National Security and Emergency Preparedness

Telecom News

2000, Issue 1

Published by the Office of the Manager, National Communications System, for the national security and emergency preparedness (NS/EP) community

TABLE OF CONTENTS

What Happened to Y2K? Koskinen Speaks Out ............ 2

When is a New Year Not a Millennium? .... 9

Early Training Helped Y2K Preparation Effort .... 15

Y2K Investments Were Sound, Industry Spokesmen Say Warnings, Remediation Believed Necessary . 16

Washington Officials List Lessons from Y2K Experience ....... 18

McConnell Says Localized Y2K Glitches May Continue to Emerge ................... 19

Y2K: Looking Ahead, Looking Back ........... 19

Y2K Made Public Better Prepared for Disasters ................ 20

# Y2K Bug Doesn't Infect NS/EP Telecommunications

By Steve Barrett
Customer Service Division,
OMNCS

As millions of Americans watched 2000 arrive with fanfare, frenzy, and fireworks, members of the National Communications System (NCS) stood ready to monitor potential telecommunications outages from around the world.

Y2K WRAP-UP ISSUE

Emergency Response Team (ERT) members with the NCS' National Coordination Center for Telecommunications (NCC) were working 8- to 12-hour shifts to track telecommunications problems, alert Government authorities about potential problems, and coordinate restoration efforts with the telecommunications industry.

ARTEL's Ken Carpenter monitors radio reports from some of the 312 SHARES stations standing by to assist in emergency telecommunications during the Y2K rollover. The SHARES Coordination Network received over 1150 availability reports from all 50 states, Puerto Rico, Canada, and Guantanamo Naval Base, Cuba. (Photo by Robert Flores, Defense Information Systems Agency.)

But as the 2000 rollover moved through each world time zone, it soon became obvious major outages were not going to occur. Although a couple of minor incidents were reported, the overwhelming majority of the Nation's telecommunications infrastructures remained

See Y2K Bug, page 11

*NS/EP Telecom News* is published quarterly under the auspices of Ms. Diann McCoy, Deputy Manager, National Communications System (NCS), to provide readers with analytical reports on issues relating to NS/EP telecommunications. Articles printed herein are for informational purposes only and do not necessarily represent official OMNCS or NSTAC positions. We invite NCS member organizations and other readers to comment on articles and suggest future topics for consideration.

▲ ▲ ▲

**For further information or additional copies, please contact:**

**Stephen Barrett**
**Office of the Manager**
**National Communications System**

**Customer Service Division**
**701 S. Court House Road,**
**Arlington, VA**
**22204-2198**

**PHONE: (703) 607-6211**
**FAX: (703) 607-4826**

**Home Page:**
**http://www.ncs.gov**

# What Happened to Y2K?

## Koskinen Speaks Out

The costly effort undertaken in the past two years to deal with the Year 2000 (Y2K) computer problem prevented massive disruptions in systems and services during the date rollover into the new millennium, according to White House Y2K coordinator John Koskinen.

Koskinen, Chair of the President's Council on Year 2000 Conversion, said in a January 18, 2000, interview in Washington that the relatively problem-free date change that occurred is an indication not that the Y2K problem was not serious, but that the work devoted to fixing thousands of computer systems worldwide was successful.

Koskinen said the absence of serious Y2K disruptions in developing countries, where remediation efforts had lagged behind those in industrial countries, is explained by the less intense reliance in those countries on digital technology, and by the fact that they were able to apply the lessons learned from dealing with the problem elsewhere.

Koskinen spoke with the Office of International Information Program's Paul Malamud about the smooth transition into the year 2000, and the work that made it possible.

**Q: January 1 has come and gone, and reports show that there were fewer disruptions of computer operations and infrastructure, on a global basis, than some had feared. In retrospect, do you feel the advance publicity and the large amount of money that went into fixing computer systems worldwide was overblown? Could this have been handled by smaller "fixes" performed on an ad hoc basis after January 1?**

Koskinen: I think a lot of people did do it in an ad hoc way, at the end, and seem to have gotten through it well. However, for organizations using large information technology structures there was no way they could do it at the last minute.

The major banks around the world worked on this for several years together, because you are talking about organizations that have millions of lines of software in code that had to be fixed. In fact, one of the reasons that people thought the world, as a whole, was going to have difficulty was that it takes so long to work through those big systems.

You have to distinguish governmental organizations and private-sector companies that had major software problems from organizations that had more straightforward information technology challenges. I think what happened was that some smaller organizations and governments have less reliance on complicated systems, and therefore, a lot of their systems either were not significantly affected by Y2K or they could take care of those in a relatively short period of time for relatively little money.

When people started working on Y2K no one knew exactly the full impact of potential failures involving large networks of computers. In addition, no one knew where in power plants, telephone systems, or chemical plants date-sensitive “embedded processors” might have a Y2K problem or not. My favorite example is elevators. Two or three years ago, the assumption was that elevators were at risk. There was concern that some elevators—if they were dependent on date-sensitive computer chips—might malfunction. But after about a year of testing, it turned out elevators did not have a problem. This meant that if you were a country or company that started your Y2K remediation efforts late in the game, you learned from the experience of others that you didn’t need to be very concerned about elevators.

And the same in chemical plants. It turned out there are only relatively a small number of critical systems in a chemical plant.

The U.S. Chemical Manufacturer’s Association and the Environmental Protection Agency issued a brochure in the middle of 1999 that said, “These are the systems that are at risk. If you are using these, this is how to fix them; if you are not using these, you are probably in pretty good shape.” So what happened was that as a result of a lot of good work, the countries and organizations that started later had the benefit of all that background and that research and information which was fairly freely exchanged; so that as they moved into late 1999, they could actually focus on things greatly at risk.

But then, turning it around, if everybody had waited until early 1999, I think the people who run the major banks around the world and similar large institutions would tell you the Y2K fix would never have gotten done. In the case of the Federal Government, for instance, we started in 1995 in a coordinated way—some U.S. Government agencies began their Y2K remediation efforts even before that—and people were working into the middle of 1999; four years later they were still working on their systems as fast as they could. So the reason a lot of serious computer programmers thought the world would never make it was because of the magnitude of the challenge.

Now could there have been less hype around the edges of the issue with some people saying the world was going to come to an end because of Y2K? We had a lot of difficulty over the last year and a half convincing people that progress was being made. The Federal Government prediction was that, in fact, there would be no major failures here or around the world, failures impacting entire nations. We also felt there would only be scattered outages in the United States; but that was seen as a minority view by some.

