1. vendor testing and verification before delivery; or 2. maintenance contractor testing and verification; or 3. In-house maintenance staff testing and verification and one of the following: a. Acceptance testing at delivery; or b. Pilot testing for an extended period before acceptance; or c. Inspector General validation that applicable tests were done and results show the product is Y2K compliant. Testing for Y2K compliance will, at a minimum, include those dates contained in the DoD Y2K Management Plan, Version 2 dated December 1998 and regression testing.	Currently, the Unified Commands do not have reporting responsibilities for any Government-wide systems. However, the USAF may be reporting systems which are operated or administered by TRANSCOM, STRATCOM, and SPACECOM.
SOCOM		
USI		
DIA		
USD(A&T)		
BMDO	Explanation of Embedded Devices: (Non-Compliant)- there are 13 usable systems that are Non Y2K Compliant. They are located at the JNTF in Colorado Springs. JNTF is awaiting final disposition as they have contacted various organizations to see if they desire them. Upon notification, JNTF will then dispose of them.	
DARPA	All internal systems are COTS. Internal system Y2K performance reports are validated by maintenance contractor testing and verification, and pilot testing for an extended period before acceptance. Testing for Y2K compliance will, at a minimum, include those dates contained in the DoD Y2K Management Plan, Version 2, April 1998, and regression testing.	DARPA operates no government wide systems.

11th Quarterly Report to OMB
Validation and Verification Methods

DLA	Independent verification of Y2K compliance is obtained by in-house maintenance staff testing and verification and acceptance testing at delivery; or Functional User, Independent Contractor and in some cases JITC. Testing for Y2K compliance will, at a minimum, include those dates contained in the DoD Y2K Management Plan, Version 2, dated April 1998, and regression testing.	DLA has three Government-wide systems: Defense Automated Address System (DAAS), Federal Logistics Information System (FLIS) and Joint Total Asset Visibility (JTAV). DAAS, FLIS and JTAV applications have been certified and implemented Y2K compliant.
DTRA	As per Appx A of the DoD Y2K Management Plan, IV & V is achieved in DTRA by 1) Audit or testing by independent contractor or national laboratory or 2) As part of acceptance testing by the program manager when the systems have been tested by a contractor.	DTRA does not operate any Government-wide systems such as FTS2000 and GPS.
DFAS	The DoD Inspector General has conducted site visits at various DFAS locations to review randomly selected systems. Outside contractors, such as JITC, have been used to validate some systems. DFAS contracted with other agencies/contractors to conduct IV&Vs using automated tools, e.g., Air Force's Systems Support Group (SSG) and JITC.	1. Centralized Expenditure/Reimbursement Processing System (CERPS), used by Dept of Agriculture, Coast Guard, and State Dept is Y2K compliant. 2. Defense Civilian Pay System (DCPS), civilian payroll function used by Executive Office of the President (EOP) is Y2K compliant 3. Defense Retiree and Annuitant Pay System (DRAS), used for viewing only by Arlington National Cemetery was implemented is Y2K compliant. 4. Financial Reporting System (FRS), used by the Coast Guard and State Dept is Y2K compliant.
DCAA		
USD(P&R)		
DeCA		
OASD/HA	Health Affairs is using an IV&V contractor, in coordination with the Information Management, Technology, and Reengineering (IMT&R) and Business Area Y2K teams, to review evidentiary performance and process documentation, and to assist with providing Y2K compliance assurance for active Health Affairs automated information systems.	Health Affairs operates no Government-wide systems.
DSCA		

11th Quarterly Report to OMB
Validation and Verification Methods

In-house maintenance staff testing and verification and acceptance testing at delivery	
DSS	
DISA	
Signed (Functional Manager, System Manager, and Validator) are required for all system certifications. Most have been audited by independent audit organizations (GAO, DOD IG, DISA IG) and OCIO.	ALL DISA Systems are Y2K compliant and fully implemented.
AFIS	
WHS	
The OSD and WHS components are using a variety of methods in order to independently validate systems as Y2K compliant. In some cases, contractors will be validating the Y2K compliance of systems. Some OSD & WHS systems will be independently validated through the audits done by the Inspector General (IG). Using a methodology similar to the IG's, OSD & WHS is also considering the possibility of allowing one OSD or WHS component to serve as an independent validator for another OSD or WHS component's systems. Another possibility involves training the Enterprise Support Organization (ESO) to perform independent validations on OSD & WHS compliant systems.	The OSD & WHS components do not operate any Government-wide systems.



Department of Defense
High-Level Plan

**Business Continuity and
Contingency Planning
(Updated)**

Submitted to
Office of Management and Budget

November 15, 1999

11th Quarterly Report to OMB

Table of Contents

Introduction	1
DoD's 1998 Focus – Fixing Systems.....	2
Management Focus.....	2
DoD Year 2000 Management Plan.....	2
Effective Senior Management Oversight.....	2
CEO Involvement	2
Accurate Reporting Mechanisms	3
DoD's Leadership Focus for 1999 – Ensuring Mission Capability.....	3
Evaluation and Testing of Capabilities.....	3
Operational Readiness Evaluations	4
Functional End-to-End Evaluations.....	5
Integration Testing.....	5
DoD Y2K Continuity and Contingency Planning	6
Business Impact Analysis	7
Core Functions	7
Planning Assumptions.....	7
General Planning Assumptions	7
CONUS.....	7
OCONUS.....	8
Site-Specific Planning Assumptions	8
Other Risks to DoD Operations.....	8
Domestic Infrastructure Disruptions.....	8
Host Nation Infrastructure Support Disruptions	8
NATO/Allied Systems Interoperability Disruptions	8
Contingency Planning Oversight and Tracking.....	8
System Contingency Plans.....	8
Operational Contingency Plans	9
DoD Y2K Day One Planning	9
Year 2000 Transition Period/Day One	9
Leadership Preparation for Decision-Making	10
CJCS Contingency Assessments.....	10
Consequence Management Planning	12
Conclusion.....	13

11th Quarterly Report to OMB

List of Figures

Figure 1 – DoD Combatant Command Operational Evaluation Activities in 1999	4
Figure 2 – DoD Functional End-to-End Evaluations in 1999	5
Figure 3 - Overall Year 2000 Table Top Exercise (TTE) Concept.....	11
Figure 4 - DoD Operational Readiness and Consequence Management Priorities.....	12

Introduction

There are four major components of the DoD Year 2000 Program: Systems Compliance – making sure all individual systems are Year 2000 compliant in accordance with the OMB five-phase process; Operational Evaluation/Testing – to buy increased assurance that our systems work in the real world; Contingency Planning – taking prudent precautions in case systems or capabilities become unavailable due to Year 2000 related problems; and Transition Period Operations – managing the remaining challenges and reporting and responding to Year 2000 related events. This document will focus on the last two of these components and address DoD Business Continuity and Contingency Planning (BCCP) Efforts and Day One Planning. It reiterates essential elements of the four major documents guiding DoD efforts on the Y2K problem:

- DoD Year 2000 Management Plan, version 2.1, September 1999.
- 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) and Day One Planning 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 and Day One Planning efforts in detail.

The scope and complexity of the Y2K problem for the DoD is unparalleled in the federal government. The Department of Defense has over 3 million people – active, Guard, Reserve, and civilian – spread all over the world. To administer this community takes over 1.5 million individual computers at hundreds of locations around the globe. As of the Monthly Report to the Office of Management and Budget (OMB), submitted on October 15, 1999, DoD has 9,480 systems, of which 25 percent (2,369) are 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 Y2K problems. In addition, the Department will have 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. Over one-third of the government’s mission critical systems are in the Department of Defense.

DoD’s first priority is to execute the national military strategy. To ensure that capability, the Department has established and promulgated priorities and procedures for managing Military Support to Civil Authorities (MSCA) and Foreign Disaster Assistance (FDA) with the normal channels. The Department will use normal channels to report and process requests for assistance, which involve the Federal Emergency Management Agency for MSCA and the Department of State for FDA. In addition, DoD continues to work with the President’s Council

11th Quarterly Report to OMB

on Year 2000 Information Coordination Center on the information required and procedures for Year 2000 related information.

In summary, despite the enormity of the problem, DoD will be ready for the Year 2000. The remainder of this document provides more details on DoD contingency planning and Day One/Transition Operations.

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 Y2K.

Management Focus

The Department's 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 Year 2000 Management Plan

The Department developed and published a Y2K management plan that specified component responsibilities and outlined how to achieve Y2K 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 Y2K Steering Committee meeting to review 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 means to reinforce that Y2K 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 Y2K 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.

11th Quarterly Report to OMB

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 Y2K 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 Y2K 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 exercising, and preparing for operations in the period surrounding Y2K transition. These were reviewed by the Secretary of Defense in a meeting held on July 21, 1999.

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. The DoD is concentrating on complex, real-world end-to-end testing of "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 (PSAs) of the Office of the Secretary of Defense (OSD), and the Commanders in Chief (CINCs) of Unified Commands.

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

11th Quarterly Report to OMB

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 General Accounting Office (GAO) provides 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 1 below.

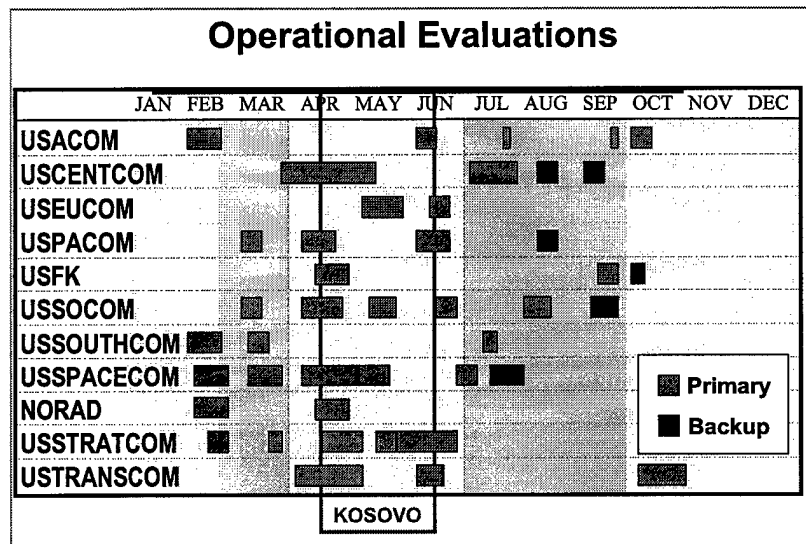


Figure 1 – DoD Combatant Command Operational Evaluation Activities in 1999

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. Results confirm that this kind of evaluation is essential to providing the additional assurance that systems will remain operational over the Y2K transition.

11th Quarterly Report to OMB

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 Y2K. 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 2 below.

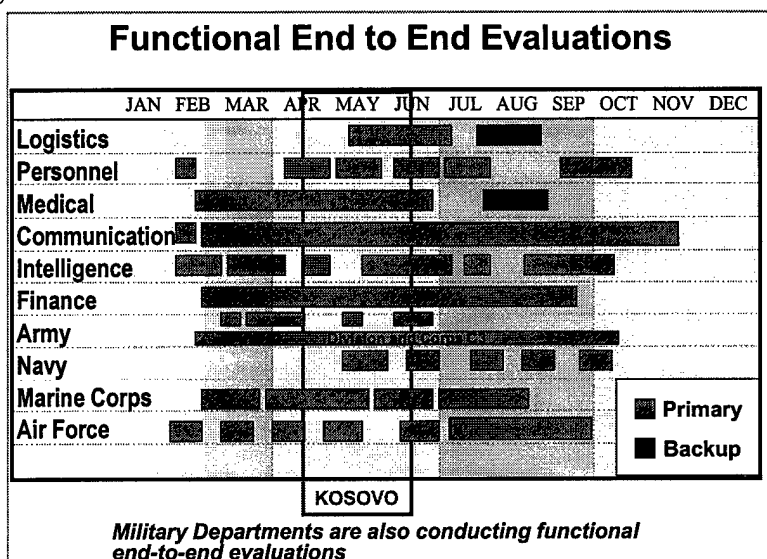


Figure 2 – DoD Functional End-to-End Evaluations in 1999

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 Y2K 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

11th Quarterly Report to OMB

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, DoD has issued a configuration management policy to ensure DoD maintains the hard won confidence in systems that will result from this comprehensive series of evaluations. The underlying tenet is a coordinated approach to configuration control involving the CINCs, PSAs, Services, and the OSD and Joint Staffs.

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 Y2K. While these extensive efforts will mitigate risk, the interconnectedness of everything guarantees that Y2K 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

11th Quarterly Report to OMB

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.

11th Quarterly Report to OMB

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

11th Quarterly Report to OMB

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.

DoD Y2K Day One Planning

Year 2000 Transition Period/Day One

The Department of Defense is well prepared for Day One operations. Throughout DoD, elements are continuously conducting reporting and responding to situations all over the world, all of the time. In fact, 24 hours a day, 7 days a week is the norm for DoD operations centers. Operational reporting procedures are in place, robust, and frequently exercised in real world operations. The Department is tuning these procedures to address the information technology and critical infrastructure issues that may be raised by Year 2000 problems. In addition, the Department is taking prudent "Day One" measures to ensure key personnel availability; prepositioning of key response assets; and availability of redundant communications throughout the date transition period. In fact, because of the wide range of dates that may generate information technology problems, DoD designated the period September 1, 1999 through 31 March 2000 as the date transition period. While most of the focus thus far has been on the 31 December 1999 to 1 January 2000 date roll over, DoD is also planning for a similar focus on the leap year transition in February of 2000. To prepare for the unprecedented nature of possible Y2K problems, DoD is developing procedures to ensure its ability to identify, report, and respond effectively to Y2K-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."

11th Quarterly Report to OMB

- Developing a strategy to ensure that DoD resources are applied in the most effective and efficient manner possible.
- Developing specific Y2K training materials to ensure everyone involved in MSCA knows the specific methods for dealing with Year 2000-related requests.
- Refining its procedures for ensuring real-time decision support information 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 Y2K contingencies and to evaluate the Department's operational contingency plans.

Leadership Preparation for Decision-Making

There were two major activities in preparing DoD leadership for dealing with Y2K: Chairman of the Joint Chiefs of Staff (CJCS) Contingency Assessments and Table Top Exercises

CJCS Contingency Assessments

The CJCS conducted Exercise POSITIVE RESPONSE Year 2000 (PRY2K). PRY2K was a series of four command post exercises scheduled from February to September 1999 and was the first national level exercise conducted under conditions of multiple Y2K mission critical system failures. The PRY2K assessed the ability of DoD to respond with timely decisions in a Y2K degraded environment and focused on the strategic national tasks of mobilization, deployment, employment, intelligence-surveillance-reconnaissance (ISR), and sustainment.

