National Security and Emergency Preparedness

Telecom News

1999, Issue 3

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

Ms. Diann L. McCoy Selected as Deputy Manager, National Communications System

Ms. Diann L. McCoy, formerly the Defense Information Systems Agency's (DISA)'s Deputy Director for the Command, Control, Communications, Computers and Intelligence Program Integration Directorate, was selected on November 5, 1999, as the ninth Deputy Manager of the National Communications System (NCS).

Ms. McCoy replaces Ms. D. Diane Fountaine, who served as the NCS Deputy Manager from July 1995 to October 1999. Ms. Fountaine has accepted a position with the International Year 2000 Cooperation Center in Washington, D.C.

The NCS consists of 23 Federal member departments and agencies and is responsible for ensuring the availability of a viable national security and emergency preparedness (NS/EP) telecommunications infrastructure. President John F. Kennedy signed a Presidential Memorandum on August 21, 1963, which established the NCS to "provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crisis, including nuclear attack."

Ms. Diann L. McCoy

Ms. D. Diane Fountaine

The NCS Deputy Manager is responsible for the day-to-day policy, technical, and programmatic oversight in coordination with all Federal Government-wide activities in national security and emergency preparedness communications.

While at DISA, Ms. McCoy was responsible for managing the development and fielding of DISA's major pillar programs, including the Global Command and Control System, Global Combat Support System, Defense Information System Network, Defense Message System, Information Assurance, and Electronic Commerce/Electronic Data Interchange. Previous to those responsibilities, she was DISA's Deputy Commander for the Center for Computer Systems Engineering, Joint Information

See Ms. Diann McCoy, page 2

TABLE OF CONTENTS

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

Ms. Diann McCoy, cont'd from page 1

and Engineering Organization.

She began her Government service career in August 1971 as a trainee in the Directorate of Materiel Management at Wright-Patterson Air Force Base, Ohio.

Ms. McCoy became a member of the Senior Executive Service in June 1989, and has held leadership positions with the Directorate of Materiel Management at the Sacramento Air Logistics Center, located at McClellan Air Force Base, California; the Joint Logistics Systems Center, at Wright-Patterson Air Force Base; and the Command, Control, Communications, and Intelligence Acquisition Oversight office for the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. She has served as the Deputy to the Commander of the International Logistics Center at Wright-Patterson Air Force Base and the Director of the Standard Systems Center at Maxwell Air Force Base, Gunter Annex, Alabama.

Ms. McCoy has a Bachelor of Science degree in Mathematics and Computer Science from Wright State University and a Master of Science degree in Logistics Management from the Air Force Institute of Technology. She is also a graduate of the Massachusetts Institute of Technology Senior Executive Program.

Ms. McCoy's awards include the Presidential Distinguished Executive Rank Award, the DOD Distinguished Civilian Service Award, the Meritorious Civilian Service Award, the Presidential Rank of Meritorious Executive Award, and the Certified Professional Logistician from the Society of Logistics Engineers.❖

Manager Says Information Assurance is Key to Warfighter, DOD Business Enterprise Success

By Stephen Barrett, Customer Service Division, OMNCS

Lieutenant General David J. Kelley, Manager of the National Communications System (NCS), told members of the President's National Security Telecommunications Advisory Committee (NSTAC) that information assurance is the key to success in serving both the warfighter and the Department of Defense (DOD) business enterprise in today's highly interconnected and shared risk environment.

Speaking at NSTAC's June 10, 1999, Business Session, held at the U.S. State Department's Loy Henderson Auditorium, LTG Kelley provided an overview of security risks to DOD networks and information assurance activities. He noted that the number of reported incidents on DOD unclassified networks had increased steadily during the first 5 months of 1999. He attributed the increase to a number of factors, including a heightened

Lieutenant General David Kelley, Manager, NCS, said information assurance is the key to success in serving both the warfighter and the DOD business enterprise in today's highly interconnected and shared risk environment. (Photo by Robert Flores, DISA)

awareness of intrusion incidents, improved monitoring tools, and trained personnel.

The Manager then said that the Internet age is creating an environment in which information is freely and easily disseminated, creating potential security risks within the national security and emergency preparedness (NS/EP) community. After providing an example of open source intelligence gathered from the Internet, LTG Kelley demonstrated how aggregation of such information could help an adversary identify a target or determine the nature of a military operation. He emphasized that DOD reviewed the content of its various Web sites and removed information that might make DOD assets vulnerable.

The Manager then highlighted DOD's approach for ensuring the protection of information. DOD examines security at all levels—from the end user through the network. He specifically cited the National Coordinating Center for Telecommunications (NCC), which provides the conduit for sharing information between Government and the telecommunications industry.

