National Security and Emergency Preparedness

Telecom News

1999, Issue 1

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

NCC Monitors Plains Tornado Telecommunications Assistance

By Stephen Barrett
Customer Service and Information Assurance Division, OMNCS

While Federal Emergency Management Agency (FEMA) personnel provided assistance to tornado victims in Oklahoma and Kansas in early May, staff personnel at the National Coordinating Center for Telecommunications (NCC) monitored emergency telecommunications support from the NCC's Arlington, Virginia, operations center.

While ready to respond, the NCC did not activate during the tornadoes that killed 43 people, injured over 600, and destroyed more than 2,500 structures in the two states. Although the storms did affect telecommunications services, local and long-distance carriers in Oklahoma and Kansas quickly restored service to the affected areas.

"The state emergency authorities in Oklahoma (and Kansas) worked quickly with their local carriers to establish

See Telecommunications Assistance, page 10

Tom Frello and son Zachary look at their brand new van destroyed by a tornado that devastated areas around Oklahoma City, Oklahoma, on May 3, 1999. (U.S. Air Force photo by Tech. Sgt. Bill Kimble.)

TABLE OF CONTENTS

NS/EP Telecom News is published quarterly under the auspices of Ms. Diane Fountaine, 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 and
Information Assurance
Division
701 S. Court House Road,
Arlington, VA
22204-2198

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

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

John A. Koskinen:

Attempting to Ensure the Y2K Problem is Last Headache of the 20th Century

By Stephen Barrett
Customer Service and
Information Assurance
Division, OMNCS

The Chairman of the President's Council on Year 2000 (Y2K) Conversion said that he does not expect major national disruptions in critical services due to the Y2K technology problem.

Speaking in Atlanta before a Federal Emergency Management Agency (FEMA) workshop last February, John A. Koskinen said there is no indication that the Y2K problem will cause national failures in basic infrastructures such as telecommunications, electric power, banking, and transportation. He also said major local disruptions are unlikely in areas where local governments and businesses are working on the problem.

However, Koskinen said some areas of the country could see problems because their local governments and businesses have not devoted "appropriate attention" to the problem or are lagging behind in their efforts to fix computer systems. He warned that the American public must prepare for the possibility that the Y2K problem could cause temporary disruptions in some basic services.

"By themselves, such disruptions are manageable," said Koskinen. "But the unique challenge the Y2K problem presents us with is the potential of numerous disruptions happening all at once." He said these disruptions would place additional burdens on the most well equipped emergency response mechanisms.

Koskinen said the Nation would be good at responding to individual challenges, but needs to be just as good about responding to multiple challenges. "We need to be thinking about how to best respond to the possibility of failures in a number of community systems that operate communications, emergency services, health care, public works and utilities, and transportation," he said.

President Clinton established the President's Council on Year 2000 Conversion in February 1998 to coordinate the Federal Government's Y2K efforts—focused on ensuring that critical Federal systems would be ready for the year 2000. In addition, Koskinen said the Council is also working to support the Y2K efforts of State and local governments, large companies, small businesses, and foreign governments.

With the year 2000 fast approaching, Koskinen said significant progress has been made in the public and private sectors over the past several months. However, he said despite the best work of everyone involved, some systems will not be ready by the end of the year, creating the possibility for disruptions in key services.

To help ease those disruptions, Koskinen said an important part of the Council's effort involves working with major industry associations in gathering Y2K readiness information. He hopes to make that information available to the public.

"We believe that we can mitigate overreaction by the public to the potential for year 2000 failures by providing them all the information we have—good and bad—on Government and industry progress," he said. "Such information is also critical to the efforts of all organizations to make plans for any contingencies."

The Y2K problem is unique and hard to quantify, which makes preparation all the more difficult.

Koskinen said the Federal Government is now working to develop a mechanism for coordinating responses of Federal agencies to potential Y2K disruptions and to take preventive action where possible. He said this effort—which will rely upon existing emergency structures within FEMA, the Defense Department, and other Federal agencies—will help to improve information flow and will depend upon close collaboration with State and local government and private industry.

Still, information flow is a two-way street, and Koskinen said some of the most important work in emergency response to Y2K would take place at the State and local level. "You can play a key role in assuring preparedness—right now," he said. "As you work to collect assessment information to determine the possible consequences of Y2K conversion in your area, you can motivate critical service providers—both public and private—to take all necessary steps to ensure that their systems are Y2K compliant."

For example, Koskinen said State officials should be reaching out to county and local governments not only to determine the progress they are making, but to also encourage them to share information with their specific public. This information would include the status of key services—like power and water—and information about how local officials are preparing to respond to any disruptions.

Finally, Koskinen said emergency personnel must be prepared to react to new assessment information as it emerges. "We at the Federal level will do all that we can over the remainder of 1999 to ensure that you and the public have the most up-to-date assessment information," he said.