This series of exercises was 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 was 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 assessed the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K. Finally, senior members of the warfighting community shared lessons learned and other vital information via secure videoteleconference (SVTC). The Secretary of Defense, CJCS, Service Chiefs, and CINCs participated in the SVTC following each exercise with a goal of recommending a strategy to the National Command Authorities to mitigate the impact of mission critical systems failure.

Table Top Exercises

In addition to the CJCS Contingency Assessments, the Department announced its plan for preparing the DoD leadership for the impact of Y2K on national security in a December 8, 1998, memorandum titled, "Participation in Department of Defense and National Level Y2K 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 Y2K failures. These activities enhance participants' understanding of potential Y2K impacts on national security; assist in the development of policy recommendations; provide continuing

11th Quarterly Report to OMB

impetus to accelerate progress on fixing Y2K systems problems; and facilitate effective contingency planning. The four-part program, depicted in Figure 3 below, included:

- A set of three functionally oriented one-day policy seminars held in November and December 1998 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 1999. 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 Y2K Coordinator, and congressional staffers.
- A DoD Defense/National Security game conducted on September 8, 1999 and completed before the national level exercise. The DoD game focused on policy and crisis management in response to a national security emergency. The DoD senior leadership fully participated, including the Deputy Secretary of Defense, the Vice-Chairman of the Joint Chiefs of Staff, the Service Under Secretaries, the DoD CIO, selected Principal Staff Assistants and the Directors of specified Defense Agencies. The State Department and FEMA also participated in the exercise.
- This activity led up to a National-level Y2K Table Top Exercise on September 18, 1999. This was a White House Y2K office inter-agency exercise, supported jointly by DoD and FEMA.

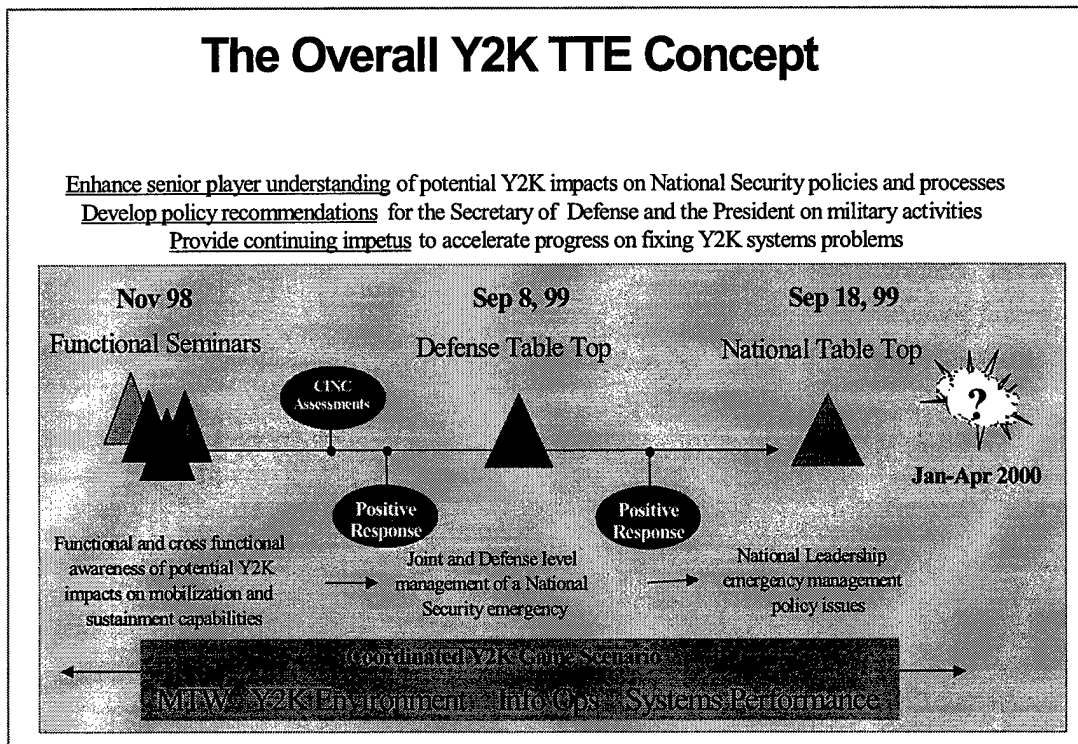


Figure 3 - Overall Year 2000 Table Top Exercise (TTE) Concept

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 Y2K 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 4 below.

DoD Operational Readiness and Consequence Management Priorities

- **Priority 1:** Units engaged in:
 - Direct Support to National Command Authorities
 - 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

Figure 4 - 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 Authorities, 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 Y2K-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 Y2K 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 Y2K date related events.

Conclusion

The DoD approach to BCCP is to provide centralized policy guidance with DoD components developing appropriate plans based on that guidance and executing them appropriately. While some planning assumptions have changed for individual plans, the overall BCCP guidance remains valid and accurate as published earlier. With respect to Day One planning and activities, DoD is well tested and positioned in terms of preparation, monitoring and response activities as outlined in GAO publication, "Y2K Computing Challenge: Day One Planning and Operations Guide" (October 1999).

- The DoD components have gone to commendable lengths to prepare both their systems and their personnel for the transition. Y2K Leave/Travel policies have been promulgated and informational messages regarding personal preparation have been broadcast in a variety of mediums.
- A system configuration management policy for Y2K to minimize changes has been promulgated, with documented procedures for obtaining necessary waivers.
- Infrastructure risk assessments have been performed by Defense Logistics Agency and by the commands responsible for coordinating and providing utilities and critical infrastructure services to DoD facilities.
- Organizational Y2K "command posts," existing operations centers, and facility special action teams have been designated. Operational forces will use their proven mechanisms for reporting and responding to changes in capability or readiness. The readiness of DoD business functions will be monitored by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Y2K Decision Support Activity (DSA). The business units of the DoD (e.g. Defense Logistics Agency, Defense Finance and Accounting Service) will report status and outages of mission critical systems to the DSA if and when they occur. Each Defense Agency and the major organizations of the services have established help desks and action teams to quickly respond to any system-related problems, while Continuity of Operations Plans ensure that core DoD missions will continue at acceptable levels.
- Y2K "Posture Levels" have been established by the Joint Staff and implemented by the Services, Commanders in Chief of the Combatant Commands, and key Defense Agencies. These posture levels provide planning and action assumptions for DoD components and a means to synchronize actions in anticipation of or response to any disruptions occurring during the date transition.

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.

11th Quarterly Report to OMB

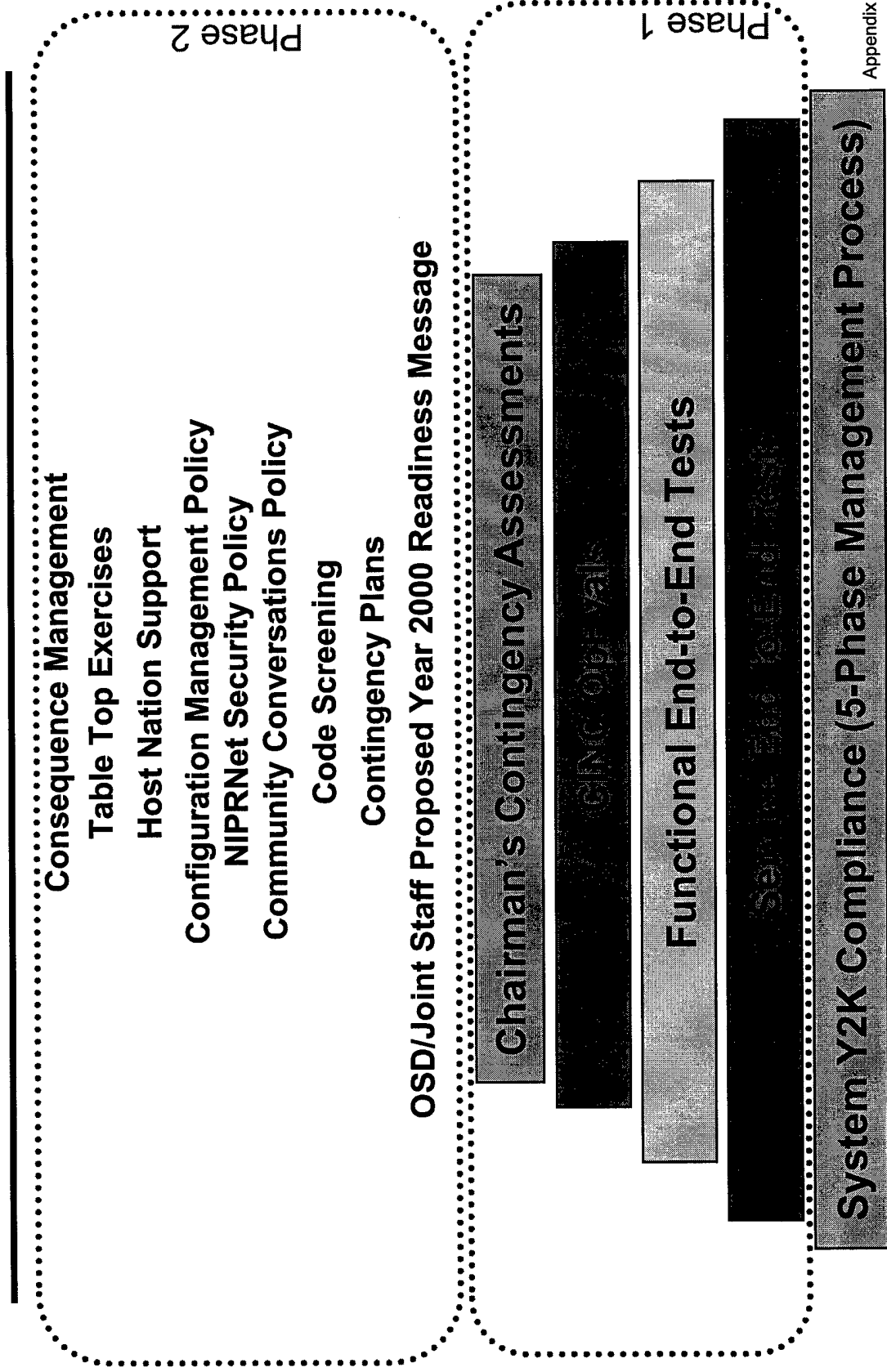
The Y2K problem is one of enormous scope and complexity for the Department of Defense, which has over one-third of the Federal Government's mission critical systems. Despite this challenge, the high percentage of systems compliance already achieved, combined with the results of end-to-end and operational 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 Y2K-related problems.

TOTAL DOLLARS to Repair Year 2000 Impact on Information Technology. Totals should include Non-DIST, DIST, MC, and Embedded - Total Y2K Costs							
Agency Acronym	Effective Date:						(in Millions)
	FY 1996	FY 1997	FY 1998	FY 1999	FY 2000	FY 2001	Total
ARMY		\$83.20	\$166.40	\$338.69	\$17.71		\$606.00
DON	\$11.52	\$46.46	\$205.67	\$637.11	\$5.16		\$905.92
USAF		\$161.00	\$598.00	\$350.00	\$5.00		\$1114.00
JS		\$0.06	\$0.93	\$11.60			\$12.59
SOCOM		\$0.78	\$12.03	\$14.70			\$27.51
USI	\$0.30	\$13.52	\$139.81	\$156.00	\$20.00		\$329.63
DIA	\$0.20	\$1.00	\$12.06	\$22.01	\$6.91		\$42.18
USD(A&T)				\$10.80			\$10.80
BMDO				\$8.11	\$2.05		\$10.16
DARPA	\$0.05	\$0.02	\$0.01	\$0.00			\$0.08
DLA	\$1.77	\$10.42	\$11.54	\$43.99	\$0.97		\$68.69
DTRA		\$0.18	\$1.63	\$6.80	\$1.50		\$10.11
DFAS	\$8.43	\$14.40	\$23.86	\$35.55	\$6.28		\$88.52
DCAA							\$0.00
USD(P&R)				\$3.00			\$3.00
DeCA				\$30.80	\$5.65		\$36.45
OASD/HA	\$0.04	\$1.43	\$26.98	\$88.78	\$6.71		\$123.94
DSCA		\$0.32	\$0.30				\$0.62
DSS				\$0.05			\$0.05
DISA	\$0.69	\$55.25	\$0.12	\$26.10			\$82.16
AFIS				\$0.36			\$0.36
WHS			\$0.10	\$0.20			\$0.30
DODIG				\$0.20			\$0.20
Total	\$22.99	\$388.04	\$1199.44	\$1784.85	\$77.94	\$0.00	\$3473.26
Additional activities reporting Y2K funding only							
ASD (C3I)				\$103.40	\$4.90		\$108.30
DOT&E				\$12.90			\$12.90
Natl Lab				\$2.00			\$2.00
Total				\$118.30	\$4.90		\$123.20
Grand Total	\$22.99	\$388.04	\$1199.44	\$1903.15	\$82.84		\$3596.46

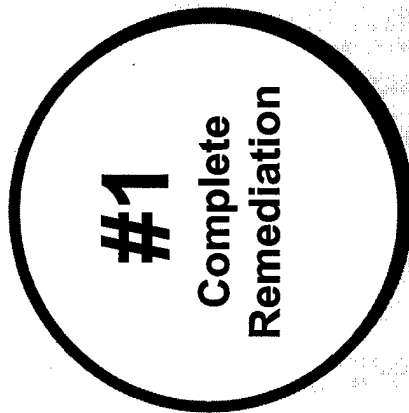
Summary of DoD Y2K Program and November 1999 Status