In its future role as an Information Sharing and Analysis Center, LTG Kelley said the NCC will facilitate information sharing among the Defense Information Systems Agency (DISA), the Joint Task Force-Computer Network Defense (JTF-CND), and the National Information Protection Center (NIPC). As the year 2000 arrives, he indicated that the NCC would receive incident reports from DISA posts around the world, beginning with the DISA Information Technology Center in Guam.

Besides speaking on information assurance issues, the Manager also briefed the NSTAC Principals on the Defense Information Systems Network (DISN), a key resource in enabling worldwide communications for the warfighter in the battlefield and within the DOD enterprise. LTG Kelley said the DISN is designed to provide secure communications throughout the DOD and will be fully implemented by 2010.

The Manager added that DISN utilizes the most sophisticated telecommunications technology available, much of which is provided by NSTAC member companies, and adapts that technology to meet the needs of the warfighter. He emphasized that while the use of terrestrial-based communications continues to grow, communications via space are becoming increasingly vital to reach deployed service members.

In concluding his remarks, LTG Kelley emphasized the importance of developing interoperable, secure telecommunications solutions that meet the needs of the warfighter in a joint service environment—including input from the services, coalition partners, and industry. He commented that NSTAC would serve as a vital resource to the Nation as those challenges are addressed.

To emphasize one of DOD's important challenges, LTG Kelley introduced retired Air Force Lieutenant General Albert Edmonds—the former Manager, NCS, and currently Chief Operating Officer of Electronic Data System's Government Industry Group. Edmonds discussed ways in which the Government—and DOD

See Information Assurance is Key, page 4

Information Assurance is Key, cont'd from page 3

in particular—uses electronic commerce initiatives to improve business operations and assist the service members in the field.

Edmonds opened by emphasizing that a strong public/private partnership is necessary to ensure the success of those electronic initiatives. He then discussed current electronic initiatives within DOD, including:

Computer Sciences Corporation Chairman, President, and CEO Van Honeycutt, (left) holds some early morning conversation with Air Force Maj. Gen. John Campbell, Commander of the Joint Task Force for Computer Network Defense during the Executive Breakfast at the NSTAC meeting held June 9, 1999. Honeycutt serves as the NSTAC chair. Campbell is also the Vice Director of DISA. (Photo by Robert Flores, DISA)

P Electronic Document Access—electronic access to documents in support of the contract process through a secure Web-based server. This initiative streamlines the contracting process and increases access to Government contracting documents;

P Central Contractor Registration—a centralized Government trading partner database. This provides a single interface to industry, establishes common business practices, and expedites contract awards;

P Electronic Commerce Processing Node—a single interface between the Government and private sector trading partners. This again establishes a single interface to industry and provides end-to-end accountability; and

P Wide Area Workflow—support of electronic receipt, storage, and retrieval of documents that support electronic procurement. This allows for the elimination of paper-based systems and ensures global accessibility and secure transactions.

Edmonds emphasized that building confidence in the process would be the key enabler of success for each of those initiatives. He said that while DOD was confident in the security of its classified networks, steps needed to be taken to ensure that the unclassified systems on which those electronic initiatives would operate were robust and secure.

To attain that assurance, Edmonds said Government needs to find trusted commercial off-the-shelf products, implement trusted processes to secure the unclassified networks, and ultimately, establish a public key infrastructure (PKI). He noted that while the technology needed to establish a PKI is in place, a strong public-private partnership is also needed to ensure public confidence in the PKI.

Next on the agenda was Air Force Major General

John Campbell; DISA's Vice Director and Commander of DOD's JTF-CND. Collocated with DISA's Global Network Operations and Security Center (GNOSC), and working in conjunction with the unified military commands, services, and agencies, the JTF-CND coordinates and directs the defense of DOD computer systems and networks.

Maj. Gen. Campbell said that to fulfill its responsibilities, the JTF-CND is engaged in a wide range of operations. These operations include monitoring DOD computer networks via its military service components and DISA's GNOSC; directing actions to defend the Defense Information Infrastructure (DII) from intrusions; and assessing the operational impact of intrusions into the DII.

In addition, Maj. Gen. Campbell detailed JTF-CND's important role in coordinating the defense of DOD networks with non-DOD Government agencies and appropriate private organizations. In particular, he stated that the JTF-CND's cooperative information sharing agreements with the NIPC and the NCC were especially critical to the JTF-CND's ability to accomplish its operational and strategic goals.

In summarizing the factors that led to the JTF-CND's creation, Maj. Gen. Campbell noted that JTF-CND's formation was consistent with DOD's realization that information superiority—the capability to collect, process, exploit, and disseminate an uninterrupted flow of information, and to deny the enemy's ability to do the same—was key to the success of the United States military in the next century. He said that several events—including the exercise Eligible Receiver (June 1997) and the attack known as Solar Sunrise (February 1998)—had been significant in demonstrating both the DII's security vulnerabilities and the need for an organization with the authority and responsibility to direct the DII's defense.