To do that, Koskinen said FEMA's Emergency Education Network (EENET) will be used to share best practices and lessons learned at the local, State, and Federal levels. Programming will include updates on Y2K preparedness through regularly scheduled National Alert Broadcasts and special broadcasts that will cover detailed discussions of Y2K preparedness and training activities.

"Ultimately, we want to ensure that people are as confident in our ability to respond to the Y2K problem as they are in our ability to respond to storms and other natural events," said Koskinen. "This is an opportunity to get out the basic disaster preparedness message that the emergency management community has been advocating for years."

Unlike storms and other challenges emergency responders face, Koskinen said the Y2K problem is unique and hard to quantify, which makes preparation all the more difficult. "But if we work together, I am confident, as the President has said, that we can ensure that the year 2000 problem is the last headache of the 20th century and not the first crisis of the 21st," he said.❖

President Clinton Names Five Members to the National Security Telecommunications Advisory Committee (NSTAC)

President Clinton announced on May 20 his intention to appoint James W. Evatt, John H. Mattingly, Dennis J. Picard, Michael T. Smith, and Lawrence A. Weinbach to the President's National Security Telecommunications Advisory Committee (NSTAC).

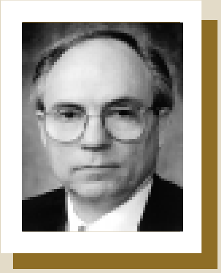
James W. Evatt, of Newport Beach, California, is President of Information and Communications Systems, one of three major business units of Boeing Information, Space and Defense Systems. He is responsible for the following product lines: satellites, Airborne Warning and Control Systems (AWACS), airborne lasers, aircraft information systems, and strategic missiles.

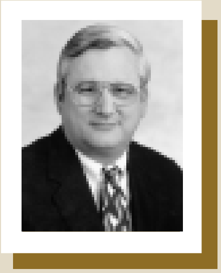
Prior to this assignment, Evatt was Boeing Defense and Space Group Executive Vice President for Business Development, responsible for developing and implementing a growth strategy for the defense and space operations of The Boeing Company. He was also Vice President of the Business Development Organization, where he was responsible for finding and developing business opportunities for Defense and Space.

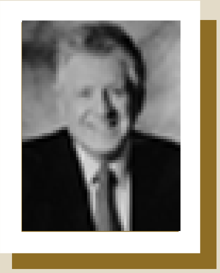
John H. Mattingly, of Fairfax Station, Virginia, is President of COMSAT Satellite Services, an organization created to manage COMSAT's international satellite services. In addition, Mattingly oversees COMSAT's current efforts to restructure INTELSAT and privatize Inmarsat and leads COMSAT's development of advanced services and technology to meet the growing demand for high-speed data and multimedia communications via satellite.

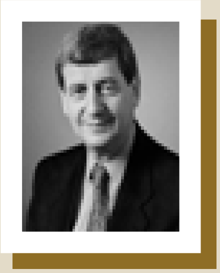
Before becoming President of COMSAT Satellite Services, Mattingly held a number of key management positions in COMSAT. Prior to joining COMSAT, Mattingly served in several managerial and executive positions at OrionNet, Inc., GTE Spacenet, and CONTEL ASC.

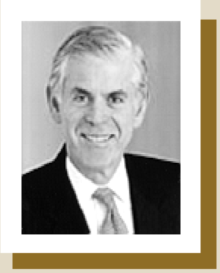
Dennis J. Picard, of Concord, Massachusetts, is


James W. Evatt


John H. Mattingly


Dennis J. Picard


Michael T. Smith


Lawrence A. Weinbach

The NSTAC provides the President with information and advice from industry's perspective regarding specific measures to maintain, protect, and enhance the nation's telecommunications resources that support national security and emergency preparedness capabilities.

Chairman of the Board and Chief Executive Officer of Raytheon Company, Lexington, Massachusetts. He assumed this position on March 1, 1991, after serving as the company's President since August 1989.

Picard was elected a member of Raytheon's Board of Directors in January 1989. He has held numerous other positions with Raytheon, ranging from General Manager of the Missile Systems Division—Raytheon's largest unit—in 1983, to Senior Vice President of Raytheon—a position he earned in 1985.

Michael T. Smith, of Marina Del Rey, California, is the Chairman of the Board and Chief Executive Officer of Hughes Electronics Corporation. Previously, he had served as Vice Chairman of Hughes Electronics Corporation and Chairman of the Hughes Aircraft Company.

Smith joined Hughes Electronics in 1985, the year the company was formed, as Senior Vice President of Finance, after spending nearly 20 years with General Motors in a variety of financial management positions. Hughes Electronics was formed after General Motors acquired Hughes Aircraft Company. He serves on several corporate boards and councils.