OASD (C3I) Y2K Office

DoD Year 2000 Risk Reduction



Major Objectives of 1999



DoD MC System Implementation

DoD MC System Plan

DoD MC System Completion Chart

Y2K Operations

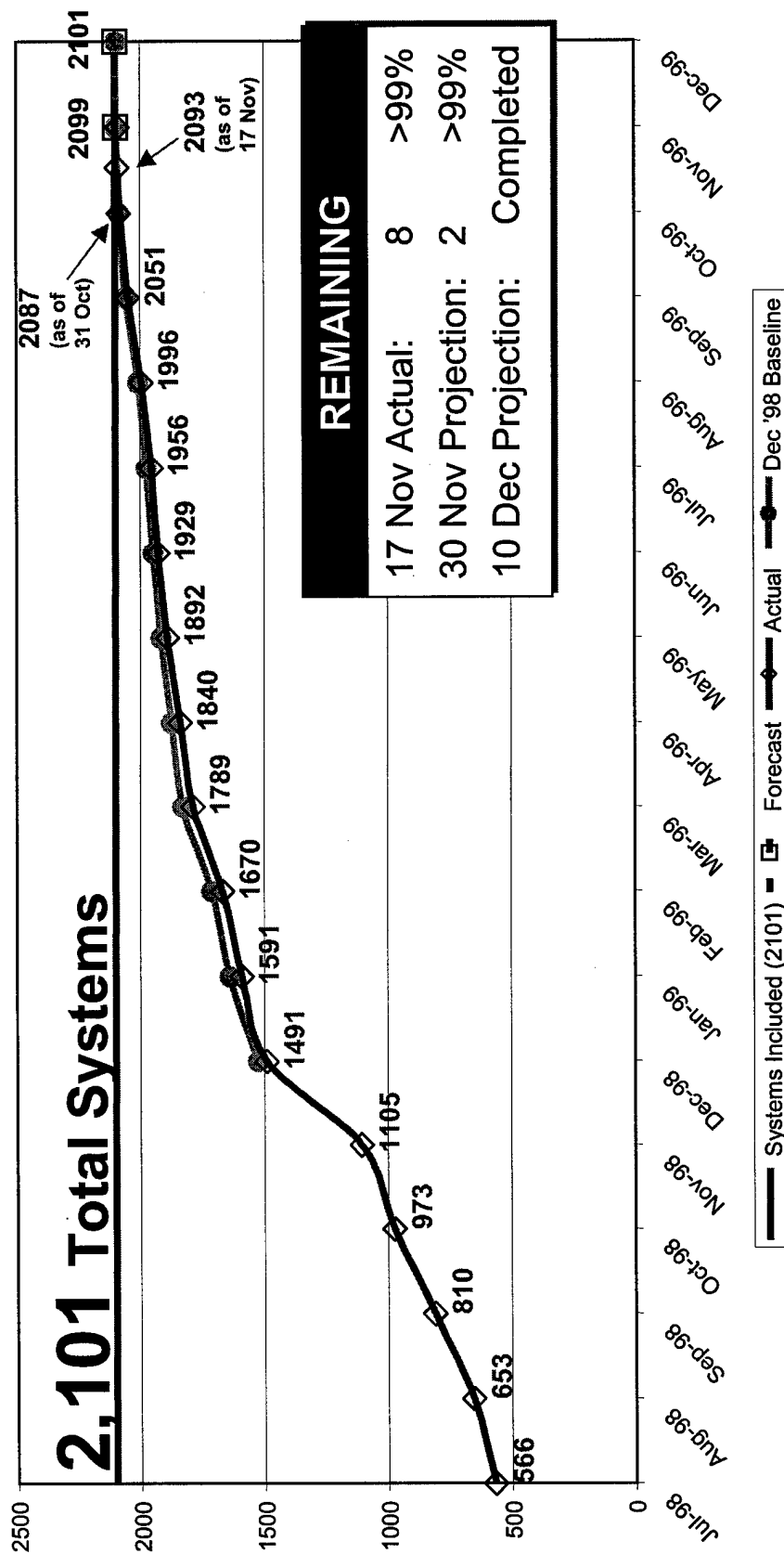
Operational Testing

Contingency Planning



Consequence Support Planning

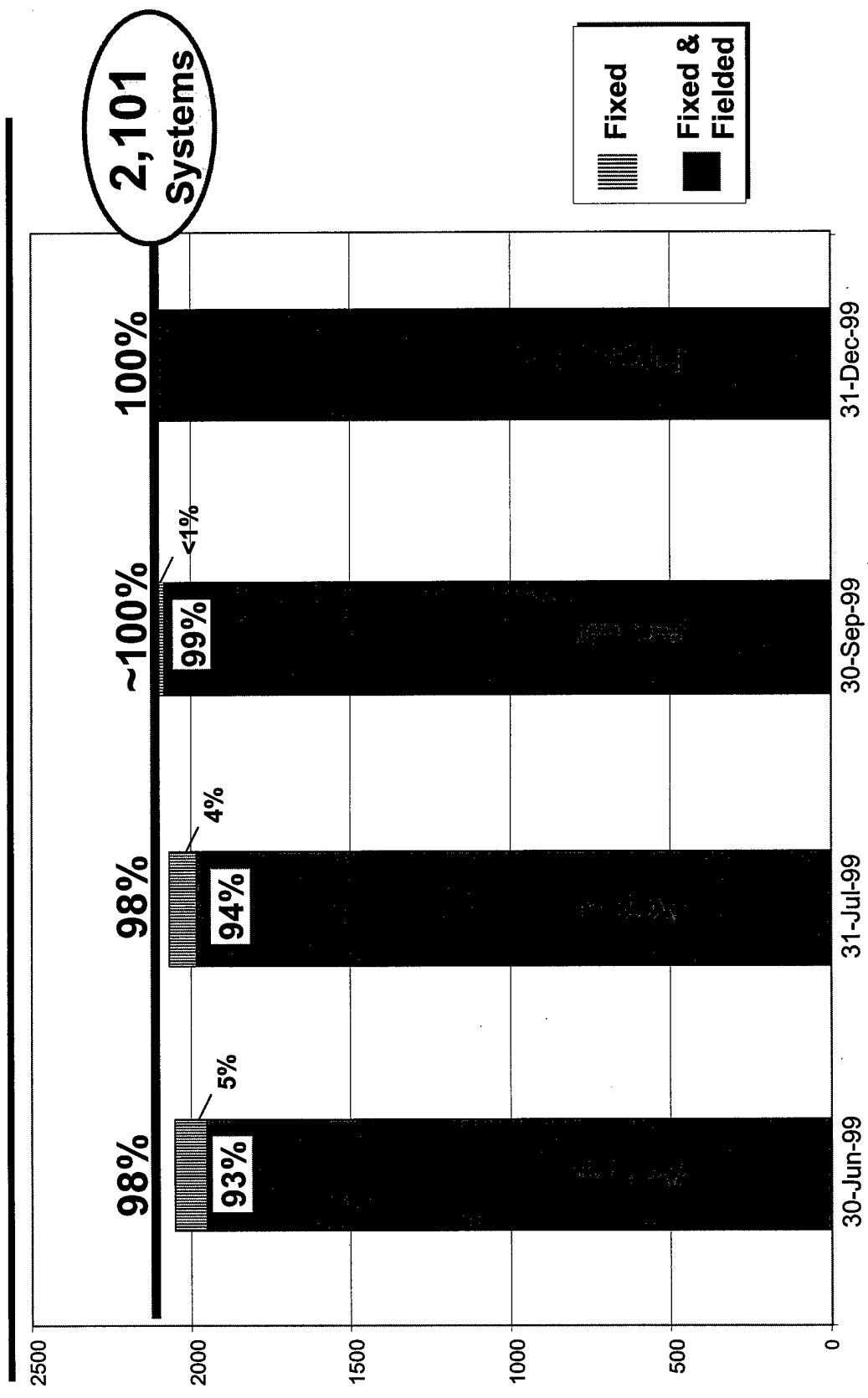
DoD Mission Critical System Completion Chart



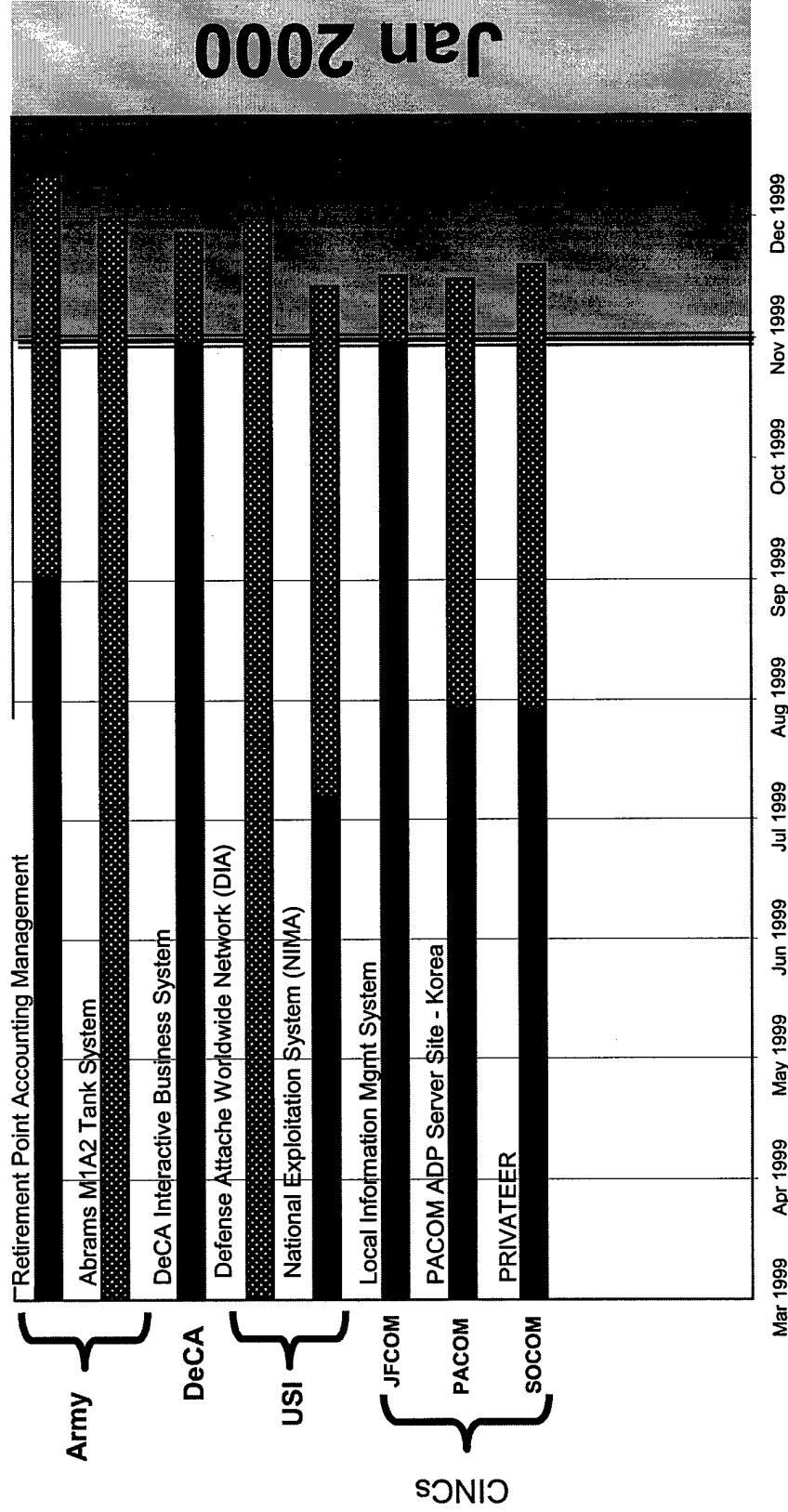
Data as of: 11/17/1999
Generated on: 11/17/1999
Excluding Dev(1), Dev(2), Terminated/Retired and Replacement

DoD 11th Quarterly Report to OMB

Mission Critical System Plan 1999



DoD Mission Critical System Implementation

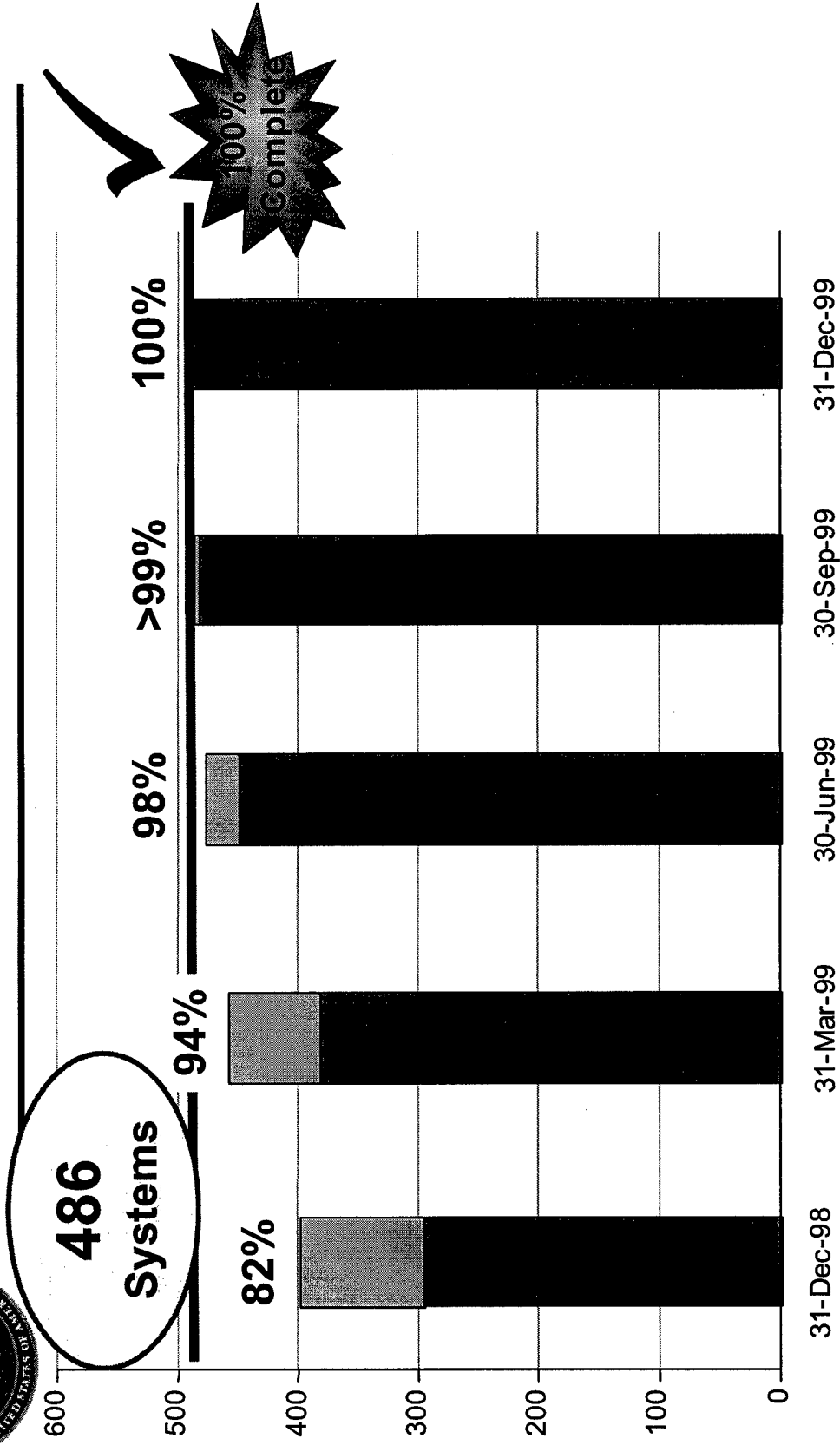


Data as of: 11/17/1999
 Generated on: 11/17/1999
 Excluding Dev(1), Dev(2), Terminated/Retired and Replacement