*"I don't think there is anyone who worked anywhere around the world on the problem who thinks that it was not a major problem."*

So there was a certain amount of press coverage and hype about whether or not the problem could be solved that probably we could have done without. Fortunately, however, the public did not overreact, which was our concern. And to the extent that publicity about the Y2K issue got more people in the last six to nine months to really focus on the problem, I think it probably helped us come to a very successful conclusion. I don’t think there is anyone who worked anywhere around the world on the problem who thinks that it was not a major problem.

There is no bank I know, there’s no power company I know, there’s no telephone company I know—I talked to a lot of them—that feel that they wasted their time or their money, or if they had spent just fifty percent less they could have done just as well. I think all of them looking back on it are very pleased that they got through without any difficulties.

**Q: It may be true that the time and financial resources spent reprogramming computer systems were well worth the sacrifice. However, there was also concern about "embedded chips"—that is those computer chips that direct the operations of machines and consumer appliances. There was an assumption they might be date-sensitive and malfunction on January 1, 2000. Yet, there have not been many reports of problems. Why not?**

Koskinen: Well, what happened, fortunately, is most embedded chips turned out not to be date sensitive. There are 30-50 billion out there. When I started this job a couple of years ago, I fondly referred to them as the growth industry of the problem, because people had begun to worry about them, yet there was no way you could get anybody to tell you the answer. I met with manufacturers of various parts of the chips, the chip manufacturers, the people that put them together, power companies, telephone companies—nobody knew the extent of the potential problem.

*"Most embedded chips turned out not to be date sensitive."*

The upshot was that (a) a lot of work had to be done investigating embedded chips, and (b) a lot of people became concerned that this would be a major issue. The advantage of the issue, however, was it got people to look beyond pure information processing. Everybody knew that banks, insurance companies, financial institutions, payroll systems were date sensitive, because they calculated how old you were, how long you had been working, what day of the year it was. People had not spent as much time taking a look at what went on in other kinds of operations: oil refineries, power companies, power plants, etc.

Fortunately for the world—and I think one of the reasons you did not see major infrastructure failure—is the chips themselves generally turned out not to care what date it was. But what we did do, because of the focus on embedded chips, was look at control systems, which are basically software or computers that run operations. So if you go onto a plant floor, you go onto a ship, you go into an oil refinery, what you see increasingly [are] people sitting at computers running the place. They are getting information from all those embedded chips and then it's all coming into a computerized process.

So the reason, for instance, that airports had a problem with runway lights was not because the lights themselves had embedded chips in them that had to care about what date it was, but the chips in the lights fed into a control system that set the cycling for the lights, and that control system cared what date it was. So the bottom line was, embedded chips turned out to be much less of an issue than people worried about: once you could find the control panels, you needed simply to update or check those. And, of course, these issues are only relevant when sophisticated control systems are in use.

As we became familiar with the issue, we began to appreciate the extent to which technological development varies throughout the world.

A lot of operations crucial to the functioning of industrial infrastructure turned out to rely on manual or analog, rather than digital, controls. It turned out a lot of the power companies and telephone processes around the world were, in fact, not affected by the embedded chip problem, which is why those countries had to spend less and also why they had less difficulty.

But even in the United States and England and places where they have very complicated systems, because they paid attention to them early on, they were able to replace the switches, replace the control systems wherever they needed to, to make sure they could continue to run them. I think we got lucky in the sense that it turned out the potential for the chip itself to stop the operation was relatively minor. The risk turned out to be again back in the software control processes, but it was important to find those to make sure that smart building systems, card access systems, plant control systems in those computers were checked. Because up until that time people were only looking at their financial management systems.

**Q: Some press reports estimate $200 billion was spent worldwide on preparing for Y2K. Do you believe that is an accurate figure?**

Koskinen: I think that's liable to be a more accurate estimate than the $600 billion number you see. This problem has been unique. It has been global. The early estimates were that $300-600 billion would have to be spent. That range itself gives you an idea that those are pretty much guesses.

We are very confident we know how much the Federal Government spent, which was $8.5 billion. The Commerce Department last fall did an analysis of all the available reports of actual expenditures, and estimated that in the United States, the Federal Government, and others spent about $100 billion to remedy the Y2K problem. We estimate that that's probably close to half of what the world spent, so that's where the $200 billion comes from. That's the lowest number you'll hear.

Everybody's still talking about $3-, 4-, 500 billion. I think those numbers do not correspond to reality. But even if it is only $200 billion, that's a lot of money.

**Q: Did the Y2K remediation process turn out to be a financial bonanza for computer engineers, consulting firms, etc., who were called in? Some have suggested they may have had a stake in emphasizing the seriousness of the problem.**

Koskinen: No, I think actually if you look at it, at least in the United States, a lot of corporations and certain Federal agencies did the work themselves, with their own staffs. There clearly were consultants and people willing to work on the outside, and one of the concerns when I started this job was there wouldn't be enough programmers available anywhere to be able to deal with the problem. The shortage of programmers never turned up. This was, in part, because people got better at figuring out how to fix these systems with windowing techniques and other technical fixes and partially because as work got done, people doing that work were freed up to work on other systems.

Although it's hard to pin down the statistics, I think a significant amount of the work was done internally, in many places. A significant amount of the money spent to remedy the problem went for upgraded equipment. Some people say that this was all a plot for all the information technology companies to sell more stuff. The truth is more subtle. Many of the companies that produce information technology over time provided free computer software "patches" designed to thwart the Y2K bug, or other kinds of free upgrades or information. When questioned about Y2K, the answer from these companies wasn't necessarily "Buy a new one of our things." The answer was in three categories: either "It's okay," or "It's okay with a fix that we'll provide to you—either sell it to you or give it to you," or "It's too old and we are not servicing it anymore and it doesn't work and you have to get a new one."

*"Some people say that this was all a plot for all the information technology companies to sell more stuff. The truth is more subtle."*

I think what happened with a lot of companies, and where a lot of the money was spent, was they looked at old legacy systems and decided that since they were going to replace those systems sometime in the next two to three years anyway, they might just as well replace them now, rather then fiddle around and try to figure out how to fix them.

I think part of the reason people are talking about a productivity gain in the global economy in recent years is that, prompted by fears about Y2K, a substantial amount of the money went for consolidating and getting rid of old legacy systems and developing and buying new, more productive and more efficient systems. Around the edges, I am sure there were some consultants trying to sell people a lot of fancy new things for no particular good reason. But I think that was a very minor part of the process.

The $100 billion in the United States was spent by thousands of different organizations, each one making its own judgments. The major Fortune 500 companies in the United States are not naive. They are not run by people who are bamboozled by sales people, either internally or externally. I think they ultimately are people who spend their money carefully.

*"The indication of the magnitude of the problem is that in most cases people found it took longer and it cost more and was more complicated than they estimated."*

If you look at their information technology budgets, most of them went up over the last two or three years. They went up not because somebody was doing a good sales job. They went up because people were discovering how difficult it was to solve this problem.