Lawrence A. Weinbach, of New York, New York, is Chairman, President, and Chief Executive Officer of Unisys Corporation. Weinbach joined Unisys Corporation in 1997, after completing his second four-year term as Managing Partner and Chief Executive of Andersen Worldwide, a global management and technology consulting firm.

Weinbach held a number of leadership positions at Andersen Worldwide from 1961 until his departure in 1997. Weinbach has taken an active role over the years on the boards of numerous "not-for-profit" organizations.

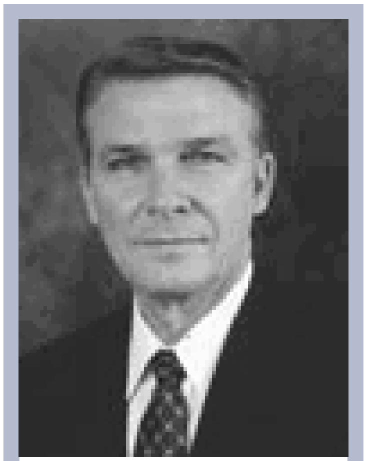
The NSTAC provides the President with information and advice from the industry's perspective regarding specific measures to maintain, protect, and enhance the Nation's telecommunications resources that support national security and emergency preparedness capabilities. The Committee addresses telecommunications issues throughout the year and periodically reports directly to the President and also to the Secretary of Defense, in his capacity as Executive Agent for the National Communications System.❖

(Courtesy of the White House Press Office.)

FEMA Director Witt Announces New Project Impact Communities

Federal Emergency Management Agency (FEMA) Director James Lee Witt announced 60 new Project Impact disaster-resistant communities on December 10, 1998. The announcements were made during a press conference at the inaugural Project Impact: Building Disaster Resistant Communities Summit in Washington, D.C.

FEMA held this summit to recognize and reward those people and communities who have worked toward saving lives and reducing damage from disasters. Project Impact is a national initiative designed to challenge the country to undertake actions that protect families, businesses, and communities by reducing the effects of natural disasters.



James Lee Witt

"I am pleased to welcome these 60 new Project Impact communities to the forefront of disaster-resistance," said Witt. "The new communities we announce today join our nationwide campaign to change the face of America's communities. It is a campaign that promotes individual, corporate, and community responsibility for saving lives, protecting jobs, and reducing property losses."

In just over one year, Project Impact has grown from seven pilot communities in seven states to an average of two communities in every State. The addition of these new communities brings the total number of Project Impact communities to 117.

"What we are witnessing here is an outstanding growth rate that can be credited to a rising interest among individuals, businesses, and communities in becoming disaster resistant," said Witt.

In each new community, a local partnership of government leaders, representatives of the business sector, and individuals will provide funding, in-kind services, technical support, and labor to undertake disaster-resistant activities. In addition, FEMA will provide technical support and funds to states to provide administrative support to the initiative.

"Natural disasters cost this country too much in dollars, infrastructure loss, and emotional and community well-being," said Witt. "We are putting an end to the damage, repair, damage and repair cycle. Project Impact is changing the way America deals with disasters."

The following listings show the new Project Impact communities by region.❖

(Courtesy of FEMA.)

Region I

Milford, Connecticut
Portland, Maine
Quincy, Massachusetts
Plymouth Township, New Hampshire
Holderness Township, New Hampshire
Salem, New Hampshire
Pawtucket, Rhode Island
Two River-Ottauquechee Regional Planning Commission (includes most of Orange County, North Windsor County, and the towns of Pittsfield, Hancock, and Granville), Vermont

Region II

Buffalo, New York
Rahway, New Jersey
St. Croix, U.S. Virgin Islands

Region III

Union Township, Mifflin County, Pennsylvania
Milford, Delaware
Virginia Beach, Virginia
Tri-County Council of Southern Maryland: Calvert, Charles, and St. Mary's Counties, Maryland
Cabell County, West Virginia

Region IV

Mobile County with Dauphin Island, and Bayou La Batre, Alabama
City of Birmingham/Jefferson County, Alabama
Boone, North Carolina
Charleston County, South Carolina
Jackson, Tennessee
Madison County, Tennessee
Lexington, Kentucky
Fayette County, Kentucky
Pensacola, Florida
Escambia County, Florida
Madison, Mississippi

Region V

Ottawa County, Michigan
South Bend, Indiana
St. Joseph County, Indiana
Urbana, Illinois
Burnsville, Minnesota
Colerain Township in Hamilton County, Ohio
Racine County, Wisconsin

Region VI

Miami, Oklahoma
Arkadelphia, Arkansas
Carlsbad, New Mexico
Mandeville, Louisiana

Regional VII

St. Joseph, Missouri
Neosho, Missouri
Piedmont, Missouri
Maryville, Missouri
Des Moines, Iowa
Cherokee, Iowa
Superior, Nebraska
Johnson County, Kansas
Kinsley, Kansas