DoD 11th Quarterly Report to OMB



Nuclear Systems Completion



as of 10 November 1999

FOR OFFICIAL
USE ONLY

Fixed
Fixed & Fielded

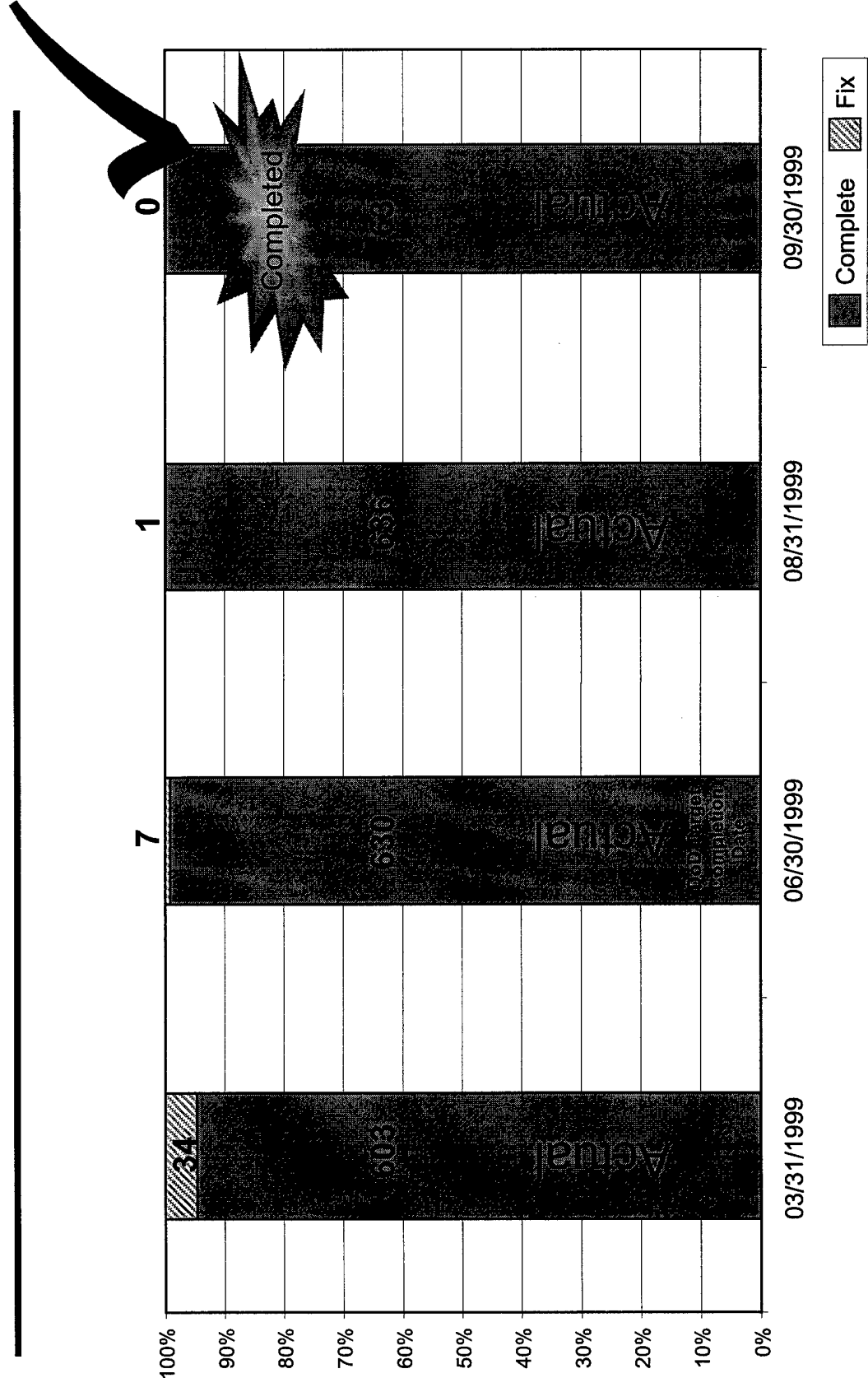
Federal High Impact Programs

100% Complete

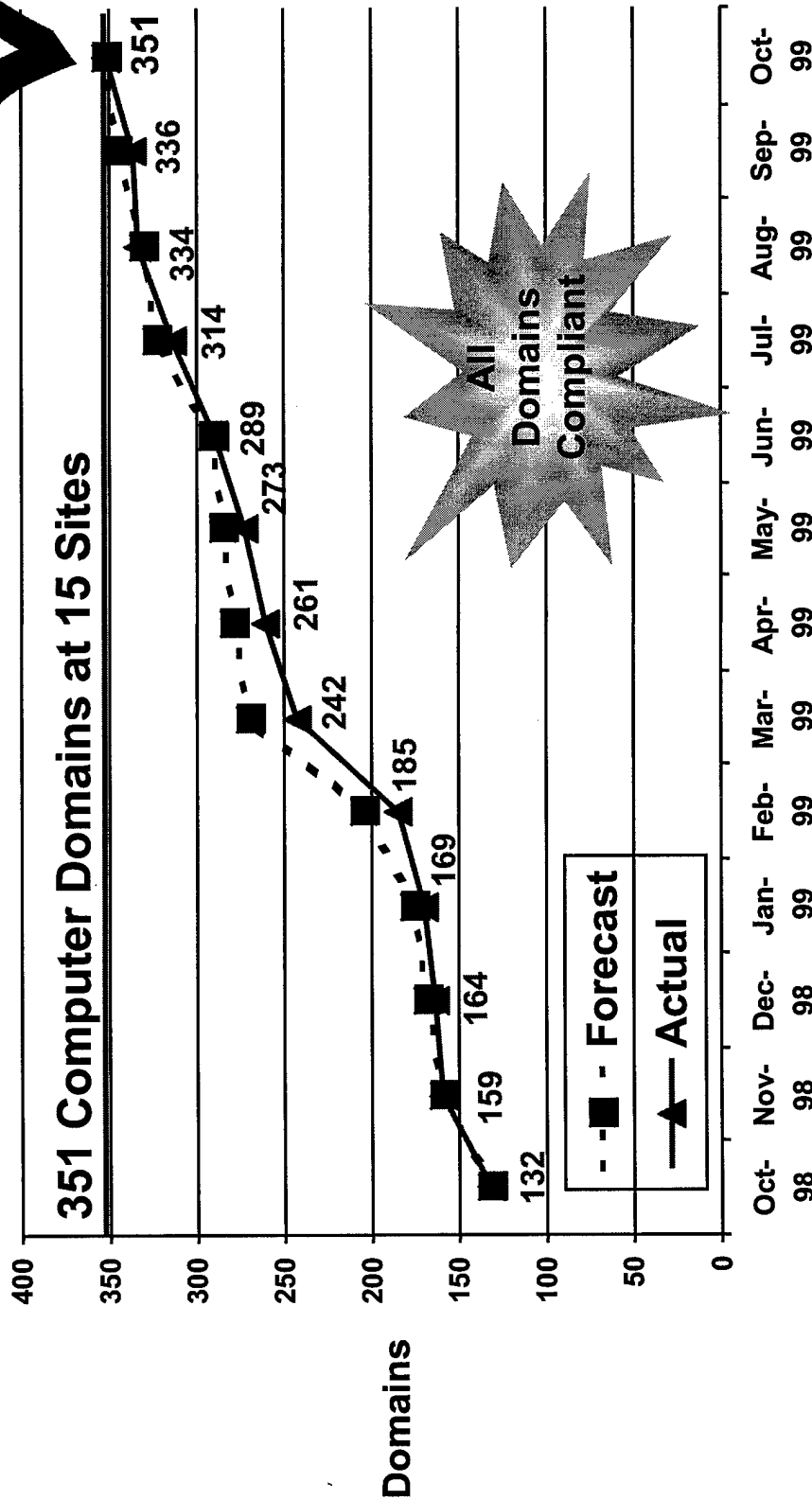
CRITERIA	MILITARY HOSPITALS	RETIREE - ANNUITANT PAY
System Compliance	✓ 100% complete	✓ 100% complete
End-to-End Testing	✓ 100% complete	✓ 100% complete
Contingency Planning	✓ 100% complete ✓ All contingency plans tested	✓ 100% complete ✓ All contingency plans tested
Data Exchanges	✓ 100% complete	✓ 100% complete
Informing the Public	✓ 100% on track ✓ Recent Press Release (30 Sept)	✓ 100% on track ✓ Mail out to all retirees and annuitants ✓ Recent Press release (14 Oct)

Installations Completion Progress

(637 Installations)