The Federal Government was the same way. We started with a Y2K budget under $3 billion and the number kept getting larger because it took more and more time, people discovered, to actually fix the problem. And so the indication of the magnitude of the problem is that in most cases people found it took longer and it cost more and was more complicated than they estimated. And these are people who are experts. They aren't naive managers employing 25 people. These are large organizations with their own in-house staff and very sophisticated managers who discovered that, in fact, in many cases it took hundreds of millions of dollars to solve the problem.

**Q: Don't mainframe computer systems tend to get replaced anyway, due to rapid advances in technology and speed?**

Koskinen: Yes. I think for those people that was their judgment. In many cases they did not realize how old and inefficient their legacy systems were or how many they had; when they looked at it, they said, "Why don't we just get rid of all this stuff?" In fact, our view five years ago in the Federal Government was that this would be a great time to inventory our own systems and get rid of the ones that were inefficient or complicated to run or always breaking down, and to procure more modern, standardized off-the-shelf equipment. I think you can find that in 20-25 percent of the cases in the Federal Government that's what happened.

**Q: Looking at developing nations, what was the extent of the problem there, as it finally manifested itself?**

Koskinen: It is always difficult to know what is going on in other nations. What we do know is that when we assembled and invited the Y2K coordinators from around the world to meet with us in December of 1998 at the United Nations (U.N.), we had about 120 countries there, and probably half of them weren't sure exactly what this problem meant. But they all agreed to work together and share information on a regional basis and on all the continents around the world.

When we had them back to the U.N. in June 1999, we had 173 countries represented—the largest meeting in history of the United Nations. And it was clear that all 173 of those delegates knew that this was a problem of some degree in their country that they needed to deal with.

Our advice to them, as to smaller businesses in the United States, was not that they go buy everything new. We advised them that some things would be just fine, but that they should take advantage of the information available, assess each situation, find out what's actually at risk, and deal with that.

Increasingly, it became clear that most developing nations didn't have much digital information technology: their power systems, their telephone systems, a lot of their systems were analog. They were automated, but their analog devices had gauges instead of digital readouts and, therefore, they didn't really have any major risks.

Our concerns, I think theirs, were primarily wherever they had gone into the digital area, particularly in financial transactions. You can take your credit card around the world and get cash almost everywhere these days. All of that depends upon financial and telecommunications systems that are interconnected between nations and continents. These were what were most at risk, it turned out. But what was going on at the same time was the central bankers of the world, out of Basel, were working with all central banks in the world and all market regulators to share information and to try to make sure there wouldn't be serious problems come January 1, 2000, with the international flow of financial transactions.

I think because of the kind of international effort and the fact individual nations paid attention to the issue where they needed to, we've only seen a few glitches—some, but just a handful of glitches in financial systems or similar telecommunications networks.

**Q: Suppose no attention had been paid to the problem and no efforts made to fix the Y2K bug in advance of January 1. What would have happened?**

Koskinen: It was clear two years ago to me after talking with a lot of experts, if nobody did anything else beyond what they had already done up until two years ago, that the world as we knew it would end. The New York Stock Exchange would not have been able to open on January 3, the financial markets would have closed, the banks would have had very great difficulty calculating accurately the money they were owed, or the money they owed to others. Payroll systems and other basic complicated financial systems in the U.S. would not have functioned.

And over time we would have had a clear degradation in telecommunications and some power systems. I think that we wouldn't have had to wait very long, if we had done nothing. As systems started to operate, they would have stopped. In fact, in spite of our largely successful remediation efforts, I have seen a list of about 90 glitches and failures around the world due to Y2K problems. This list is an indication where we were headed if we didn't do anything.

My disagreement with the doomsayers was the view that we could never fix it. Some believed that it was such a complicated problem and it infected everything potentially and that we'd never get enough cooperation, enough work done together, enough information sharing, to be able to get it done in time.

*"I think because of the kind of international effort and the fact that individual nations paid attention to the issue where they needed to, we've only seen a few glitches."*

My view was that if we mobilized all possible resources, we could, in fact, make a significant impact on minimizing the risks. If you talk to major financial institutions in this country, major banks, major telephone companies, they will all tell you that they are delighted and breathing a great sigh of relief that their systems are running today. They are confident that they wouldn't have run if they hadn't done all this work in advance.

In the State of California, Los Angeles County, an enormous jurisdiction, estimates that about 60 percent of their intelligent systems would have stopped. They'd looked at, literally, thousands of systems—they went through them all—and the vast majority of them had problems that if they hadn't corrected them would have stopped them cold—they would not have been able to pay benefits to local people, they would not have been able to pay their payroll.

So the irony is that because people worked at it in such a consistent way, and there was effective information sharing, and because people got better at it as we went through it, people are now questioning whether it was a big problem in the first place. Historically, in information technology the world hasn't done well with big problems.

Major projects usually cost too much. They take a long time to get done, and they usually don't work well, which is why a lot of the doomsayers were information-technology programmers. They weren't people off the street—they were people who looked like they should know. Some of them said it would be impossible. So one of the great ironies is, the world having pulled together to meet this challenge and deal with a major information technology problem, having done it not a hundred percent perfectly, but pretty well, close to 98 percent perfectly, we now confront the other side of the coin—"Could you have spent less"? Oh, that's a good question to pursue, but when you're running one of those companies, if you had a major failure in the first week of January, in the year 2000, the acceptable answer wouldn't be "I didn't quite get it done," but "Look how much money I saved by not fixing it right."

**Q: Does the Y2K experience hold any long-term implications for the global information infrastructure?**

Koskinen: There are a number of possible implications. Many organizations worldwide now have a better inventory of their information technology, and a better understanding about the critical nature of it. In the future, they'll manage these systems better.

In addition, I think focusing on the Y2K risk will help us with understanding issues of information security as we go forward. Information security has not received the attention it deserves, just as information technology itself in some places has been seen by top managers as peripheral to the function of an organization: "Well those are the geeks, those are the techie guys, I don't know what they're talking about."

I think what happened with Y2K is chief executives, national leaders, top managers, discovered that you don't need to know about "bits" and "bytes," the technical language of information technology, to understand that if it doesn't work you are out of business. People running organizations understand that the operations of information technology and the security of information technology go to the core of their ability to run their systems and run their businesses. So I think that that will help us as we go forward, ensuring that, in fact, we provide the appropriate protections for those systems in the future.

And as we've said, I think most people will have better systems when they get done with it. They will have upgraded; they will have replaced their legacy systems. Finally, in terms of national and international cooperation, it's not quite clear where it goes into the future. Within the United States, you've seen a tremendous amount of information sharing and cooperation within industry groups and across industry groups trying to deal with this problem.