Region VIII

Clear Creek County, Colorado
Morgan County, Colorado
Flathead County, Montana
Natrona County, Wyoming
Valley City, North Dakota
Huron, South Dakota
Salt Lake City, Utah

Region IX

Las Vegas, Nevada
Yuma, Arizona
San Bernadino County, California
Napa County, California
Berkeley, California
Maui County, Hawaii

Region X

Multnomah County, Oregon
Walla Walla County, Washington
Kenai Peninsula Borough, Alaska
Kamiah, Idaho
Lewis County, Idaho

Joint Task Force on Computer Network Defense Now Operational

The Department of Defense (DOD) officially stood up its Joint Task Force on Computer Network Defense (JTF-CND) on December 30, 1998, under the command of Air Force Maj. Gen. John H. Campbell. Secretary of Defense William S. Cohen approved the formation of the joint task force on December 4, 1998.

Working in conjunction with the unified military commands, the military services, and other Department of Defense agencies, the joint task force will be responsible for the defense of DOD networks and systems from intruders and other attacks.

The JTF-CND will serve as the focal point within the DOD to organize a united effort to defend its computer networks and systems. It will monitor incidents and potential threats to DOD systems; it will also establish links with other Federal agencies through the National Infrastructure Protection Center (NIPC) to share information on activities across the information infrastructure. When attacks are detected, the JTF will be responsible for directing DOD-wide recovery actions to stop or contain damage and restore network functions to DOD operations.

Defense exercises and real world events in 1997 and in early 1998 demonstrated the need for an organization within the Department to coordinate its defensive activities and to have the authority to direct the necessary actions for that defense. Cohen directed the creation of a joint task force to provide the necessary operational authority consistent with accepted joint doctrine.

The JTF-CND will report through the Chairman of the Joint Chiefs of Staff to Secretary Cohen, since the joint task force is not currently assigned to a unified command. The JTF-CND will be located at and supported by the Defense Information Systems Agency (DISA) to take full advantage of the existing operational computer network capabilities of DISA's Global Operations and Security Center, the military services, and DOD agencies.❖

(From a DOD release.)

Deputy Commerce Secretary Announces Consortium of Private Sector Coordinators for Critical Infrastructure Protection of the Communications and Information Sector

By Sallianne Fortunato
National Telecommunications and Information Agency

WASHINGTON, D.C. — Deputy Secretary of Commerce Robert Mallett on February 25, 1999, announced the creation of a consortium to serve as the private sector coordinators to work with the Commerce Department in developing a plan to protect the Nation's critical infrastructure as part of President Clinton's Critical Infrastructure Protection (CIP) Program.

The President's program identified eight critical infrastructures including communications and information, transportation, energy, banking and financial services, public health services, water supply, government services, and oil and gas delivery systems.

The Sector Coordinators for the communications and information sector will be a consortium of three key trade associations. Those three associations are the Information Technology Association of America (ITAA), headed by Harris Miller; the Telecommunications Industry Association (TIA), led by Matthew J. Flanigan; and the United States Telephone Association (USTA), chaired by Roy Neel.

Other private sector industry groups will participate in the program, to help achieve the widest effective representation for the protection of the information infrastructure.

"The vulnerabilities of the Nation to attacks on our critical infrastructures had gone largely unrecognized until the groundbreaking work of the President's Commission," said Deputy Secretary Robert Mallett. "The President has set in motion the governmental machinery to protect these infrastructures that will establish effective partnerships with industry in order to fully meet the national goals of infrastructure protection."

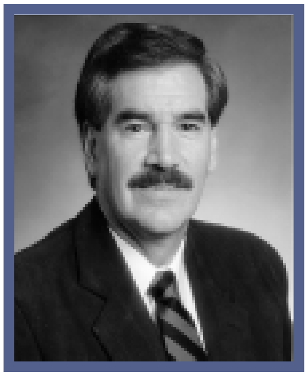
The Sector Coordinators will work with the National Telecommunications and Information Administration (NTIA) in the Commerce Department in developing plans for protecting the communications and information sector. Critical infrastructures are those physical and cyber-based systems essential to the basic functioning of the economy and Government. The Government/industry partnership will help raise the level of awareness concerning the threats we face as a Nation, as well as the vulnerabilities to be managed.

The President assigned the Department of Commerce as lead agency with responsibility for the communications and information infrastructure. Secretary of Commerce William M. Daley designated NTIA to carry out these responsibilities. Larry Irving, Assistant Secretary for Communications and Information and Administrator of NTIA, will serve as the Sector Liaison Official to work with the communications and information sector. For additional information on the CIP, please contact Irwin Pikus, Director, Communications and Information Infrastructure Assurance Program (CIIAP), at NTIA, 202-482-1116.