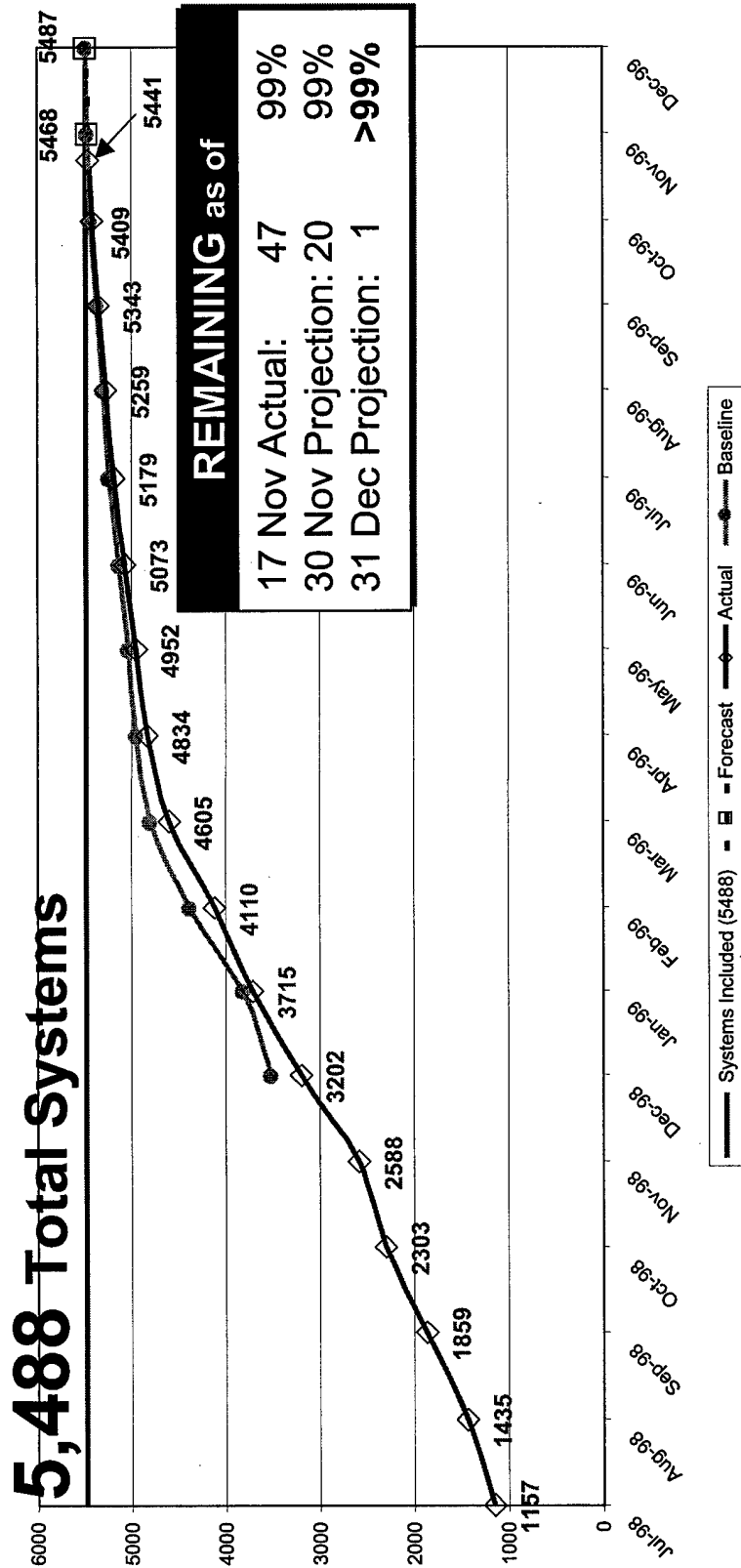


Defense Megacenters Computer Domain Completion Chart



Schedule

DOD Non Mission Critical System Completion Chart



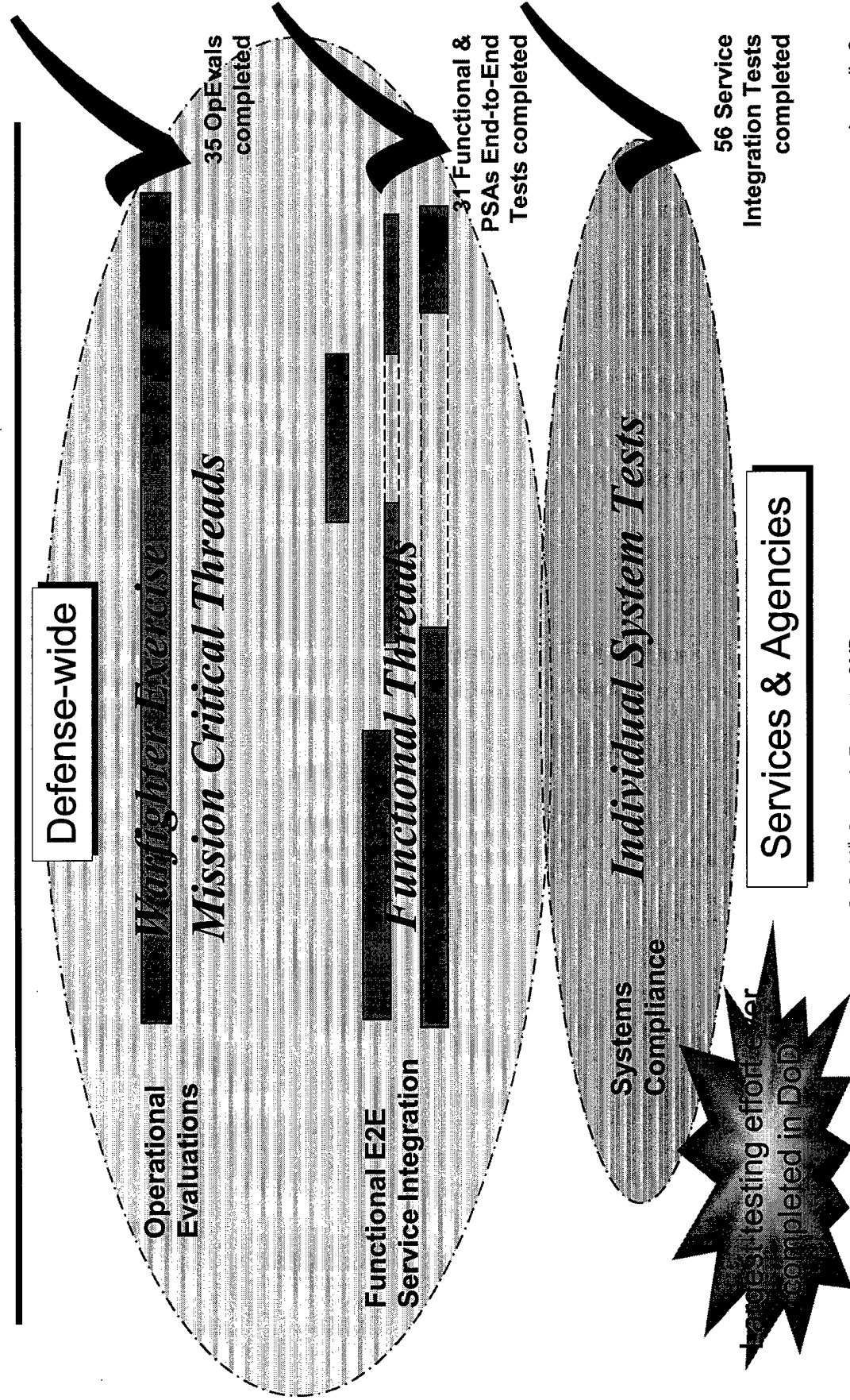
Embedded Systems

Agency	Devices Controlled by Information Technology and/or by Microchip									
	PCs & Servers			Comm Hardware/Software			Facilities & Other			
Acronym	Compliant	Unknown	Non-Comp	Compliant	Unknown	Non-Comp	Compliant	Unknown	Non-Comp	
ARMY	460,988		12,121	58,360		226	66,128		2,325	
DON	636,975	0	26,095	70,043	0	5,960	254,052	0	1,588	
USAF	304,472	0	16,783	138,146	0	4,605	1,374,088	0	27,324	
JS										
SOCOM										
USI	17,025	0	261	248	0	11	2,203	23	80	
DIA										
USD(A&T)										
BMDO	1,632	0	0	22	0	13	6	0	0	
DARPA	515			257			221			
DLA	117,515	0	0	14,359	0	0	18,540	0	0	
DTRA	2,707	0	0	483	0	0	17	0	0	
DFAS	30,234	0	226	542	0	146	12,268	0	1	
DCAA	4,652			383						
USD(P&R)										
DeCA	5,522		0	427		0	10,271	0	0	
OASD/HA	99,457	0	4,800	16,954	0	0	352,419	0	1,128	
DSCA	518			77						
DSS										
DISA	23,282			3,125						
AFIS										
WHS	15,237	0	0	1,749	0	0	0			
DODIG	1,726		0	4		0				
Total	1,722,457	0	60,286	305,179	0	10,961	2,090,213	23	32,446	

Cost Estimates

TOTAL DOLLARS to Repair Year 2000 Impact on Information Technology. Totals should include Non-DIST, DIST, MC, and Embedded - Total Y2K Costs									
Agency	Effective Date:						(in Millions)		
	FY 1996	FY 1997	FY 1998	FY 1999	FY 2000	FY 2001	Total		
ARMY		\$83.20	\$166.40	\$338.69	\$17.71		\$606.00		
DON	\$11.52	\$46.46	\$205.67	\$637.11	\$5.16		\$905.92		
USAF		\$161.00	\$598.00	\$350.00	\$5.00		\$1114.00		
JS		\$0.06	\$0.93	\$11.60			\$12.59		
SOCOM		\$0.78	\$12.03	\$14.70			\$27.51		
USI	\$0.30	\$13.52	\$139.81	\$156.00	\$20.00		\$329.63		
DIA	\$0.20	\$1.00	\$12.06	\$22.01	\$6.91		\$42.18		
USD(A&T)				\$10.80			\$10.80		
BMDO				\$8.11	\$2.05		\$10.16		
DARPA	\$0.05	\$0.02	\$0.01	\$0.00			\$0.08		
DLA	\$1.77	\$10.42	\$11.54	\$43.99	\$0.97		\$68.69		
DTRA		\$0.18	\$1.63	\$6.80	\$1.50		\$10.11		
DFAS	\$8.43	\$14.40	\$23.86	\$35.55	\$6.28		\$88.52		
DCAA							\$0.00		
USD(P&R)				\$3.00			\$3.00		
DeCA				\$30.80	\$5.65		\$36.45		
OASD/HA	\$0.04	\$1.43	\$26.98	\$88.78	\$6.71		\$123.94		
DSCA		\$0.32	\$0.30				\$0.62		
DSS				\$0.05			\$0.05		
DISA	\$0.69	\$55.25	\$0.12	\$26.10			\$82.16		
AFIS				\$0.36			\$0.36		
WHS			\$0.10	\$0.20			\$0.30		
DODIG				\$0.20			\$0.20		
Total	\$22.99	\$388.04	\$1199.44	\$1784.85	\$77.94	\$0.00	\$3473.26		
	Additional activities reporting Y2K funding only								
ASD (C3I)				\$103.40	\$4.90		\$108.30		
DOT&E				\$12.90			\$12.90		
Natl Lab				\$2.00			\$2.00		
Total				\$118.30	\$4.90		\$123.20		
Grand Total	\$22.99	\$388.04	\$1199.44	\$1903.15	\$82.84		\$3596.46		