In addition, there are better lines of communication between the private sector and the Government sector in a lot of countries. Then we had this kind of unique cooperation on an international organizational basis with national coordinators representing individual nations, and so we have a list now of 173 national coordinators that we've been sharing information with back and forth who have been holding regional meetings.

There have been at least two regional meetings in every continent of the world in the last year, sharing information, working together. What you're most likely to see in the future is that, on a regional basis, countries that have worked together on information technology for Y2K are likely to continue to do that.

South America is now talking about how they can continue this kind of informal information sharing, to do a better job with electric power, and oil and gas development now that they see how it all relates for the first time throughout the continent. We've had some discussion with the national coordinators at their request.

Is there a way to continue this informal, non-bureaucratic approach to sharing information? It's not quite clear where that'll go. There are a lot of different initiatives for improving the use of information technology in the world and nobody wants to duplicate those efforts. But on the other hand, one of the unique things about Y2K was it was dealt with generally very effectively by ad hoc coalitions.

The International Y2K Cooperation Center was funded by the World Bank with contributions from the United States. It had an affiliation with the U.N., but it was really a freestanding organization. And the Joint Year 2000 Council, which functioned under the Bank for International Settlements, with market regulators and insurance regulators as well as bank regulators, was pulled together as an ad hoc group. Over 200 major financial institutions in countries around the world cooperated in ways they never had before.

They all had a goal, which was we had to deal with Y2K. So there was a common enemy that people could deal with. Now that we've dealt with that, there's a common goal of everyone being more efficient in using information technology and taking advantage of it. Whether we'll be able to figure out how to capture that experience and that momentum going forward into the future is still not clear. Groups won't do well just meeting for the sake of meeting. I think there is, at a minimum, a great interest in developed as well as developing countries to find a way to continue to share information about what's going on with electronic commerce, what's going on with information security, but it's still open as to what will come of this.❖

(Courtesy of the Office of International Information Programs, U.S. Department of State.)

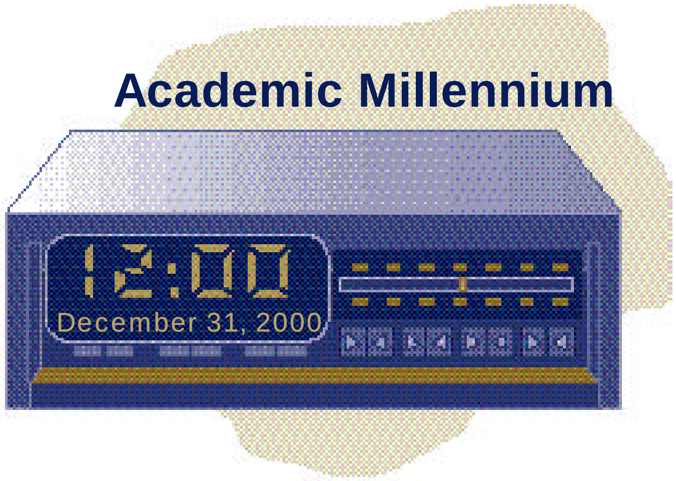
# When is a New Year Not a New Millennium?

Commentary by Don Carr
Fort Belvoir Public Affairs Office

I got a "Millennium Countdown Clock" for Christmas. It's a digital clock with "01-01-00" on top and "It's coming ..." on the bottom. Instructions that came with it said the clock was preset to count down to midnight, December 31, 1999. The manufacturer calls that the "Celebration Millennium." There are also instructions for resetting the clock to count down to midnight, December 31, 2000, what the manufacturer calls the "Academic Millennium."

So, thanks to my "Millennium Countdown Clock," things I've been confused about for 30 years of military and Federal service are suddenly clear. Take promotions, for example. I always thought the only way to get promoted was to achieve some time-in-grade or service milestone. That's "academic," right? Now, thanks to the Millennium Clock people, I know I can just tell my supervisor, "Hey, promote me **NOW** ... I wanna party ... it's called a 'celebration' promotion!"

You might guess that I've grown really weary of "millennial hype." I'm one of the six or seven on the planet who believes that, contrary to overwhelmingly popular belief, the last midnight of 1999 was ***not*** our entrée to "the new millennium." In spite of all the hype and circumstance that came to a head that night and the next Saturday morning, the "First Baby of the New Millennium" hasn't been born yet. "The First Marriage of the Third Millennium" hasn't occurred yet. Nothing of the sort is possible, since the third millennium has yet to begin.



A lot of those who ***say*** we've entered the third millennium (thinking that to ***say*** so ***makes*** it so) actually know better.  But, they're the sly and cunning ones who say it to you while asking you to come buy something.  Marketers know words like "new," "millennium," "gala," "final," and "celebration" combine magnificently as potent ammunition in their assault on our wallets. Marketers take as gospel P.T. Barnum's credo that there's a "sucker born every minute" who just ***knows*** there's more to new years than, well, buying new calendars.

Things got downright bizarre last New Year's Eve. One has to wonder about all those couples who got married at midnight on December 31, 1999, to stake a claim to the "first marriage of the new millennium."  A couple from right here in Virginia flew to the Fiji Islands to lay claim to the "First Marriage of the New Millennium in the Whole World."  Each new day breaks somewhere around Fiji, see, where a hotel invited the couple to have their wedding there.  (Can't wait to see what that hotel plans for January 1, 2001 ...)

What about all those kids born in hospitals claiming to be the "first babies born in the new millennium"? I couldn't believe the cat fighting that went on between area hospitals trying to lay claim to the "first millennium baby."  One hospital called the media to report a baby born at 12:01, only to learn another hospital had already staked that claim.  So the first hospital called in a second time to report that, "Our doctor was wrong ... the baby was born at 12:00:30, so ours was the first one after all."

The Y2K "non event" added to the confusion. Some genius a few years back decided that, since 2000 is a millennium year, it would be nifty to refer to the problem as "the Millennium Bug."  The masses took that to mean, "Yeah, we **ARE** going into a new millennium ... what a perfect time for the computers to go berserk ...."  And there you have it:  every Y2K warning was a reminder that that's when "the New Millennium" begins.

Wrong, unless you count years differently from how you were taught to count.

Think about it.  Would you accept a $1,999 paycheck from an employer who agreed to pay you $2,000?  Does it matter or doesn't it?  If I gave you $2,000, how would you be sure?  You'd count it, right? And you wouldn't count the 2,000th dollar until you laid it out on the counter, right?

Well, silly as it sounds, the fact is that the year 2000 isn't out on the counter yet, so how come people accept 1,999 years as a millennium?

Part of the answer is that a whole lot of organizations and publications put out "Millennium" souvenir catalogues, brochures, newspapers, and magazines last year.  One local paper devoted an entire issue of its glossy Sunday magazine to photos of what it called the "American Century."  That's fine, and it's definitely a keeper as far as coffee table decorations go.  But, it lops off an entire year of said century.  Why couldn't they have waited until **THIS** year and published photos from the ***whole*** century?