The President's goal is to achieve a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for Government systems by the year 2000.❖

(Courtesy of NTIA Public Affairs.)

Harris Miller



Matthew J. Flanigan

Roy Neel

The Sector Coordinators will work with NTIA and other lead agencies to:

- **Provide public and private sector perspectives relating to national infrastructure assurance objectives and strategies;**
- **Promote infrastructure assurance education and training, and advocate the use of the best practices within the communications and information sector;**
- **Coordinate international infrastructure protection issues with the State Department to develop a strategy and framework for cooperation on critical infrastructure protection with friendly, like-minded countries, international organizations, and multinational corporations; and**
- **Identify research and development (R&D) needs, and incorporate those findings into a national infrastructure R&D program.**

Telecommunications Assistance, cont'd from page 1

emergency services and reestablish telecommunications," said Navy Commander Lynne Hicks, who monitored emergency telecommunications from the NCC on May 5. She said AT&T and MCI-WorldCom reported no network outages in the affected areas, but that AT&T did move a mobile call center into Oklahoma City for locals to make outbound phone calls.

The NCC kept track of telecommunications concerns through press reports, through coordination with industry representatives both at the NCC and in the two states, and through monitoring radio transmissions from both states via the Shared Resources (SHARES) High Frequency Network.

President Clinton declared the tornado sites as Federal disaster areas on May 4, with FEMA activating its emergency support team that same day. Along with FEMA logistics, operations, information, and planning elements, FEMA activated teams that handled:

- Emergency Support Function (ESF) #3 (Public Works),
- ESF #6 (Mass Care),
- ESF #8 (Public Health and Medical Services), and
- Department of Defense issues.

Other Federal agencies and ESF teams monitored the tornado recovery situation from their respective operations centers.❖

James Witt, Director of FEMA, greets a woman at a shelter with her family after the Oklahoma tornado destroyed their home. She was among the hundreds of tornado victims which the FEMA emergency support team assisted. (Photo by Mannie Garcia, FEMA)

PSN Security Primer Now Available

By Art Schoenwetter
Customer Service and Information Assurance Division, OMNCS

The Office of the Manager, National Communications System (OMNCS) recently issued a report, *"Public Switched Network Best Practices Security Primer,"* to increase the awareness of the importance of Public Switched Network (PSN) security.

The report contains security guidelines and recommendations that constitute a basis for sound practices within the PSN. The creation of this document resulted from growing concern over the security of PSN communications, given the interdependencies of the Nation's infrastructures. These concerns are rooted in the realization that new markets and business opportunities, coupled with legislation on telecommunications reform, will bring new players into the telecommunications arena who may lack the experience and awareness needed to secure the network.

In order to secure the PSN, service providers need to know what to secure, how to secure it, what needs to be considered up front, what needs to be done on an ongoing basis, and a number of other vital factors. These factors form the basis of this report.

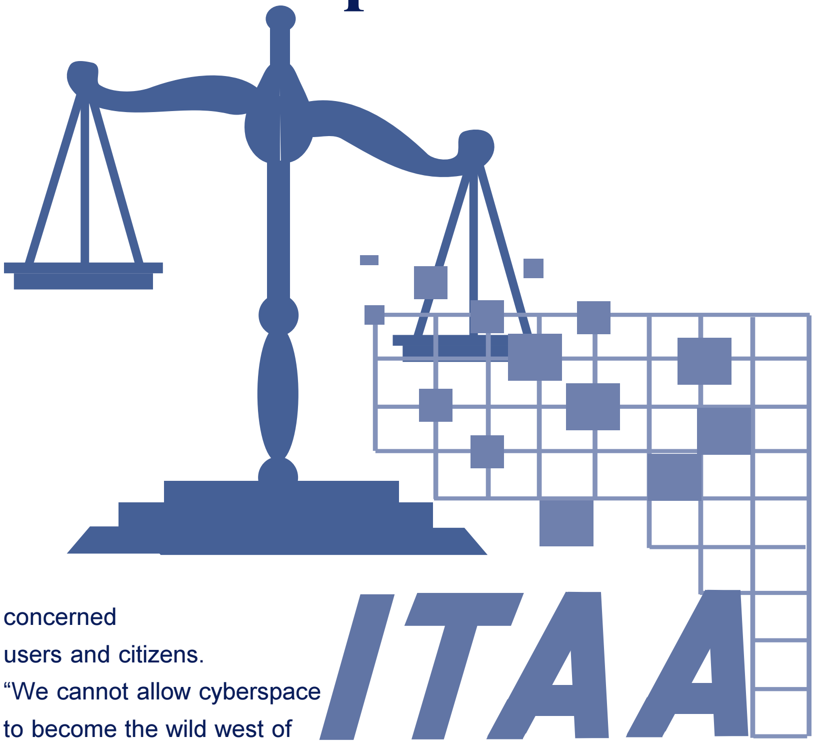
As this report is based entirely on open source information, readers may distribute it widely within their organizations. The report is available from the Office of the Manager, National Communications System.❖

The creation of this document resulted from growing concern over the security of PSN communications, given the interdependencies of the Nation’s infrastructures.