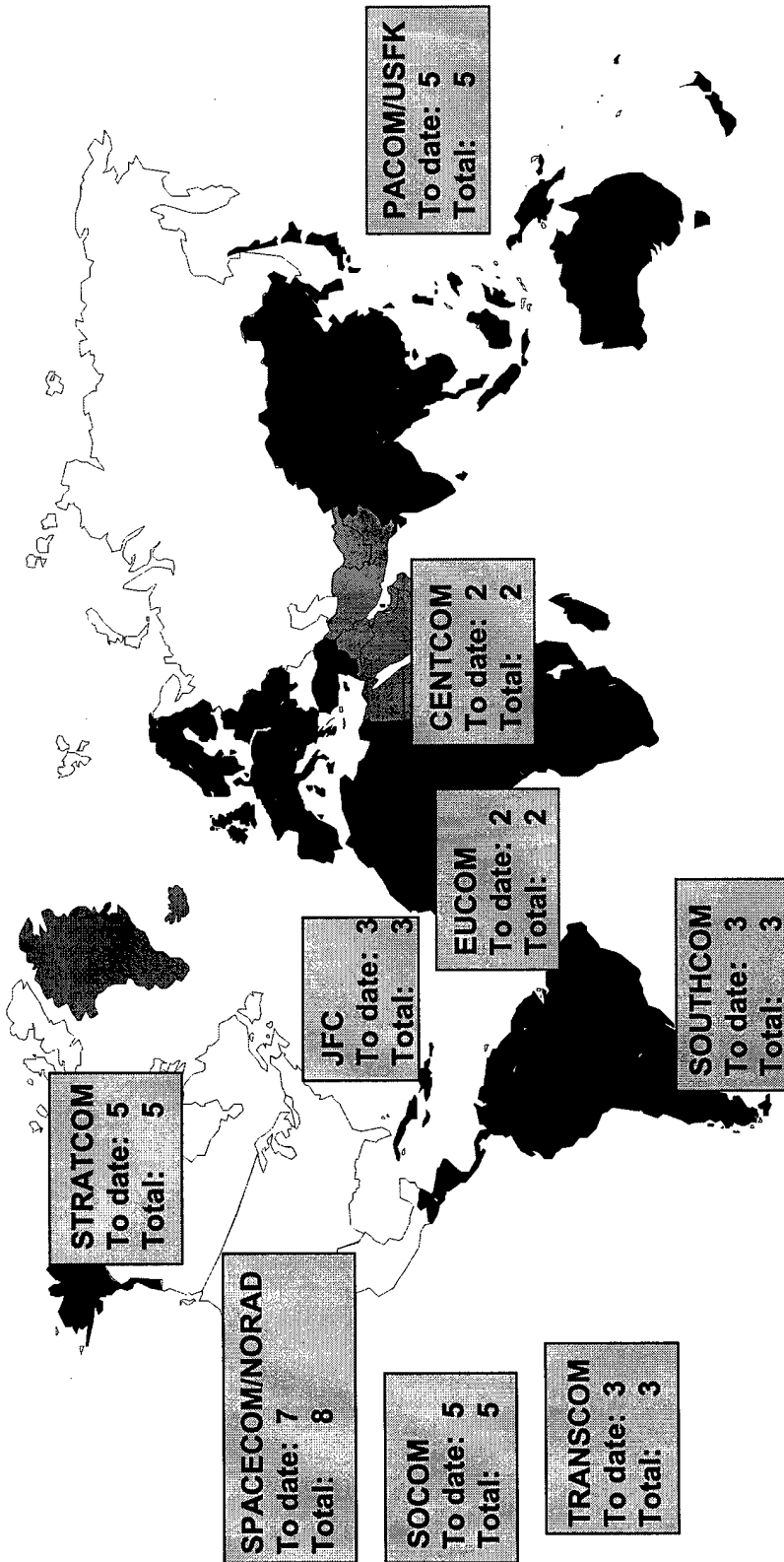
Enterprise-Wide Evaluation



CINC OpEval Requirements

☒ At least 25 OpEvals

☒ At least 2 OpEvals conducted by each CINC

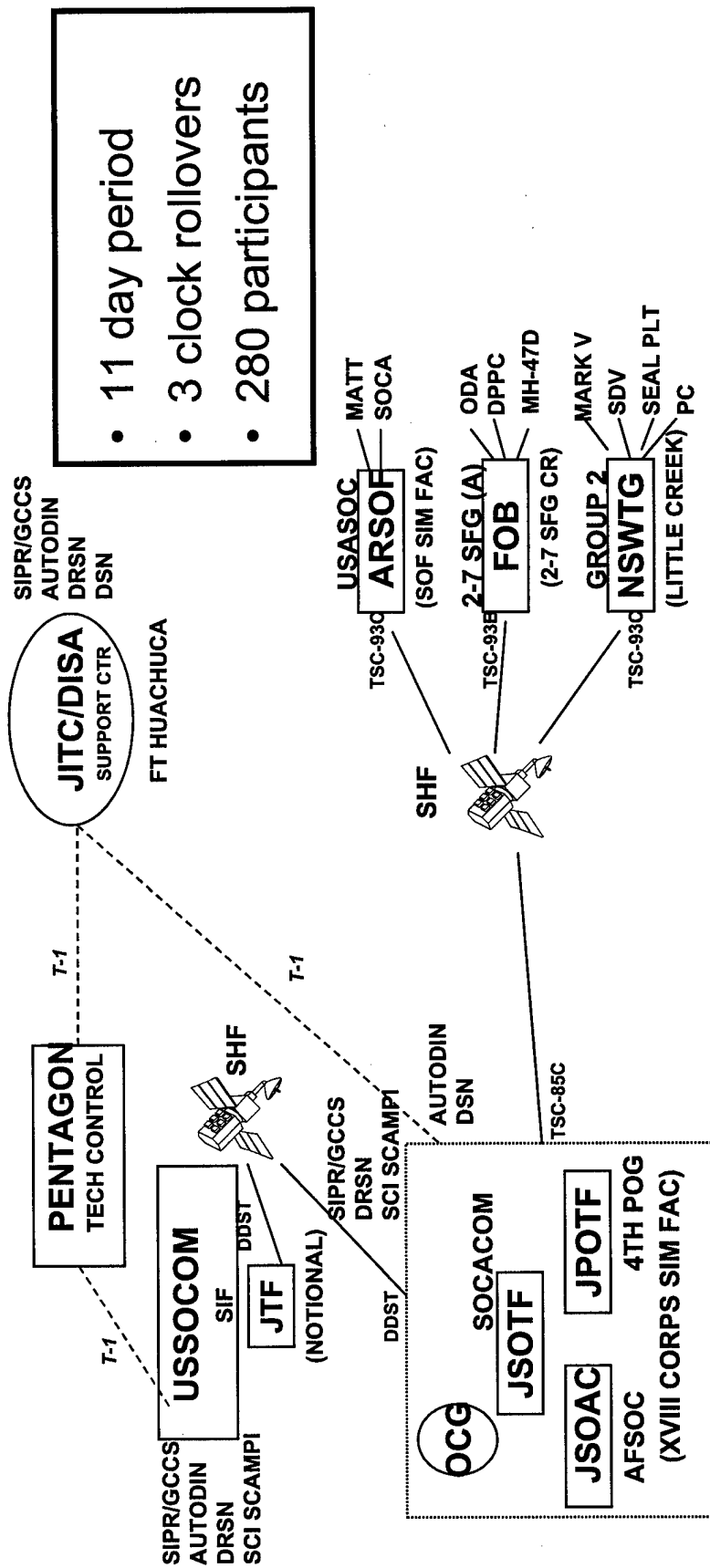


Required	To Date	By 15 Dec	Total
25	35	36	36

SOCOM OpEval 5

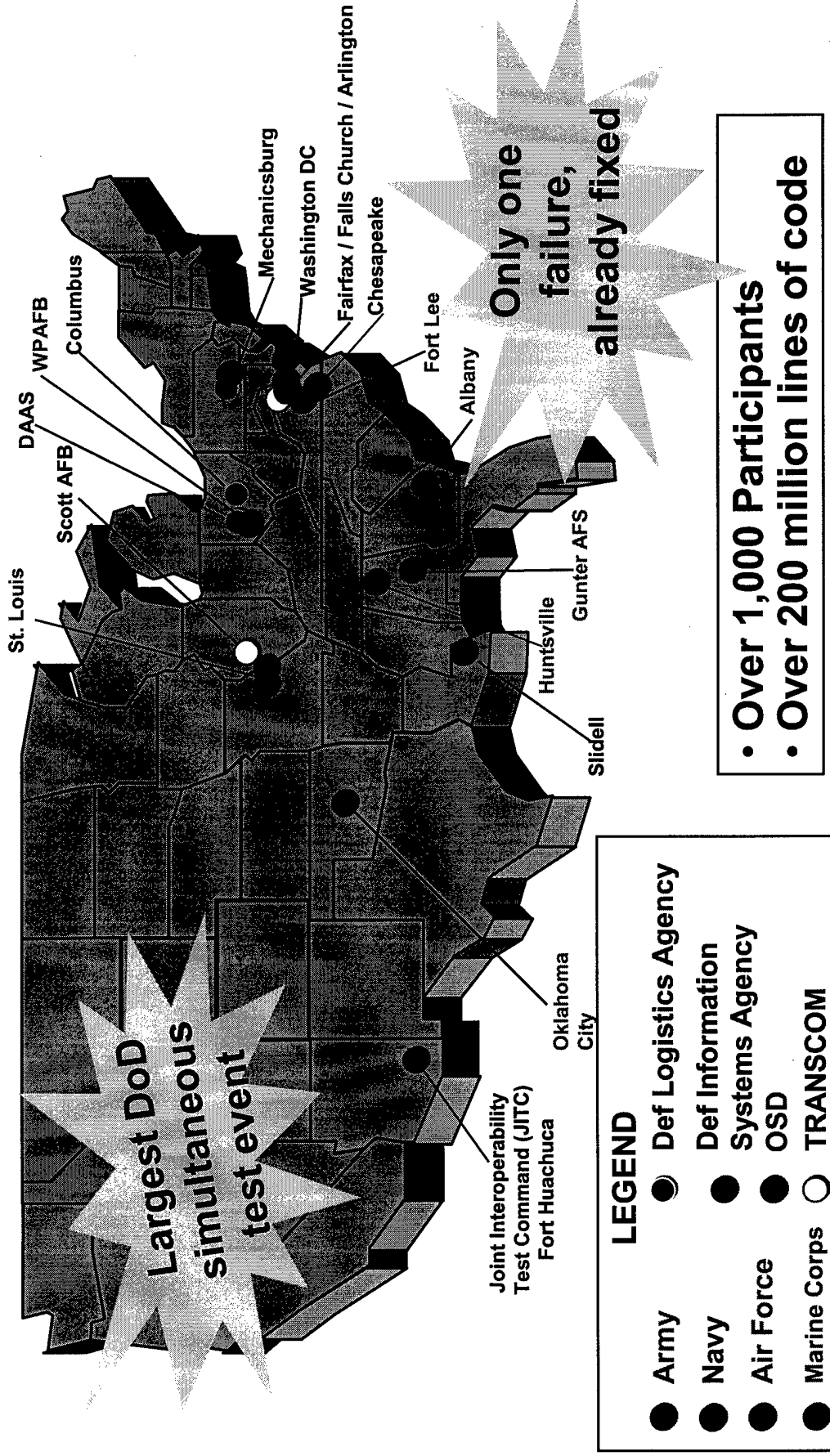
Operational Architecture

Scope, Magnitude, Complexity



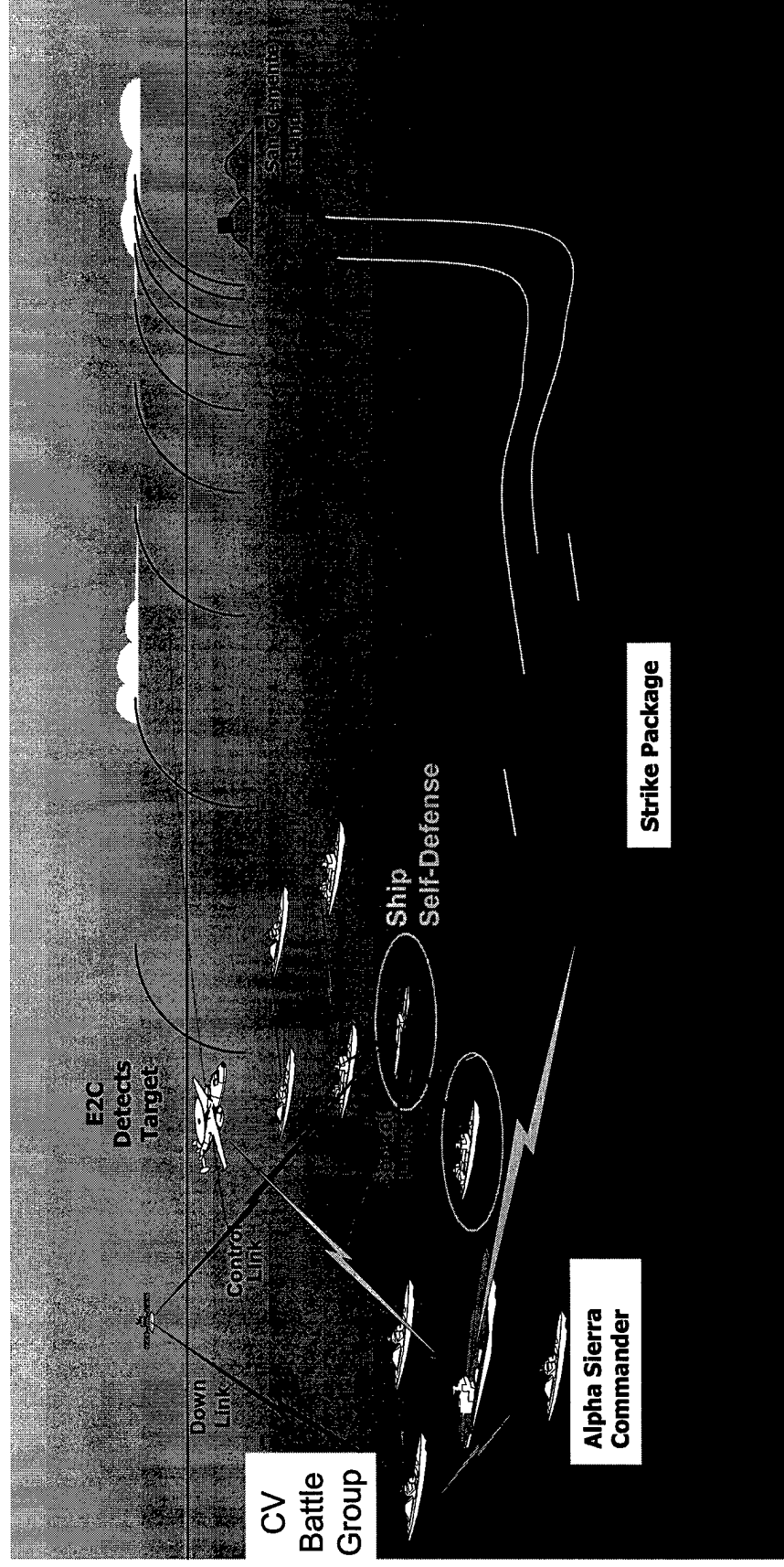
Logistics End to End (E2E) Test Sites and Participants

Scope, Magnitude, Complexity

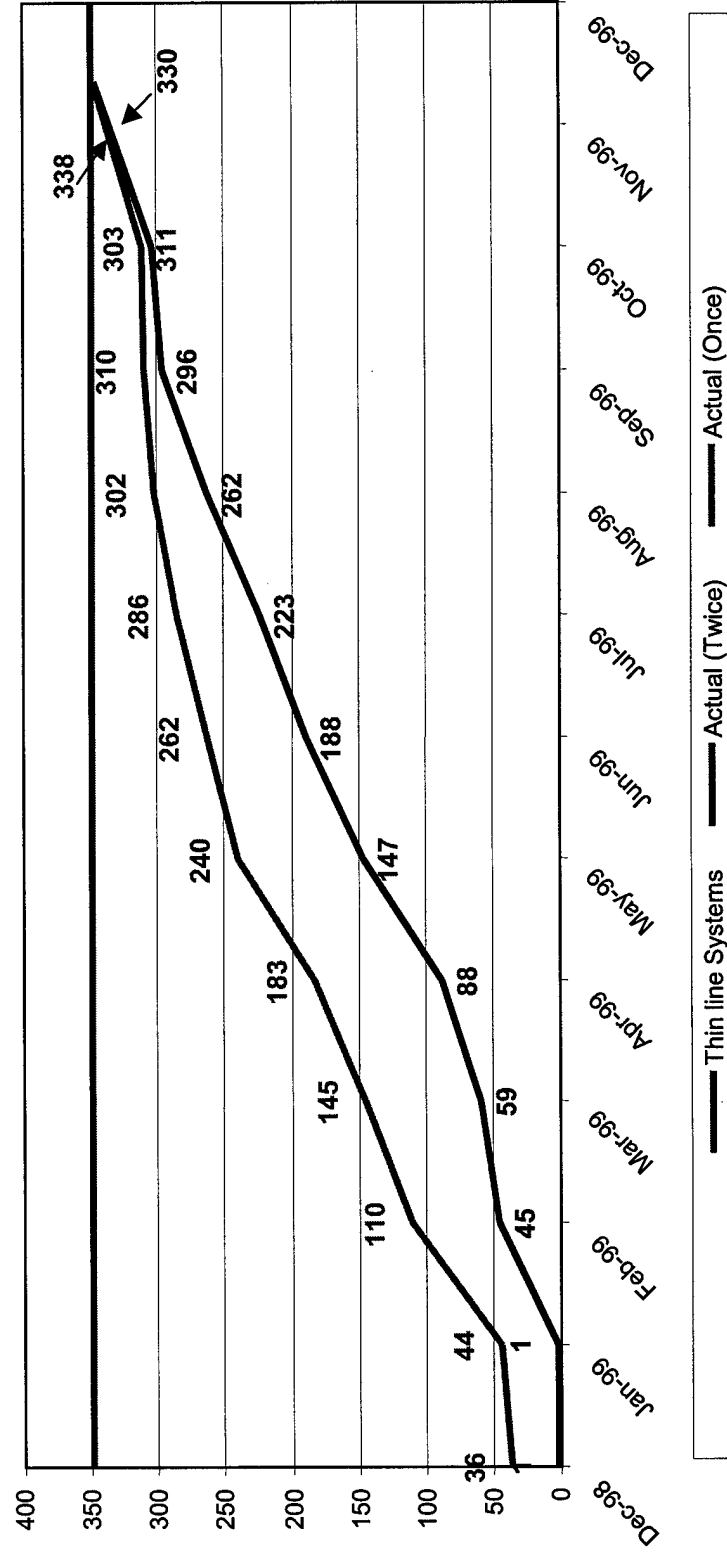


Navy Battle Group System Integration Test (BGSIT)

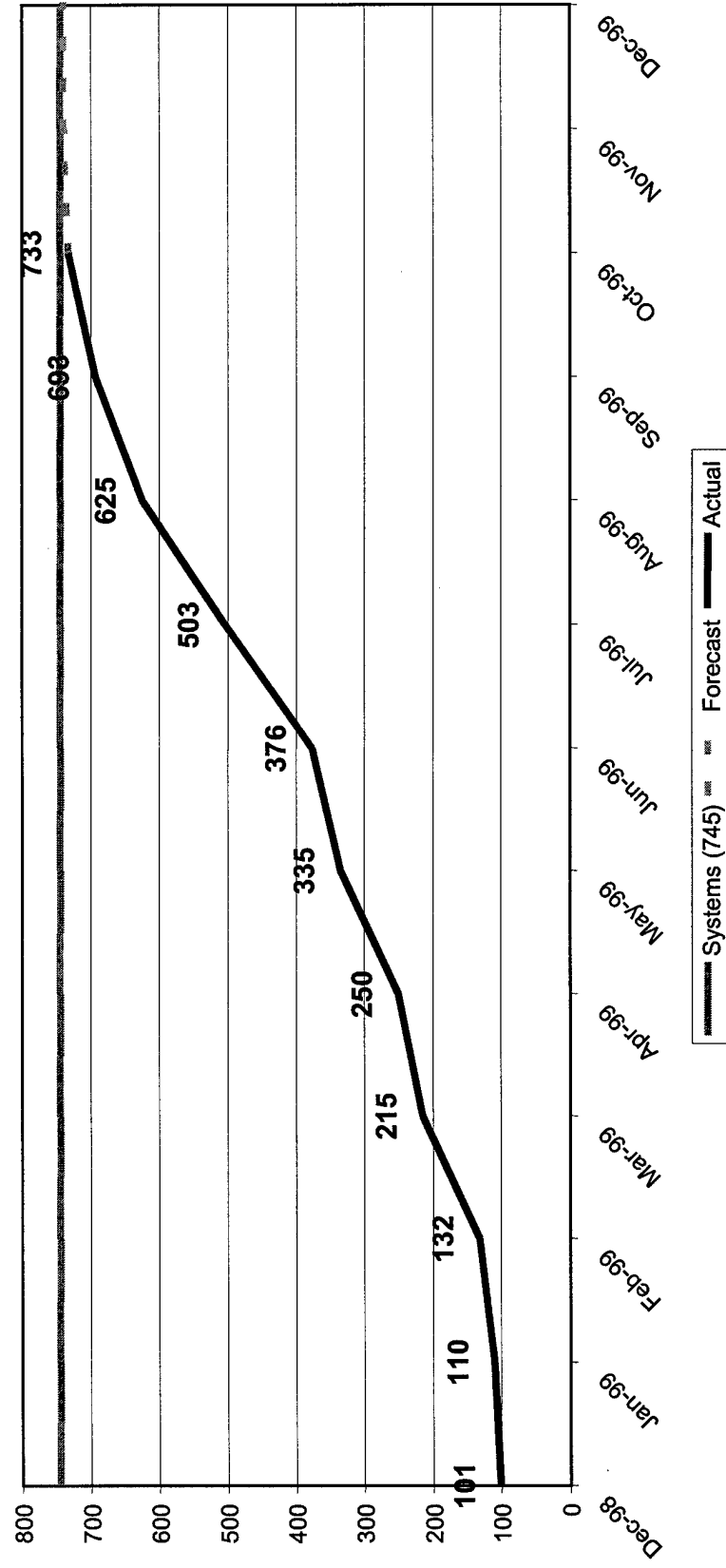
Scope, Magnitude, Complexity



Total DoD CINC OpEval Systems Test Completion (2 Tests)

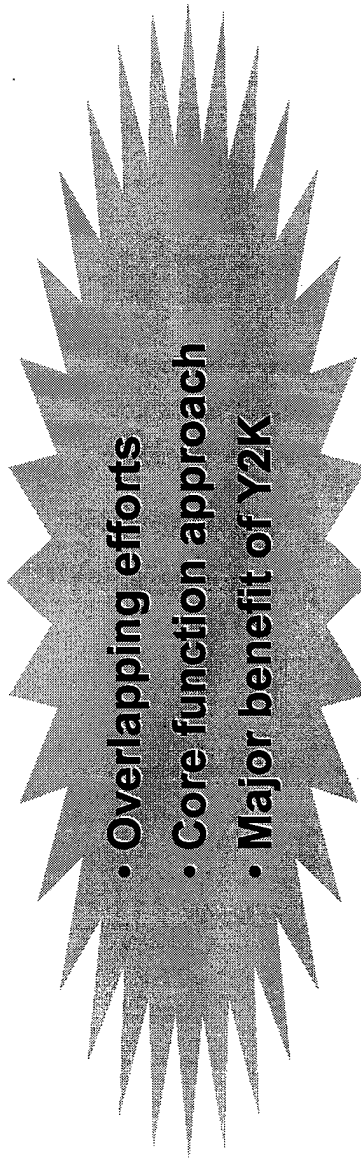


Total DoD CINC OpEval Systems Test Completion (1 Test)