Indeed, the media should carry most of the blame for people not wanting to wait just one more year to celebrate "the new millennium."  Thanks to media wanting to be right in the thick of it, things got downright stupid as we entered the holidays.  Newspapers, radio, and TV stations reported with abandon about plans for the upcoming "New Millennium."  They reported official proclamations of the "last [insert your favorite observance] of the century" (yep, people who screw up millennia generally screw up centuries, too, since centuries and millennia tend to run in tandem).

Journalism schools teach that about the only thing worse than getting facts wrong is to go ahead and publish them, anyway.  In that light, this "millennium hangup" isn't a trivial one.  The issue gets to the credibility of the source reporting a claim as fact without question.  It is the ***opinion*** of those who hyped it as fact that 2000 brought us the new millennium.  Instead of challenging the point, most media jumped on, with the apparent attitude that, "Hey, it don't matter."

How would you, gentle reader, like it if the *Belvoir Eagle* were to get the facts right only when it chooses to, and play around with them whenever, in someone's **OPINION**, it doesn't matter?

Facts, like paychecks, do matter.  It matters that we've not yet had the 20th century's—or the second millennium's—final President's Day, Valentine's Day, Army Birthday, Fourth of July, Veterans Day, Thanksgiving, or Christmas.  We will only achieve such milestones ***this*** year as we reach their dates on the 2000 calendar.

The year 2000 **IS** a "millennium year." The way I look at it, 2000 gives us 366 days (did you know 2000 is a leap year?) to celebrate **TWO** millennia, the one we're about to close, and the one we're about to open. I humbly suggest that, all year long, we celebrate a two-for-one, out-with-the-old-in-with-the-new "Millennial Gala."

But, brace yourself for what I call the "Y2K+1" warning. Beware those bearing baubles inscribed, "01-01-01: The New Millennium—This Time It's Real!"

I say we just party around them.❖

(Carr is Chief of Command Information and Media Relations at Fort Belvoir, Va., where this commentary appeared in the *Belvoir Eagle*. Carr's opinion is not necessarily that of the National Communications System.)

## Y2K Bug, cont'd from page 1

National Coordinating Center for Telecommunications (NCC) Manager Bernie Farrell briefs Emergency Response Team members on current operations in the NCC conference facility, converted to a backup operations center during Y2K operations in December and January. The conference room was used for conference call briefings, but monitoring operations remained in the NCC Operations Center. (Photo by Robert Flores, Defense Information Systems Agency.)

active—unaffected by the rollovers on New Year's Day.

For thousands of technicians worldwide, solving the Year 2000 (Y2K) technology problem involved identifying and implementing technology to ensure computers and software throughout the Nation and the world would recognize "00" as 2000 and not 1900. Because the response of computer systems to this problem was not fully understood, in an electronic information-dependent society the Y2K technology problem could have caused a serious dilemma, interrupting key services like transportation, banking, power, and telecommunications.

As a result of the Nation's successful Y2K preparations and the lack of problems in the telecommunications sector, the country (and the world) saw a New Year's holiday celebrated by millions without Y2K incident.

Bernie Farrell, Manager of the NCC, said he was not surprised at the lack of telecommunications problems—both stateside and worldwide. "The telecommunications industry had conducted extensive internal testing as well as testing between and among national and international partners," he said. "Additionally, our almost daily contact with industry representatives—knowing the extent of the contingency plans provided a level of confidence that, in the small chance something did go wrong, all the right players were in place to quickly rectify the situation."

In following the lead of the President's Council for Year 2000 Conversion, the NCC activated 24-hour operations on December 30, 1999. During the first few hours, the NCC staff finalized their computer network connections with both the Y2K

Don Smith of the NCC monitors Y2K reports headed to the President's Y2K Information Coordination Center, while Gerry Versis (left) and Julia Brown scan incoming reports. The three team members worked day shifts during NCC Y2K operations. (Photo by Robert Flores, Defense Information Systems Agency.)

Information Coordination Center (ICC) and the Federal Emergency Management Agency's (FEMA) 's emergency operations center.

Staffing the NCC was a variety of Government personnel, telecommunications industry members, and Government contractors ready to tackle the Y2K challenge as a team. NCC ERT members were ready to process incoming telecommunications reports from 82 national and international telecommunications companies, monitor High Frequency (HF) radio transmissions through the Shared Resources (SHARES) HF Radio room, and report telecommunication status information to the ICC. "We also had staff in the ICC providing status nationally," said Farrell, "and a representative prepositioned at FEMA headquarters in case a disaster occurred during the rollover."

Yet because there were few problems, the NCC New Year's watch went from a fully staffed, 24-hour operation to a minimally staffed Y2K watch over the New Year's weekend. By the time midnight on New Year's Day hit Los Angeles, Seattle, and San Francisco, the NCC began reducing staff—keeping in mind that the first business day was still to come.

### Database Success

Although the Y2K problem never materialized, Farrell was pleased with the success of the telecommunications database reporting system designed for the

Y2K. "The information provided through the database was more than was needed to meet our ICC requirements, he said."

The database consolidated input from telecommunications companies worldwide and permitted NCC personnel to identify, analyze, and report potential telecommunications outages. Farrell said the system first surpassed the NCC's initial goals of U.S.-only information sharing. They then added 19 Canadian companies and 70 International Telecommunication Union (ITU) member companies to provide an early warning capability for all participants.

"Major segments were part of the ITU testing program, so we were confident that the telecommunications sector would be viable," said Farrell. "We did not, however, have detailed information on the state of readiness of supporting infrastructures, and that was cause for some concern—will the power grid fail and cascade into a telecommunications outage?"

However, Farrell said that in a very short period of time, the NCC was able to translate industry's and Government's requirements into a viable tool. "We provided the means for anonymous reporting for those that wished anonymity, while allowing groups to share predetermined elements based on the sharing agreements," he said.

From the time the Operations Center went operational on December 28, 1999, until the NCC stopped monitoring input on January 4, the NCC system received more than 95,000 "hits" from the telecommunications companies participating in the information sharing program with the NCC. The system recorded over 40,000 hits on New Year's Eve as companies around the world began reporting pre- and post-rollover information.

NCC ERT personnel recorded an additional 45,000 hits in monitoring system updates.

Over 90 command centers worldwide submitted status reports to the NCC—ranging from a low of 20 reports during the initial day to nearly 260 reports during the New Year's Eve-New Year's Day timeframe. "We had daily conference calls with all U.S. participants," said Farrell, "and were connected via private lines to major telecommunications industry Y2K operations centers, as well as the ICC, and key federal departments and agencies."