Moreover, he said that threats to the DII in the forms of state-sponsored and terrorist attacks, industrial and foreign espionage, disgruntled employees, and hackers were expected to become more serious.

By equipping a computer network defense capability where none had previously existed, Maj. Gen. Campbell said the JTF-CND provides an effective interim solution to DOD's computer network defense problem, pending the finalization of a Unified Command Plan to address DII defense issues.

Noting the United States Space Command would assume responsibility for DOD computer network defense on October 1, 1999, Maj. Gen. Campbell said that the JTF-CND would retain its present role as DOD's single point of contact for defensive computer network operations.❖

Emergency Responders Battle Hurricane Floyd Along U.S. East Coast

As Hurricane Floyd blew into the Caribbean on September 13, 1999, all levels of emergency responders along the East Coast of the United States prepared for its landfall.

Although the hurricane had diminished to Category II (96-110 mph) status when it made landfall on September 16 near Cape Fear, North Carolina, it nevertheless created a unique situation for some Federal emergency responders.

Hurricane Floyd was unusual in that its path would eventually cross 15 states, spanning four General Services Administration (GSA) regions. Between September 16 and September 23, 10 states within these regions from Florida to Connecticut issued major disaster declarations, triggering activation of the Federal Response Plan.

The four-region disaster area of Hurricane Floyd

See Hurricane Floyd, page 6

States Issuing Disaster Declarations

Region I	-	Connecticut
Region II	-	New York, New Jersey
Region III	-	Delaware, Maryland, Pennsylvania, Virginia
Region IV	-	Florida, North Carolina, South Carolina

Hurricane Floyd, cont'd from page 5

made it necessary for GSA to undertake an unusually aggressive disaster response. Hurricane Floyd was unique in that disaster declarations affected GSA Regions I through IV.

Once the President signs a disaster declaration, the Federal Emergency Management Agency (FEMA) activates the FRP and the necessary Emergency Support Functions (ESF). As the primary agency for ESF #2 (Communications), the National Communications System (NCS) has the overall telecommunications coordination responsibilities for disaster response efforts.

To support these efforts, the NCS uses a Memorandum of Understanding with GSA's Federal Technology Service (FTS) to cover the dispatch of a Federal Emergency Communications Coordinator (FECC) to a disaster site.

In situations like Hurricane Floyd, where the deployment of additional FECC's is required, the

See Hurricane Floyd, page 8

FECC Deployment

Name	Region	Deployment Location
Mike Wade	1	North Carolina Emergency Operations Center (EOC), Raleigh, North Carolina
Leon Meiskin	2	FEMA Region II Regional Operations Center (ROC), New Jersey
Juan Ortiz	2	Caribbean (standby)
Robert Tausek	3	South Carolina EOC, Columbia, South Carolina
John Penman	4	FEMA Region IV ROC Atlanta, Georgia; SC EC
Daniel Smith	5	FEMA Region IV ROC
Russ Colomo	7	North Carolina EOC
Edwin Vest	8	Florida EOC (Tallahassee); FEMA Region IV EOC
Leroy Gallegos	9	Georgia EOC
Art McLemore	10	North Carolina EOC

Scenes from Hurricane Floyd

Sea surge preceding the arrival of Hurricane Floyd damages this and other structures at Holden Beach, located south of Wilmington, North Carolina. (Photo by Dave Gatley, FEMA)

New Jersey Port Authority Police search through home basements to ensure residents were not trapped in their homes during flooding caused by Hurricane Floyd. (Photo by Andrea Booher, FEMA)

Members of the Raritan (New Jersey) First Aid Squad assist a Bound Brook, New Jersey, resident following flooding caused by Hurricane Floyd. (Photo by Andrea Booher, FEMA)

Hurricane Floyd, cont'd from page 7

FTS Office of Information Security (OIS), under the direction of Tom Burke, has the responsibility for coordinating the dispatching of additional FECC's to the disaster sites.

During the response to Hurricane Floyd, Tom Sellers from the OIS's National Security and Emergency PreparednessBranch (and the NCS Council of Representatives member from GSA) coordinated the additional response efforts with the affected regions. Sellers worked with the Manager of the National Coordinating Center for Telecommunications(NCC), and FEMA to ensure that personnel were deployed to the required Emergency Operations Centers (EOC) in a timely manner.