Public Switched Network Best Practices Security Primer

Table of Contents

Justice Department, ITAA Announce Cybercitizen Partnership



The Information Technology Association of America (ITAA) and the Department of Justice (DOJ) announced on March 15 the Cybercitizen Partnership—a new alliance between the high-tech industry and the U.S. Government. It is designed to promote computer ethics and civic responsibility in the cyber age.

The partnership also aims to aid law enforcement and industry in the battle against a new breed of criminal—the online outlaw. ITAA President Harris Miller, Attorney General Janet Reno, and several high-tech Chief Executive Officers (CEOs) who support the plan announced the new program at a press conference.

Officials at the Justice Department and ITAA said that computer crime is a growing problem worldwide, increasing concern that new information-based assets must be protected and preserved. A recent survey by the Computer Security Institute estimates that more than 60 percent of companies have experienced financial losses due to cyber crime. The proliferation of low-cost computers and networks have spread information technology to every quarter of society.

The partnership will conduct a major national campaign to educate, raise awareness, and provide resources to empower concerned users and citizens. “We cannot allow cyberspace to become the wild west of the information age,” said Attorney General Janet Reno. “If we are to ensure public safety and responsible computer use, then Government, industry, and the public must all work together. This Cybercitizen Partnership is an exciting beginning.”

ITAA President Harris Miller agreed: “I predict we will see cyber crime proliferate in the very near future if we as an industry, working with Government, do not take every necessary step to educate computer users on the consequences of irresponsible cyber behavior."

Miller said there is simply no greater priority than protecting what has rapidly become the bricks and mortar of this country’s economic well-being—our information technology infrastructure—from falling victim to cyber criminals and delinquents. “We are delighted to play a leadership role in critical infrastructure protection by collaborating with the Justice Department on the Cybercitizen Partnership,” said Miller.

One ITAA member company, Computer Sciences Corporation (CSC), has taken a leadership role within ITAA to actively address cyber concerns and is representative of many of the members.

“As a provider of IT solutions for Government and industry, we have a firsthand view of the growing potential for cyber crime and the need to protect our country’s technology infrastructure,” said Van

Van Honeycutt

> “As a provider of IT solutions for Government and industry, we have a firsthand view of the growing potential for cybercrime and the need to protect our country’s technology infrastructure.”

Honeycutt, CSC’s Chairman, President, and CEO. “Government and the private sector can always accomplish more by working together on challenging issues such as this.”

Honeycutt, who is also Chair of the President’s National Security Telecommunications Advisory Committee (NSTAC), said CSC is proud to be the first company to contribute to the private sector fund for the Cybercitizen Partnership. “We encourage others within the IT and telecommunications industries to do their part to ensure the future safety of our society,” he said.

The partnership as it is currently conceived will consist of three complementary segments. The first segment is a “good cybercitizenship” public awareness campaign designed to engage children, young adults, and the wider user community on the basics of critical information protection and security, and the limits of acceptable online behavior. The goal of the campaign is to foster responsible cybercitizenship, educate the public on how to protect cyber resources, and decrease the likelihood of attacks through a heightened level of civic preparedness.

A second component is a user-friendly computer and network security directory to help public and private sector organizations quickly find the computer security resources they need to protect information assets.

Finally, an Information Security Professional fellowship program between industry and Government will raise the awareness levels of participants with respect to the views, perspectives, and needs of their respective counterparts.

Knowledge and experience will be gained that will help shape the development and enhance the utility of potential information products to be shared within and between Government and industry.

ITAA consists of 11,000 direct and affiliate members throughout the U.S. which produce products and services in the IT industry. The association plays a leading role in public policy issues of concern to the IT industry, including taxes and finance policy, intellectual property, critical infrastructure protection, telecommunications law, encryption, securities litigation reform, and human resources policy.

ITAA members range from the smallest IT start ups to industry leaders in the software, services, systems integration, telecommunications, Internet, and computer consulting fields. ITAA also serves as one of three Information and Communications (I&C) Sector Coordinators under President Clinton’s Presidential Decision Directive 63.

Those wishing to learn more about ITAA and its positions on the issues may connect its Web site at http://www.itaa.org. For more information about the Department of Justice’s computer crimes and intellectual property section, check out its Web site at http://www.usdoj.gov/criminal/cybercrime/ccips.html.❖

(Originally released by ITAA; edited for NCS release.)