Contingency Plans: Type & Status

- **System** (Restore Disrupted Systems)
 - Information Technology/Chief Information Officer Centric
 - Required: Date-aware Mission-critical Systems
- **Operational** (Ensure Successful Mission Execution)
 - Operator / Commander Centric
 - Identify Alternative Procedures, Workarounds, Gap-fillers
 - Required As Directed by Each DoD Component
 - Excellent models for DoD (USMC, DLA, DFAS)



- Overlapping efforts
- Core function approach
- Major benefit of Y2K

Chairman's Contingency Assessment

Exercise Execution Timeline

- Four assessments
 - Duration - 3-5 days each assessment
- Execution from February - July 1999
 - PRY2K-1 (Mobilization) 4 - 8 Feb 99
CENTCOM/Services/Selected Agencies
SVTC - 3 Mar 99
 - PRY2K-2 (Deployment) 3 - 7 May 99
PACOM/Services/Selected Agencies
SVTC - 26 May 99
 - PRY2K-3 (Employment/ISR) 14 - 18 Jun 99
EUCOM/SOCOM/Services/Selected Agencies
SVTC - 14 Jul 99
 - PRY2K-4 (Sustainment) 30 Aug - 3 Sep 99
PACOM/Services/Selected Agencies
SVTC - 29 Sep 99

Community Conversations

Video

Base, Post, Camp, Station, Visits

Telecom

- Status of Defense
- DoD Support to Civilian Authority
- Contingency Planning
- Base Commanders Assessment

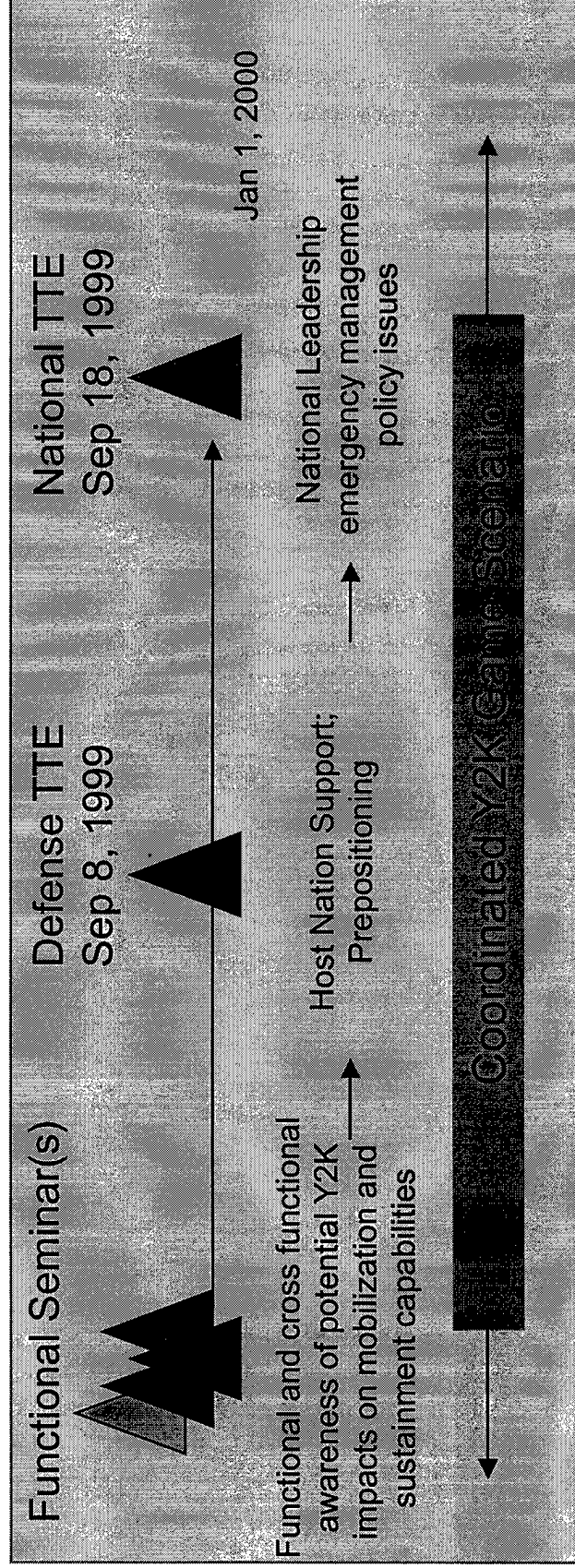
Local Community

- Power
- Water
- Banking
- Transportation
- Telecommunications
- Medical
- EMA

Shared Knowledge Managed Expectations

**When Good People Are Given Good Information,
They Make Good Decisions.**

Table Top Exercises



DoD TTEs

- Spawned similar efforts at FEMA, DoS, NATO, IC
- DoD TTE events designed to:
 - Assess the impacts of possible foreign and domestic Y2K-induced degradations
 - Define policy, resource and priority issues associated with those impacts
 - Identify options for addressing those issues
 - Examine the effectiveness of options
- DoD is prepared for Y2K

OSD Y2K Outreach

Host Nation Support

GOAL - Provide geographic and functional CINCs with information on the ability of host nations to provide continued support to overseas DoD operating locations during the Y2K transition period

- Information needed for areas outside DoD operating locations
- Information not normally available through DoD-only channels but required for continuity of operations and contingency planning
- Coordination required at several levels to gain access to information
 - Y2K International Inter-Agency Working Group (IIWG) established to coordinate U.S. Government efforts and information sharing
 - Co-chaired by DoD/State with PCY2K, DoE, DoC, DoT, NIC participation
 - DoD efforts involved OSD (C3I, A&T, DISA, DTRA, DLA), JCS, CINC Y2K Offices(EUCOM, CENTCOM, PACOM, TRANSCOM), Services, DoD/IG
 - Additional coordination with NATO, SHAPE, USFJ, USFK, US Embassies, and several international agencies and trade associations
- Information developed allows CINCs and Services to better understand what to expect during transition and determine best use of resources

OSD Y2K Outreach

US - Russian Y2K Cooperation

GOAL - Address Y2K issues of mutual national security concern and provide assistance and expertise toward managing potential problems

- OSD Outreach has coordinated the efforts in five cooperative program areas

- 1) Y2K Information Technology Management - Lead: OSD Y2K Office
 - Provide technical assistance in assessing/correcting IT systems and expertise in contingency planning and consequence management
- 2) Missile Warning - Lead: OSD Policy and JCS
 - Established a Center for Y2K Strategic Stability (CY2KSS) in Colorado
 - U.S. and Russian officers will jointly monitor and share missile warning information
 - Purpose is to reduce the risk of misunderstanding if a system failure occurs
- 3) Special Communications Links ("Hotlines") - Lead: DISA
 - U.S. and Russia have worked closely to ensure Hotlines between national political & military leaders are Y2K compliant and redundant

OSD Y2K Outreach

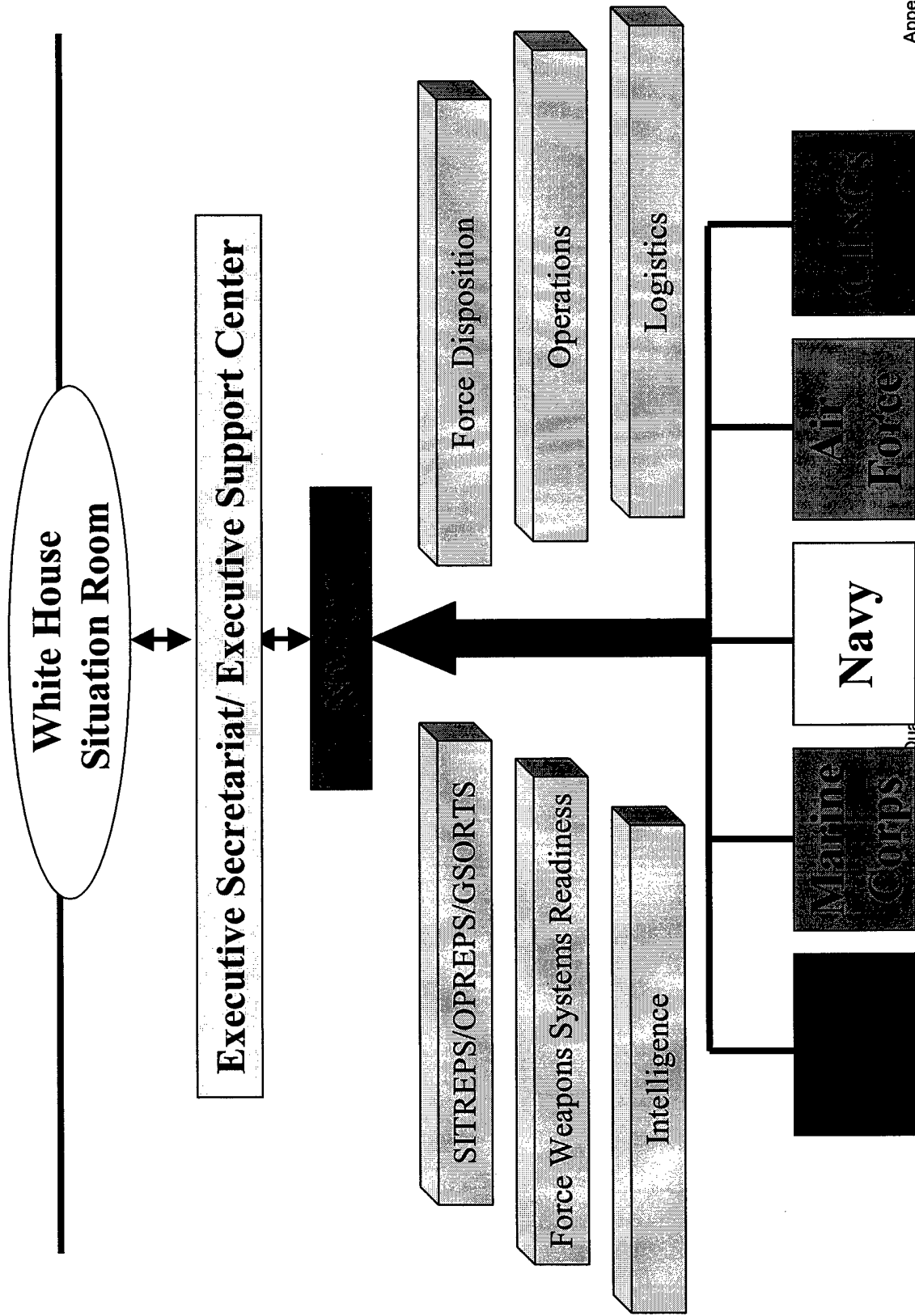
US - Russian Y2K Cooperation (Cont'd)

- 4) Nuclear Stockpile Security - Lead: DTRA
 - Intended to ensure control, security, and accountability of Russian nuclear materials, including stockpiles, weapons labs, and associated technology, during the Y2K transition
- 5) Nuclear Command & Control - Lead: USSTRATCOM
 - Exchange of nuclear specific Y2K management program information, general status, and management experiences

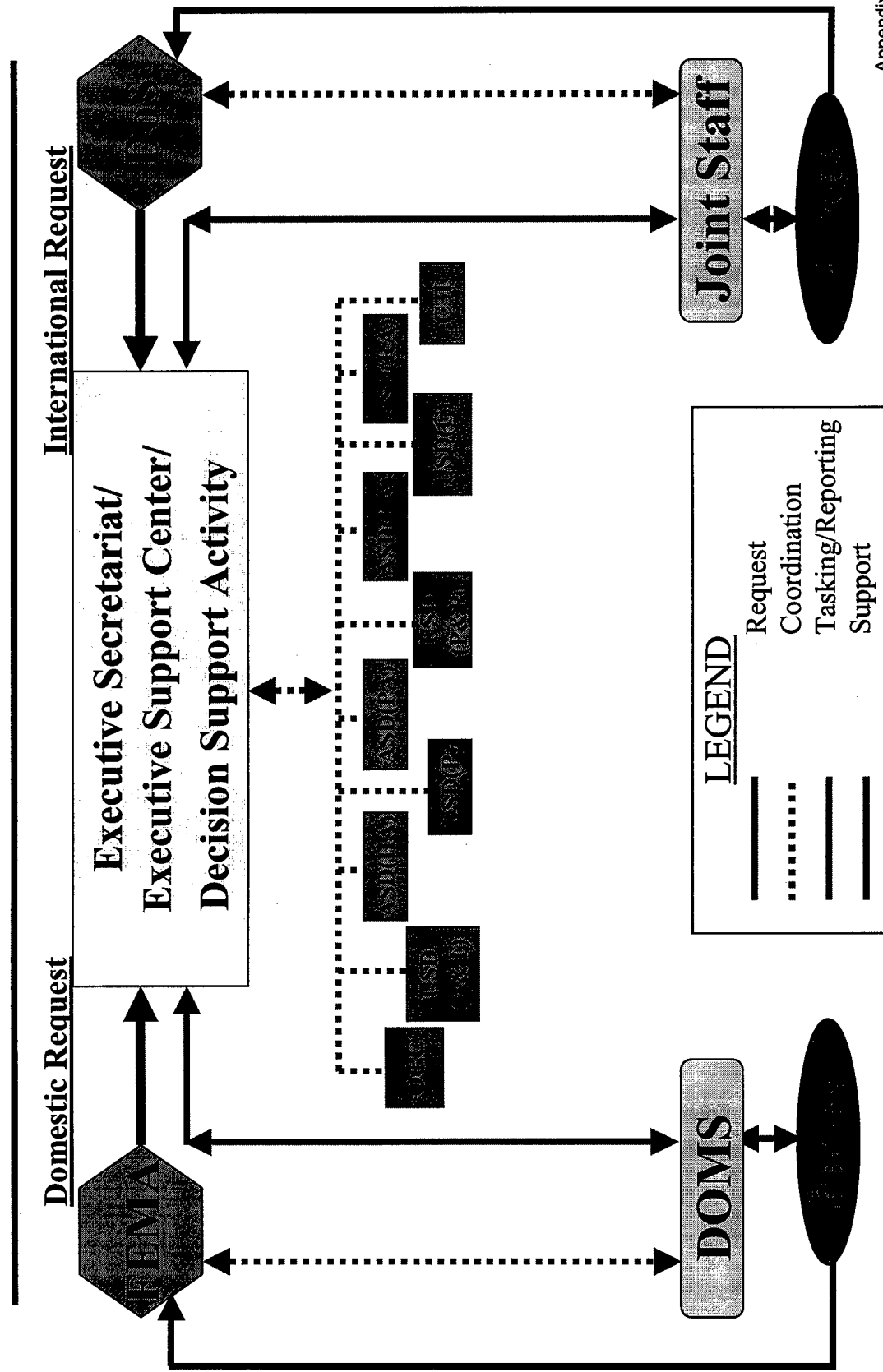
DoD Operational Readiness and Consequence Management Priorities

