

# DoD Focusing on Year 2000 Computer Fixes

JIM GARAMONE

WASHINGTON — Jan. 1, 2000, is a deadline staring all of DoD in the face.

That's when DoD military and civilian workers find out if years of hard work have been successful. DoD is working to solve its Year 2000 problem.

The Year 2000 problem, its nickname "Y2K" becoming more familiar every day, came from the early days of automated data processing.

Then, computer memory was precious. To save memory, programmers for decades used only the last two digits of years rather than all four — 1998 would be written "98." In 2000, however, when computers see "00," they may not know whether it's 2000 or 1900.

So why is this a problem? The United States runs on computers, mostly linked together. Almost every computer and computer program contains some type of clock or date function. A date error might not affect much in some cases. The results could be disastrous, however, if the date controls electronic bank deposits or critical equipment.

For high-technology, computer-dependent DoD, a Y2K computer glitch might cause an F-15 fighter pilot to crash. A date error in a pay computer system may mean thousands don't get paid on time — or get paid wrong amounts. Telecommunications, transportation, the electric power grid, the movement of gas through pipelines: All these and more are controlled through computer networks. A date error could shut them all down.

"This is really the first major engagement of the information warfare age," said William A. Curtis. He is director of DoD Y2K oversight and contingency planning in the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

"We know what the enemy is, and we know when it's going to strike," he said. "We know what's going to happen. We know what to do to fix it. We're not going to have that sort of perfect intelligence in the next engagement. But how we handle this one will really set the stage for how we handle attacks in the future."

Curtis said DoD expects to spend \$1.9 billion correcting the Y2K problem. All told, the U.S. Government will spend about \$4.3 billion.

According to some estimates, he said, fixing the problem in every automated system in the United States could cost about \$30 billion.

In DoD, the Year 2000 problem is also a readiness issue. The U.S. military mission is to defend the United States and its critical interests before, during, and after 2000. There are 25,000 computer systems in DoD. Of these, officials said 2,800 are mission-critical.

"We must make sure the American people know that they are safe and that our potential adversaries know that the Year 2000 does not pose a vulnerability that they can exploit," Curtis said.

Recent reports by the General Accounting Office, the Office of Management and Budget, and the DoD Inspector General found the Department is about four months behind schedule. But DoD is making progress: A congressional committee assigned DoD a grade of "D" for the last quarter — up from an "F" last time. OMB assigned DoD to "Tier One" — its red zone, meaning DoD must do more, more, more.

"The technology behind this is not tough. We know how to fix it. It's not a technical problem," Curtis said. It is a tremendous management problem. The year problem could be hiding in so many applications, machines, and systems that weeding out every instance is a massive effort, he said.

The goal, simply, is to have computer systems work. To get there, DoD is developing what officials call an Enterprise Level Strategy. At the heart of this strategy are three vectors: report and evaluation, programmatic oversight and coordination, and test and contingency planning.

The report and evaluation vector will help senior management see where problems lie and learn lessons from past experiences. Agencies will report monthly instead of quarterly.

"There are only six quarters left until the year 2000," Curtis said. "We need information monthly so we can see where we need the effort." He said officials have designed the reporting system to be useful and not just a bureaucratic exercise. The core of this effort is a DoD Web site at <http://www.disa.mil/cio/y2k/cioosd.html>. Links to the Department's recently updated Year 2000 Management Plan and much more Y2K information are at this public site. DoD will share information with the GAO, OMB, the DoD Inspector General, and other federal agencies.

The programmatic oversight and coordination vector looks at Year 2000 progress in functional areas and the interfaces among systems, agencies, and allies. Part of this effort is certifying systems as Y2K-compliant. The GAO report found some agencies were confused about the certification process. DoD will change this process so it is uniform across its agencies.

DoD does not operate in a vacuum. DoD systems connect with systems in other federal agencies, private industry, and allies.

Defense Secretary William S. Cohen discussed the Year 2000 problem with NATO defense ministers during the recent NATO Ministerial in Brussels, for example.

U.S. regional commanders in chief are also sensitive to the operational aspects of the Year 2000 problem, and they are working with regional allies to work it out, Curtis said.

The test and contingency vector will be the primary focus in fiscal 1999, Curtis said. Enterprise testing is the hot topic. DoD uses three levels of testing: Systems-

centric tests individual systems; functional-centric tests ensure Year 2000-compliant systems throughout a functional area; and enterprise tests – or mission-centric tests – assure end-to-end performance of systems and interfaces across the range of U.S. military missions.

Enterprise testing extends systems tests to functional area testing and beyond. The regional commanders in chief will combine all these functional areas in enterprise systems tests during exercises. An enterprise system is all functional systems that work together. These tests will begin as soon as possible, Curtis said.

Agencies must, however, develop contingency plans in case the fixes do not work. "There may be unanticipated disruptions," Curtis said. "The U.S. military still has to be ready to accomplish its mission. Contingency plans must be in place."

Other initiatives on the Year 2000 problem are:

- A moratorium on modifications to any computer system that is not Year 2000-compliant.
- Establishing a High Risk Systems Board that will meet with senior leadership of every system in Year 2000 jeopardy.
- Ensuring all mission critical systems have contingency plans.

Also, DoD will establish a Y2K Augmentation Force. This group will man hotlines and update Web sites. It will support mission testing and functional-centric tests. The group will also provide emergency-response teams based at critical areas during the rollover to the new millennium.

"We have redirected our efforts by keeping our eyes on the goal," Curtis said. "The Department of Defense is focused on ensuring we have on Jan. 1, 2000, a force that is able to execute the National Military Strategy, unaffected by a date-related failure of its computer systems."

Editor's Note: This information is in the public domain at <http://www.dtic.mil/afps/news> on the Internet.