During this time, Farrell said there were three cases where Y2K trouble reports—tickets—were shared with telecommunications industry representatives. Two of the three incidents occurred overseas and were handled by regional companies.

Farrell said none of the database users reported any degraded performance, although the system had a brief 5-minute outage on January 3—3 days after the critical rollover period ended. Farrell said the outage was caused due to a conflict with backing up information to a tape.

## SHARES Remained Ready

While the majority of the NCC personnel dedicated their efforts to receiving reports via computer, folks monitoring SHARES HF radio traffic played a crucial role in the NCC's Y2K preparedness.

Also working in shifts of 8 to 12 hours, contract personnel activated the SHARES Coordination Network at 8 a.m. on December 26. During the next 9 days, 312 stations representing 36 Federal, State, and industry organizations participated in SHARES Y2K operations, filing 1155 station availability reports.

Farrell said the operation marked the first time the National Telecommunications Coordinating Network (NTCN) HF Radio, SHARES, the NCS Regional Managers HF Radio Network, and the General Services Administration (GSA) combined resources for a joint, on-air operation.

The SHARES Coordination Network returned to routine operations on January 3, 2000.

## GETS Also Prepared

As 2000 arrived, national security and emergency preparedness (NS/EP) personnel were also ready to handle priority voice communications through the Government Emergency Telecommunications Service (GETS).

Recognizing the potential impact of the Year 2000 date change on GETS, the OMNCS last spring approached the Alliance for Telecommunications Industry Solutions (ATIS) to have GETS included in Year 2000 tests being planned by ATIS' Network Testing Committee (NTC). These tests included stress testing of calls in a laboratory environment, representing the networks of local,

Emergency Response Team member Dorothy Proctor reaches for a call while monitoring incoming reports during the Y2K rollover at the NCS's NCC. Proctor was one of many NCS members who worked at the NCC during the New Year's holiday. (Photo by Robert Flores, Defense Information Systems Agency.)

long-distance, wireless, and foreign carriers.

After thorough analysis of test data, ATIS reported that "…no Year 2000 date-related anomalies were observed during NTC testing…. All of the GETS features tested performed in the Year 2000 date environment as they did during the baseline test."

GETS personnel anticipated that the New Year's Eve holiday would generate heavy call volume over the Public Switched Network (PSN)—making it difficult for NS/EP users to place emergency Y2K calls. To combat the potential problem, the OMNCS issued over 7,650 GETS cards during Y2K preparations to national, state and local emergency agencies, authorizing their use in the event of Y2K-related problems.

### A Ton of Thanks to All

Farrell said that many OMNCS and contractor staff put in long hours ensuring that the database was operational and providing optimum service throughout the rollover. However, Farrell did single out three OMNCS staffers for their exceptional contributions.

"John O'Connor and Carl Law were instrumental in ensuring the operational integrity of the database, and DeOnna Taylor worked with all of the international partners, overcoming language barriers, making sure only those authorized were granted access, and once granted access provided the necessary training to permit successful participation."

### Next Step - ISAC

With the successful use of the database to monitor Y2K, the system now moves to its next phase —modifying the Y2K database for receiving and processing infrastructure protection data as part of the NCC's new role as Information Sharing and Analysis

Center (ISAC) for telecommunications.

Since going operational March 1, the NCC will gather, analyze, and disseminate private sector and Government telecommunications information to its participating entities. The NCC becomes the central hub for sharing critical NS/EP telecommunications information on vulnerabilities, threats, intrusions, and anomalies between companies and the Government.

"We had the ISAC mission in mind while developing and deploying the Y2K database," said Farrell. "We knew we had to demonstrate that a secure, trusted environment could be built and administered, and that we could properly handle proprietary data."

Farrell believes the NCC database has successfully demonstrated that sharing information can be done and said the NCC now needs to rework the Y2K database into a viable medium for real-time network intrusion reports, network anomalies, and outages.❖

(Gabor Luka of the Technology and Programs Division, OMNCS, contributed to this article.)

# Early Training Helped Y2K Preparation Effort

By Steve Barrett, Customer Service Division, OMNCS

The National Coordinating Center for Telecommunications (NCC) staff prepared for a scenario far worse than what occurred January 1 with Year 2000 (Y2K). NCC Emergency Response Team (ERT) members began preparing for possible Y2K problems as early as last April in a series of training sessions conducted by the Training, Exercise and Regional Support (TERS) Branch, Office of the Manager, National Communications System (OMNCS).

"With Y2K, we faced a different problem than we do when responding to earthquakes and hurricanes," said Bernie Farrell, Manager of the NCC. "Not only did we need to train the teams on the database application, we needed to reallocate our normal response functions to address triaging—how would we address multiple failures occurring internationally?"

Farrell emphasized that the OMNCS had to train teams to analyze patterns that could develop, then identify what the national security and emergency preparedness implications of the failure meant to the national infrastructure.

> *"With Y2K, we faced a different problem than we do when responding to earthquakes and hurricanes."*

In a program touted as "Wipe Out Millie, the Millennium Bug," TERS personnel began training programs designed to inform all OMNCS personnel on Y2K, its potential dangers to the telecommunications infrastructure, and the steps both Government and the telecommunications industry were taking to combat Y2K.

Following two sessions designed to explain the basic information to all OMNCS staff, the TERS concentrated its final two training segments toward ERT members who would staff the NCC during the rollover. Team members received briefings on NCC policy and operations during the 6-day rollover period, and learned how their telecommunications mission tied in with the Information Coordination Center (ICC).

They also attended training sessions on the NCC computer programs and equipment needed during Y2K operations—including the Y2K reporting database, Emergency Response Link (ERLink), Local Exchange Carrier (LEC) Map, and National Telecommunications Coordination Network (NTCN). Team members then were able to practice using the equipment during the "9-9-99" exercise conducted at the NCC in conjunction with the ICC and other Federal agencies.❖

# Y2K Investments Were Sound

## *Industry Spokesmen Say Warnings, Remediation Believed Necessary*

By Leslie Getzinger
Washington File Staff Writer

After the remarkably smooth transition from 1999 to 2000, some critics have been saying the large investments made to deal with the (Year 2000) Y2K computer problem were a waste, but those who actually conducted or presided over Y2K remediation efforts say the efforts clearly were needed.

An estimated $200 billion was spent worldwide to prevent computer date-reading problems from occurring with the arrival of 2000, according to the President's Council on Year 2000 Conversion.

During the briefing marathon kept up by the President's Council during the days of the changeover, John Koskinen—Chair of the President's Y2K Council—said there are still people asking questions about whether it was too much money, and whether Y2K was just hype.

"I think people understand that computers are complicated, these systems are risky," said Koskinen. "What they are as far as I can tell is very satisfied and pleased that the systems [problems] were solved, and that we worked on it together."