- **Priority 1: Units Engaged In:**
 - Direct Support to the 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 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 Nation's quality of life

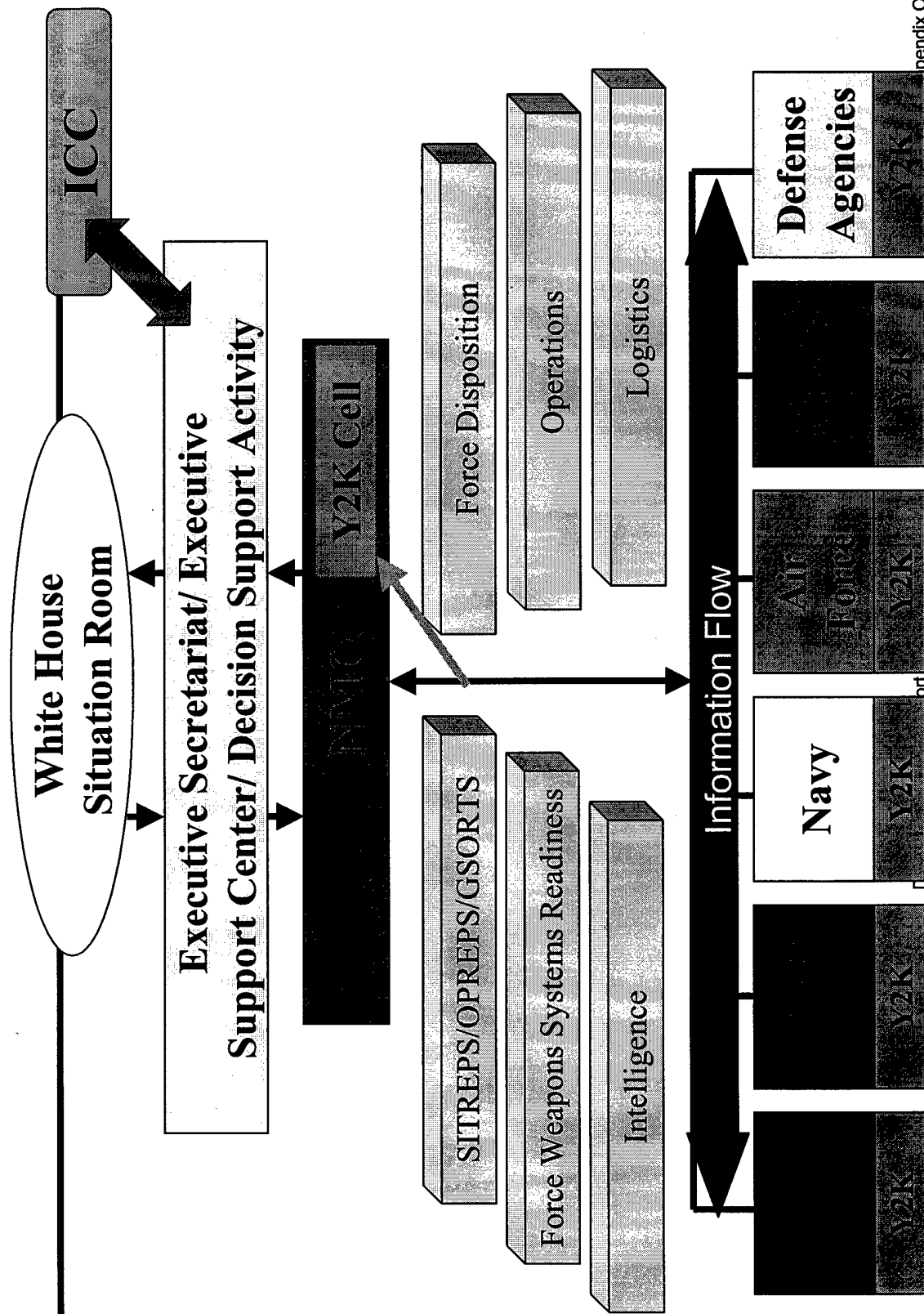
DoD Operational Reporting



DoD Consequence Management Reporting



Y2K Information Reporting



DoD Year 2000 Risk Management

Additional Initiatives

- Configuration Management Policy
- NIPRNet Security Policy
- Code Screening

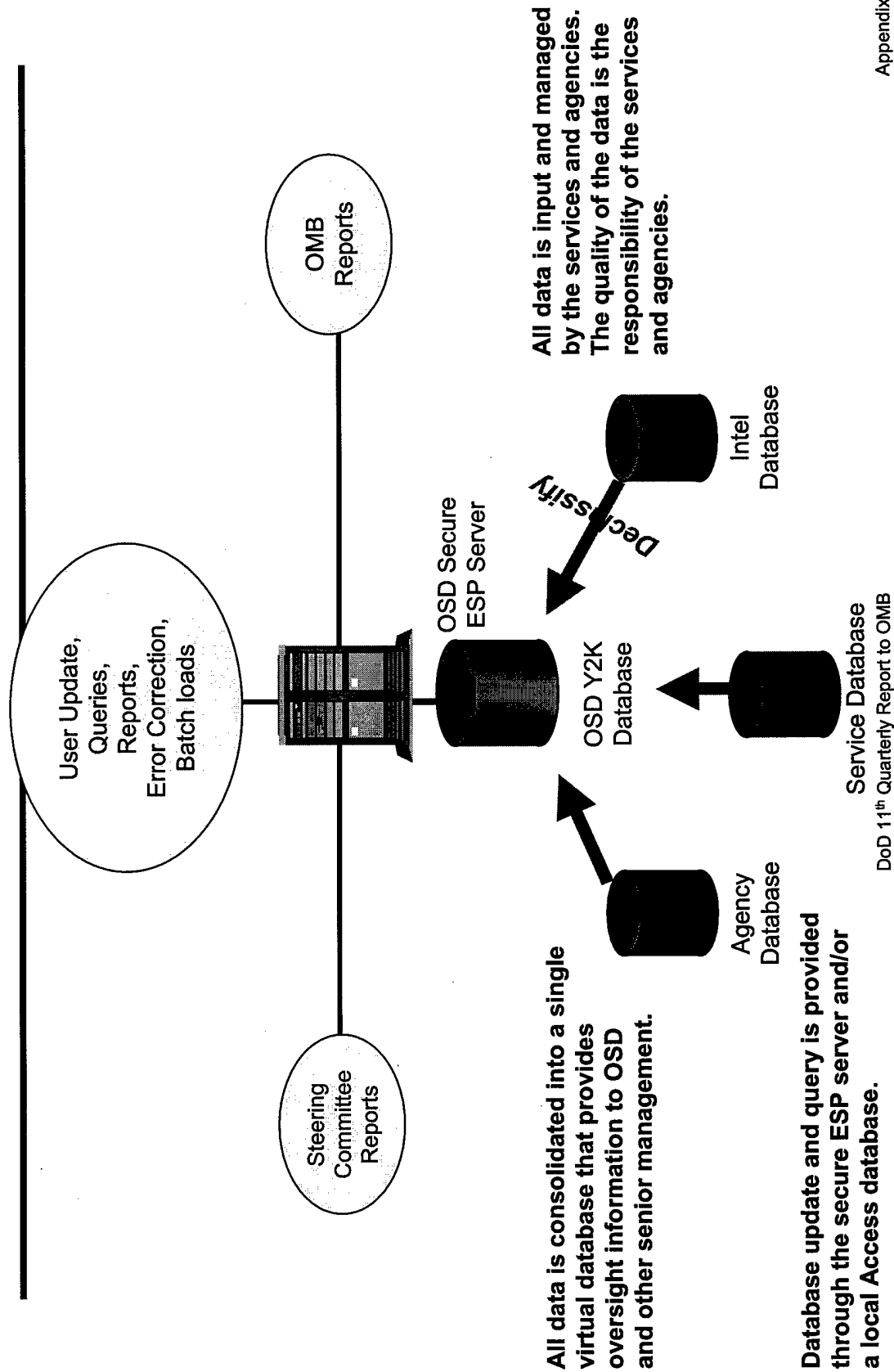
Configuration Management Policy

- Purpose:
 - Assure compliant systems remain compliant through the Y2K transition
- Signed on 20 August 1999 by DepSecDef
- Major Provisions:
 - PEOs notify CINCs/PSAs of proposed change
 - CINCs/PSAs have 10 working days to veto
 - Silence = consent
 - Applies 1 Sep 1999 to 15 Mar 2000

NIPRNet Security Policy

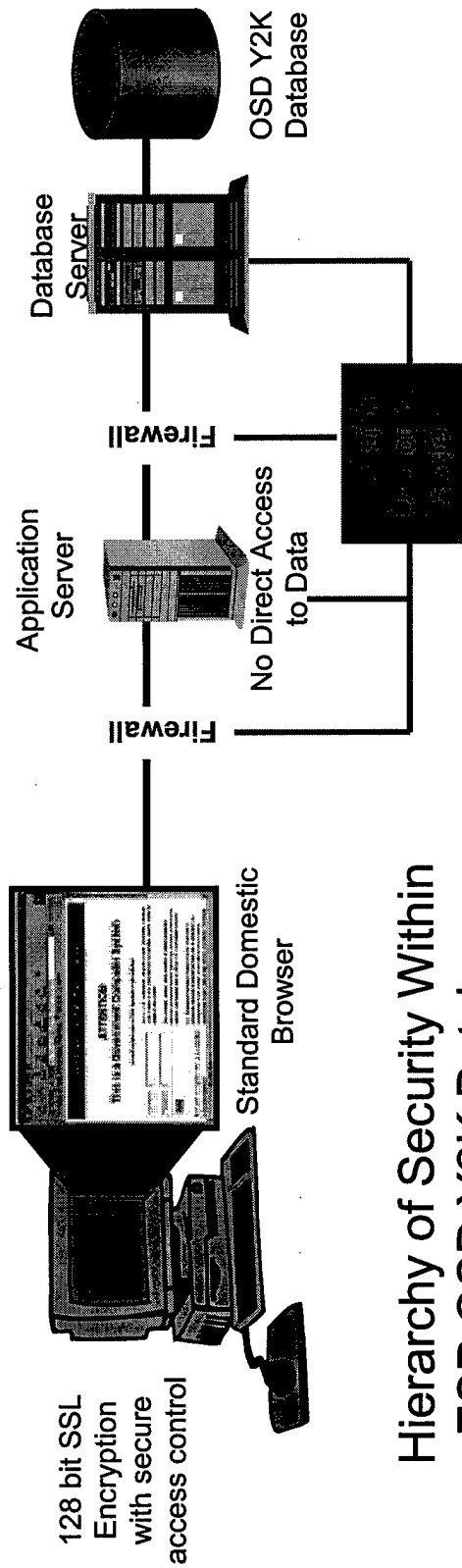
- Signed on 22 August 1999 by SCO
- Major Provisions:
 - Identifies existing Directives: DoDD 5200.28, Security Requirements for AISs, and JCS memo CM-510-99, Information Operations Condition (INFOCON)
 - Establishes the NIPRNet as the only authorized route for military access to the Internet
 - Allows for waiver for properly protected, direct Internet connections
 - Requires termination or waiver of direct Internet connections prior to December 15, 1999
 - Requires monthly reporting of noncompliant connections
 - Permits unregulated educational and morale, welfare, and recreational Internet connections so long as those networks are not also connected to the NIPRNet
 - Permits properly protected dial-in/dial-out connections
 - Recognizes the DSAWG as the organization tasked with adjudicating security issues

Current OSD Y2K Database

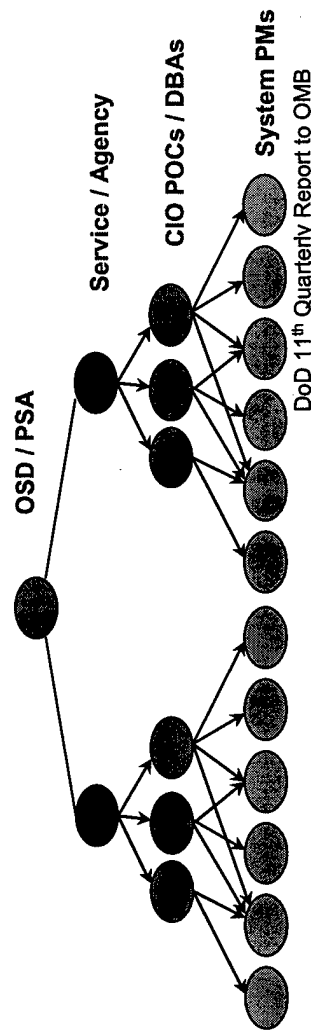


Current OSD Y2K Database Technical Architecture

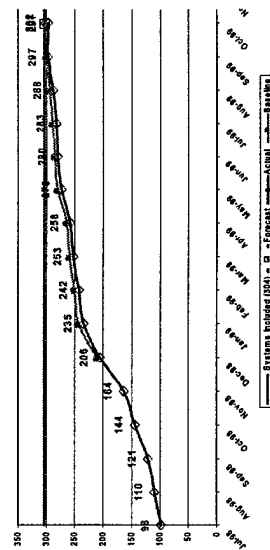
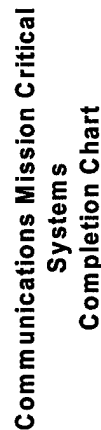
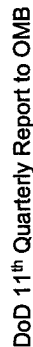
ESP provides a secure web environment that support collaboration tools as well as Y2K database reporting and update capabilities.



Hierarchy of Security Within ESP OSD Y2K Database



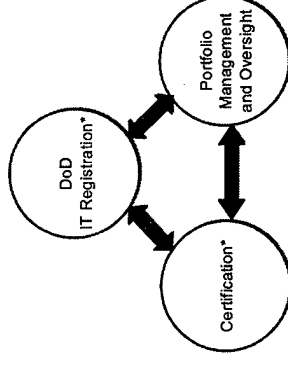
The access control for data and functions within ESP is set up as a hierarchy which allows the services and agencies to manage their own ids and access control for their user community. OSD has high level reporting access to the consolidated information



FY2000 Defense Appropriations

Bill Language

Sec. 8121



- All mission critical and mission essential information technology systems must be registered with the DoD CIO by March 31, 2000
- Systems not registered cannot be funded
- Registration is notification “together with such information concerning the system as the Secretary of Defense may prescribe”

Summary

- Department of Defense will be ready for Y2K
- Significant efforts to reduce risk
- Prepared to respond promptly If disruptions occur
- Working to maintain public confidence