1999 is 'Year of Testing' Y2K Solutions, Hamre Says

"I would like to take this opportunity to state unequivocally that our nuclear command and control system has been thoroughly tested and has performed superbly."

By Jim Garamone
American Forces Press Service

Deputy Defense Secretary John Hamre told lawmakers that 1999 is “the year of testing” and that the Department of Defense (DOD) has made excellent progress in ensuring the department is year 2000 (Y2K) compliant.

Hamre testified before the House Government Reform Committee March 2. He forecasted that 93 percent of DOD’s computer systems would be Y2K compliant by March 31, the Office of Management and Budget deadline.

He said computer systems involved with nuclear weapon command and control are already compliant. “I would like to take this opportunity to state unequivocally that our nuclear command and control system has been thoroughly tested and has performed superbly,” he said. “We will continue to test and evaluate our systems involved with this most important function as our highest priority.”

Hamre said the Y2K problem, or millennium bug as it is also known, is particularly critical to DOD because of the department’s reliance on computers. “These are not simply weapon systems, the category best-prepared for the year 2000, but command and control systems, satellite systems, the Global Positioning System, highly specialized inventory management and transportation management systems, medical equipment, and important systems for payment and personnel records.”

DOD has about 9,900 computer systems with about 2,300 deemed mission critical. “DOD also operates over 600 military bases, which are like small towns, where the infrastructure is also vulnerable to year 2000 problems,” Hamre said.

DOD assigned responsibility for fixing Y2K problems to the defense leaders and warfighting commands. This high-level oversight has given added impetus to the program, he said.

While 7 percent of DOD computers will not be compliant by the March 31 deadline, DOD will continue working to make them compliant by the end of the year. He said those systems are receiving an “exceptional measure of management focus and oversight.”

Hamre is briefed each month on systems that will miss the deadline. "Systems that continue to slip may have development and fielding efforts frozen, particularly if [they] are intended to replace an already compliant system," he said.

The focus of effort this year will be on complex, real-world, end-to-end testing of DOD business functions and warfighter missions, Hamre said.

"During 1999, we will test everything from paying service members to exercising vital command and control capabilities from 'sensor to shooter,'" he said. These tests include the "skein" of systems that must operate together to perform a mission or function. He called the Y2K testing the largest and most comprehensive evaluation plan in DOD history.

Hamre said testing in this manner is as complex as going to war. It involves all areas of DOD, and, he said, the testing would increase in scope and complexity as the year goes on.

All regional commander-in-chief exercises conducted this year will include Y2K play. "We are using the department's warfighters, the commanders-in-chief, to evaluate operational readiness to conduct operations unaffected by the Y2K problem," Hamre said. The department has scheduled 31 commander-in-chief operational evaluations—six more than required by the 1999 Defense Authorization Act.

The DOD Inspector General will oversee the tests and the General Accounting Office and the Office of Management and Budget will review the results. Hamre said DOD has already conducted three tests, and he called such evaluations "essential to providing the additional assurance that our systems will remain operational over the millennium date change."

Yet even with all these tests, there will probably be Y2K impacts on DOD. Hamre said the department is working on contingency plans in case Y2K problems crop up. The Chairman of the Joint Chiefs of Staff and the regional commanders-in-chief are working through the Universal Joint Task List to ensure operations can continue if Y2K problems occur and they are putting workarounds in place that will allow commanders to accomplish their missions.

Finally, DOD is working with other U.S. Government agencies. "DOD must be able to assure operational readiness to react to challenges to U.S. national security, while at the same time assisting the Nation in such a fashion as may be necessary to negate disruptions to the domestic infrastructure," Hamre said.

DOD is sponsoring Exercise Positive Response Y2K, a series of command post exercises that will run through September. The premise of the exercises is how DOD and the country react when multiple Y2K-related failures occur.

"The concept is to remove mission-critical systems and capabilities from play during the conduct of a robust warfighting scenario and then assess DOD's ability to respond with timely decisions," Hamre said. "In addition, the exercises possess the ability of the services to execute operational contingency plans and to mitigate problems associated with Y2K."

Other Y2K DOD actions include:

- Sharing DOD's expertise with other Federal agencies. For example, DOD Health Affairs has already done Y2K testing on biomedical equipment. Officials are sharing test results with the Department of Veterans Affairs, the National Institutes of Health, Indian Health Service, and others.

- The National Guard will conduct a communications test under Y2K conditions. Success is defined as the Guard being able to talk to all 54 States, territories, and the District of Columbia simultaneously.

- DOD is working closely with the ministries of defense in Great Britain, Canada, and Mexico. The United States is also working on the Y2K problem within NATO and with Pacific Rim allies.

- DOD is working with Russia on Y2K threat reduction plans.