*Those who actually conducted or presided over Y2K remediation efforts say the efforts clearly were needed.*

In total, the U.S. Government spent $8.5 billion on Y2K, expenditures closely monitored by the Senate Special Committee on the Year 2000 Technology Problem. Vice Chairman Senator Christopher Dodd said "…the success of the initial rollover period would not have been possible without the painstaking preparations that were made."

Dodd continued, saying that the resources dedicated to reprogramming millions of lines of code, testing and retesting equipment, developing contingency plans, and educating the public were well placed.

The worthiness of the Y2K remediation effort is also endorsed on the international level. In a statement on January 4, 2000, Bruce McConnell, Director of the International Y2K Cooperation Center (IY2KCC) said, "we are proud of the outstanding international program that has successfully addressed the potentially serious impacts of the Y2K computer problem. Unprecedented international cooperation and the dedicated efforts of millions of Y2K workers have given us this exciting result."

But not declaring victory too soon, the IY2KCC will wait to issue a complete evaluation of international efforts in February.

The Department of Defense repaired or modified almost 7,000 systems in its remediation effort. Former Deputy Defense Secretary John Hamre said in a January 4, 2000, press conference that, "…this was an investment that we had to make." Hamre went on to say that future information security efforts are "going to be built on what we had learned from this and using the foundation of the year 2000."

Secretary of Energy Bill Richardson also defended the legitimacy of the Y2K investment. The U.S. electricity, natural gas, and oil industries spent $5 billion on remediation and rapid response systems, and

Richardson said the effort produced “a simple, uneventful, uncomplicated changeover.”

“Millions of Americans potentially could have lost heat and power” if electric and natural gas utility systems had not been fixed,” Richardson said. “Numerous glitches in the global oil supply and delivery system could have combined to disrupt oil flow."

The Federal Aviation Administration (FAA) and the Joint Airworthiness Authorities (representing European aircraft manufacturing countries) got an early start in 1997. At that time, they tested and found “no safety-of-flight issues for airborne systems,” according to FAA Senior International Analyst Craig Lindsay. He continued, “It was necessary to do a complete safety review of the software to come to that conclusion.” However, other problems were identified in ground systems, including air navigation and air traffic control monitoring stations, data communications, and maintenance programs.

Besides preparing for the year 2000, these efforts led to upgrades or replacements of older technology, new contingency plans that can be useful in the future, and enhanced partnerships with companies, international organizations, and foreign governments.

Koskinen affirmed the value of testing and correction that was conducted by the air industry. One hundred twenty airline systems may have malfunctioned had it not been for the $2.3 million spent worldwide, he said. Prior to remediation, he pointed out, potential Y2K problems existed in a variety of air-related services including baggage handling, security access, flight display systems, and runway lights.

Remediation of air traffic control systems fell to the U.S. Department of Transportation, which spent $448 million to fix Y2K problems. Its remediation efforts focused on a variety of public safety areas in addition to air travel, including highways, mass transit, and oil and gas pipelines.

Industries from manufacturing to medicine report they had many systems that would have malfunctioned without extensive remediation efforts.

John Hall, a spokesman for the American Bankers Association, said in a phone interview that without the industry’s extensive Y2K remediation program, automatic teller machine and credit card transactions would have been delayed or declined. He said loan and account balances would have been incorrectly calculated, and direct deposit payments would not have been processed.

Bill Mundt of the Secretariat for the Global 2000 Group, which monitored Y2K preparedness in international banking, said that each bank is reliant on “home-grown” coding of programs that were susceptible to Y2K glitches because every transaction deals with dates. These programs could not be fixed with off-the-shelf patches, but fixes had to be developed on an individual basis. “It cost a lot of money, but we got our money’s worth,” said Mundt.

In another area, David Peyton, Director of Technology Policy at the National Association of Manufacturers said that any cutting, welding, or drilling system with a computer-controlled program would have been affected.

“Time is a critical, essential variable input along with other factors,” said Peyton. “The just-in-time inventory process used by many companies to keep overhead costs low would have been unforgiving to any Y2K-induced delivery interruptions, he said. Trucks transporting products hundreds or thousands of miles only have a quarter to a half hour window at loading docks, so any shocks to the system would have been felt immediately.

According to Bob Cohen, Senior Vice President for the Information Technology Association of America, pharmaceutical companies discovered that fixes were necessary in many facets of their industry, including manufacturing, medical supply systems, electronic payment systems, and date-stamping to indicate potency levels and expiration.

“The amount spent was necessary and appropriate” not just for the pharmaceutical industry but overall,” said Cohen. “No doubt a learning curve developed and those that started first provided guidance for companies that got a late start," he said in offering an explanation of why even organizations that started their remediation efforts late were able to avoid Y2K disruptions.❖

(The Washington File is a product of the Office of International Information Programs, U.S. Department of State.)

# Washington Officials List Lessons from Y2K Experience

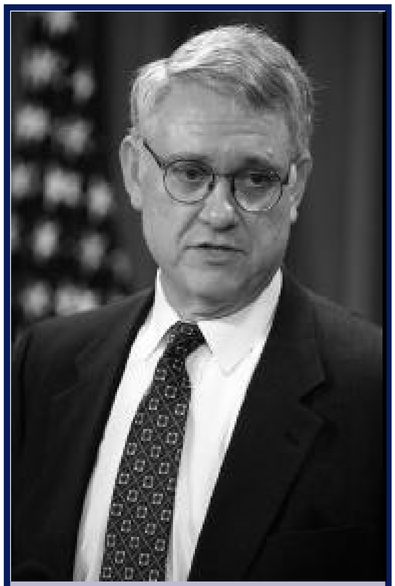
By Thomas Eichler
Washington File Staff Writer,
Department of State

The successful U.S. Government/private sector collaboration over the past couple of years to deal with the Year 2000 (Y2K) date change problem could serve as a model for meeting technology challenges in the future, according to Former Deputy Secretary of Defense John Hamre.

Hamre, briefing February 1 at a Y2K review session at the Center for Strategic and International Studies in Washington, said that preparations for the date turnover proved that partnership between Government and the private sector can solve difficult problems.

Hamre said the Defense Department, with its vast array of computer systems worldwide, experienced only one significant Y2K-related problem—with one reconnaissance satellite and its ground-based information processing equipment. But he said the emergency system that had been set up for handling such failures worked as planned, and backup procedures restored operations in a matter of hours.

Hamre said a major benefit from the Y2K experience in the Defense Department is recognition of the dependence on information technology. The Department, he said, became truly serious about fixing the Y2K problem only when top-level management came to realize that this was not just a technical problem but a "war-fighting problem," threatening the U.S. military's ability to carry out its basic function.



Former Deputy Defense Secretary John Hamre briefs on DOD results following the Year 2000 rollover. (Photo courtesy of DOD.)

Hamre said the Y2K experience also highlighted what will be a major problem for Government and other institutions in the 21st century: how an organization whose elements each have their own top-to-bottom structures can deal efficiently with a problem that cuts across all elements.

Senator Bob Bennett, Chairman of the Senate Special Committee on the Year 2000 Technology Problem, told the group that some of the early fear of widespread Y2K-related disruptions resulted from a miscalculation of the threat from embedded chips. Electronic chips are built into a wide range of modern mechanical equipment, from elevators and fire trucks to medical devices and home appliances. The chips are used so widely that it was impossible to check them all, and some warned that a date change malfunction in even a small fraction of the chips could lead to widespread, and cascading, breakdowns in essential systems.

Bennett said his committee finally came to understand, during the past year of Y2K preparations, that while a certain percentage of chips might malfunction at the time of the date change, such malfunctions probably would not shut down whole systems. After coming to that conclusion, he said, the committee felt confident that the country had time and resources sufficient to deal with the Y2K problem successfully.

Bennett, a Republican, praised John Koskinen, Chair of the President's Council on Year 2000 Conversion, saying he did a "superb job" of focusing attention on the problem and promoting action to solve it.

Bennett said multinational firms played a positive role in worldwide efforts to prepare for the date change. These firms showed their ability to effect solutions, he said.

He criticized some media outlets for their treatment of the Y2K issue, describing his own experiences resisting frequent attempts by reporters to draw from him alarmist warnings and critical comments on Government Y2K efforts.

"First, no one listened" to calls from his Senate committee for attention to the Y2K problem, he said; later the committee was criticized for not being "apocalyptic" in its warnings. Now that the date transition has passed with relatively few disruptions, those who advocated attention to Y2K are being criticized again, he said, on the charge that they exaggerated the seriousness of the threat.

He defended the State Department's late-1999 warnings to travelers of possible serious Y2K-related disruptions around the world. There was no precedent for this kind of problem, he said, and "all wanted to err on the side of caution."

Bennett said Y2K-related computer system malfunctions could occur in the months to come, because many of the "fixes" were only short-term bridging measures, leaving permanent remediation still to be accomplished. These malfunctions, and the steps taken to deal with them, will occur in a "patchwork fashion," he said, and the number and the cost will never be known, because they will be dispersed randomly across the economy and few will bother to report them.❖

(The Washington File is a product of the Office of International Information Programs, U.S. Department of State.)

## McConnell Says Localized Y2K Glitches May Continue to Emerge

Bruce McConnell, Director of the International Year 2000 Cooperation Center, said there continues to be no reports of serious disruptions anywhere in the world due to the Year 2000 (Y2K) computer problem.

McConnell said "localized glitches" would probably continue to emerge over the weeks ahead, but that they will occur sporadically, not simultaneously. "Although they will, in some cases, temporarily degrade quality of service, we do not expect them to proliferate or interact to cause any serious disruptions," he said.

It was believed by some that computer systems might stop working due to the Y2K problem, causing electrical power grids, water systems, or energy supply systems to fail.

When asked why there were not a lot more Y2K-caused failures around the world—especially in countries that had spent far less time and money than the United States in preparing for the year 2000—McConnell said that most countries do not use Y2K-vulnerable digital controls for things like the production of power or telecommunications.

"Digital computers are primarily used to provide management information," he said. "When they fail they can gum up the works or degrade quality, but they don't cause actual service failures. For that reason we were not surprised that there were no major disruptions."

McConnell also admitted that Y2K experts might have overestimated "by a little bit" the Y2K vulnerability of infrastructure systems like power grids, telecommunications, and air traffic. "In the air traffic area...there are manual processes that they go to all the time when there are power outages or the radar goes down," he said. "So that kind of risk management culture in critical service areas has probably mitigated the threat."❖

## Y2K: Looking Ahead, Looking Back

By Paul Stone
American Forces Press Service

Bill Curtis, principal director for the Department of Defense (DOD) Year 2000 (Y2K) repair effort during the past 2 years, looked back recently on his role as one of DOD's key Y2K managers. Curtis said the military learned valuable lessons that will help the department manage information technology in the future.  He said DOD's Y2K repair and testing effort was an investment of time and effort that will pay DOD dividends for years to come.

During the course of the Y2K challenge, he said leaders at all levels came to appreciate the military's dependency on information technology.

"We fixed a lot of infrastructure and an awful lot of computer code got cleaned up," Curtis said. "We've gone into the year 2000 with a much better set of systems than we had before and a far better system for maintaining them.

Other benefits he cited included:

**P** A clear understanding of what systems are vulnerable to computer hackers and how to better protect them in the future.

**P** Development of models to manage and track the use of information technology throughout DOD.

**P** Better working relationships with both Federal agencies and foreign nations—all of which DOD worked closely with to ensure Y2K did not impact either U.S. or overseas installations.

"It was a tremendous effort and we've all learned a great deal from the experience," he said.  I owe a great deal of thanks to those who led the way, from our top leaders on down to those who were fixing the problems in systems throughout DOD.  They're the real heroes of Y2K."❖

## Y2K Made Public Better Prepared for Disasters

While the Y2K "bug" has been costly and anxiety producing for the Nation, there is a silver lining, according to James L. Witt, Director of the Federal Emergency Management Agency (FEMA).

Y2K—while one of the biggest technological challenges ever faced—also gave us an opportunity to raise awareness about the need for general emergency preparedness across the country," Witt said.  "These efforts will go a long way to helping the American people be prepared for the inevitable tornado, earthquake, flood, or hurricane of the future."

FEMA used the opportunity afforded by Y2K to offer specific preparedness advice to families.  All families were encouraged to prepare for Y2K as if for a winter storm. Specifics about storing canned goods, collecting battery-powered flashlights, and storing water were distributed through a variety of publications and through state and local emergency managers.

"Often, the public does not heed our ongoing message that it pays to be prepared," Witt said.  "With Y2K, though, people were paying attention."

Y2K awareness activities meshed with the agency's ongoing efforts to promote risk reduction through Project Impact: Building Disaster Resistant Communities. Under this national initiative, communities work with FEMA, State officials, and private sector partners to assess their particular disaster risk and take pro-active steps to reduce potential damage in the future.

FEMA also found that Y2K helped strengthen working relationships between the agency and state and local governments, increased the agency's outreach to the private sector, and provided an opportunity to update emergency and contingency planning.

"I won't say that Y2K is a beneficial issue," said Witt. "But I will say that there was a silver lining in terms of public awareness about preparing for and preventing disasters."❖

(Courtesy of the President's Council on Y2K Conversion and the Federal Emergency Management Agency.)