There are no Federal plans to call up the National Guard or other reserve components.❖

DSS Expansion Broadens Federal IT Security Choices

By Philip Bulman
National Institute of Standards and Technology
Public Affairs

Upon a favorable recommendation from the National Institute of Standards and Technologies (NIST), the Secretary of Commerce has expanded the Digital Signature Standard (DSS), clearing the way for Federal agencies to choose from a broader field of computer security products.

Digital signatures confirm the identity of the signer and verify that electronic information has not been altered. They are gaining wide use in electronic commerce transactions.

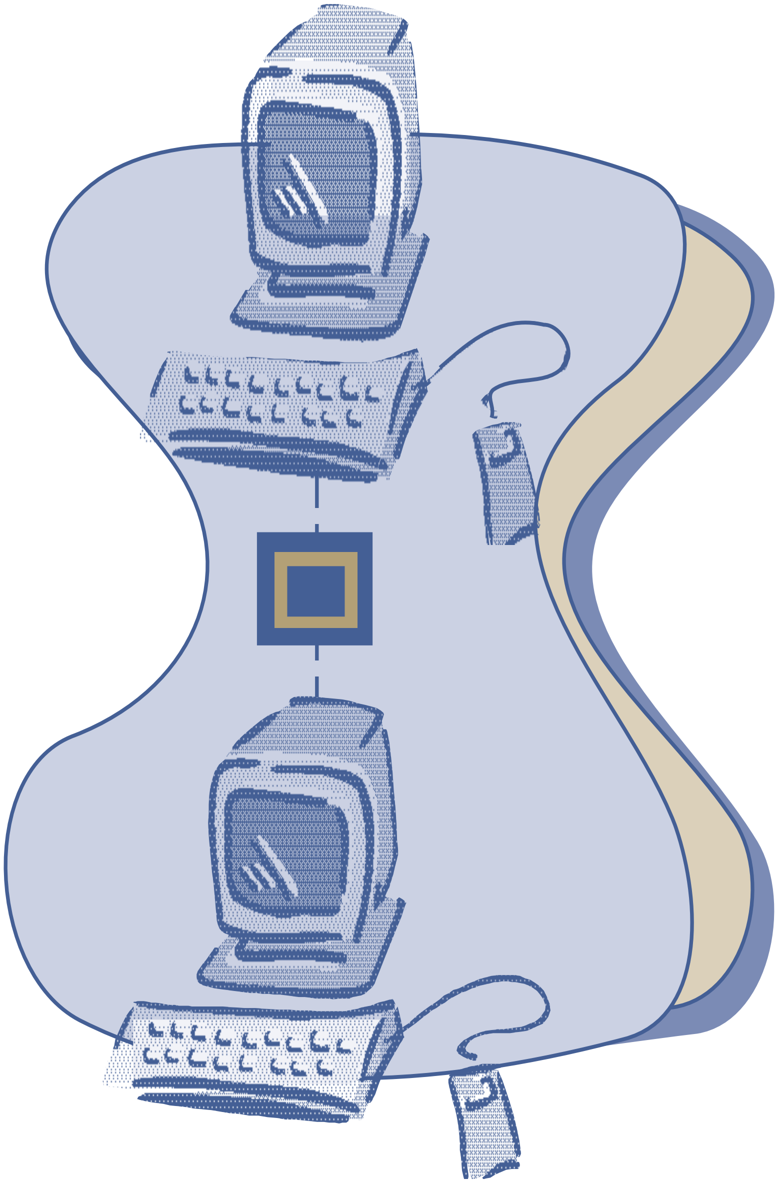
The DSS was approved in 1994. It specified the use of a single technique for generating signatures using the Digital Signature Algorithm. Mathematical formulas called algorithms are at the heart of computerized encryption systems and various other computer security products.

In 1997, NIST announced that it was considering revising the standard to allow for other algorithms in generating digital signatures. The notice specifically mentioned the possibility of adding RSA and elliptic curve techniques for generating signatures, and asked for public comments. These comments overwhelmingly supported a revision.

The revised Federal standard allows for the RSA technique. This follows the recent approval of an RSA standard (X9.31) by the private-sector American National Standards Institute (ANSI). ANSI is expected to approve a standard based on the elliptic curve technique in the future.

The revision of the Federal standard will greatly increase the number of off-the-shelf digital signature products that Federal agencies can buy.

NIST, in a recent Federal Register notice, asked for public comments on the revised standard, which is formally known as Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard.



The public may send comments to the Information Technology Laboratory, Attn: DSS/X9.31 Comments, NIST, 100 Bureau Drive, Stop 8970, Gaithersburg, Maryland, 20899-8970. Comments may be sent electronically to FIPS186RSA@nist.gov. Specifications of the FIPS 186-1 are available electronically at http://csrc.nist.gov/fips/.❖

(Courtesy of NIST Public Affairs.)