With Floyd impacting most of the East Coast, FECC's were dispatched from areas as far away as Region IX (San Francisco) and Region X (Seattle) for a deployment period of approximately 10 days. Under the direction of the NCC and FTS, the FECC's role was to deploy to the scene as the principal Federal telecommunications coordinator in the disaster area. Floyd's impact on the East Coast required that the other Regional FECC's leave their normal jobs, travel on very short notice, and then work at least 12 hours a day, 7 days a week for the duration.

The FECC's worked with FEMA communications personnel to quickly establish telecommunications services for the disaster field office. The FECC's also served as the primary interface between the Government departments and agencies and the telecommunications industry for response coordination and setting of restoration priorities.

Representatives from numerous Federal agencies prepare for Hurricane Floyd support at the FEMA Regional Operations Center in Atlanta. (Photo by Andrea Booher, FEMA)

In addition, the FECC's maintained critical interface capabilities between FEMA and other organizations that were providing emergency support. They also furnished situation reports to update telecommunications activities in the disaster area.

The response to Hurricane Floyd once again demonstrated that the cooperative efforts of GSA and NCS enable emergency responders to fulfill their assignments expeditiously, and provide critical telecommunications resources to Federal, State, and local Governments, which enable post-disaster recovery to begin.❖

With the image of Hurricane Floyd behind them, President Clinton and FEMA Director James Lee Witt discuss plans to provide support to communities impacted by the storm. (FEMA photo)

Hamre Provides NSTAC DOD Perspectives on Y2K, Technology Challenges

By Stephen Barrett
Customer Service Division, OMNCS

Deputy Secretary of Defense John Hamre told members of the President's National Security Telecommunications Advisory Committee (NSTAC) that the computers and systems of the Department of Defense (DOD) are prepared for the Year 2000 (Y2K) and the Department has no doubts regarding its ability to defend the United States during the transition to the new millennium.

Hamre's remarks came during the Business Session of the NSTAC XXII meeting held June 10, 1999, at the U.S. State Department's Loy Henderson Auditorium. Hamre told the Business Session audience that 98 percent of DOD mission-critical systems were fixed and certified through independent testing, and that only 40 mission-critical systems (out of a total of 2,100) remained to be tested and certified.

He said DOD would focus its remediation efforts on fixing those systems before the end of the year and added that 85 percent of the Department's 4,000 non-mission-critical systems have been fixed and certified.

The Deputy Defense Secretary was quick to credit Air Force General Richard Myers, the Commander-in-Chief of the U.S. Space Command, for the success in testing critical systems. "General Myers and SPACECOM really took the lead in this," he said. "They were the first ones to demonstrate what it took. They did a series of exercises, all the way from the early-warning radars to the command centers, to the processing centers, to the President, to the forces in the field in a string of communications 30 and 40 deep, to find out where we would have a problem."

Hamre said the Defense Department was "pleasantly surprised" that the fixes and the testing that have been done largely proved that they worked. "We have a couple of little problems," he said, "but they have demonstrated that there's no question that we'll be able to defend America on the 1st of January, on the 2nd of January, on the 29th of February, and all those other days [after]."

Detailing DOD's Y2K priorities, Hamre noted that

See Hamre Provides Perspectives, page 10

Deputy Defense Secretary John Hamre told members of NSTAC that the Government needs NSTAC assistance in addressing the technological challenges of designing interoperable security solutions, as well as ways to embed security in the information technology infrastructure. Hamre's request came during the NSTAC XXII Business Session, held June 10, 1999, at the U.S. State Department in Washington. (Photo by Robert Flores, DISA)

Hamre Provides Perspectives, cont'd from page 9

because Y2K remediation for DOD systems is nearly complete, the emphasis is shifting to forces deployed overseas and their dependence on host country infrastructure readiness. "For example, all the countries in Asia that have been struggling with very significant economic problems all of a sudden have to tackle the Year 2000 problem and it is quite a challenge," said Hamre.

Although the Y2K problem will not affect DOD's ability to wage war abroad, Hamre expressed concerns about quality of life issues for the troops and their family members overseas. He explained that DOD was working with host countries on Y2K preparedness issues, including DOD augmentation of host country resources, where needed, and the development of Y2K contingency plans. He added that the regional Commanders-in-Chief are working with host governments and conducting a survey to find out whether we need to pre-position assets for the rollover.

Next, Hamre briefly discussed the need for open dialogue between industry and Government in the current era of dynamic technological change. He told the audience that the Government needs NSTAC assistance in addressing the technological challenges of designing interoperable security solutions and ways to embed security in the information technology infrastructure. He emphasized that a strong partnership between industry and Government was vital in finding solutions to those challenges.

"I know that a lot of you are rather wary about this encryption issue," said Hamre. "I'm not asking you to get into the debate as it relates to privacy or to law enforcement issues. Rather, we need you to tackle the much deeper, more complicated problem of how we embed security 'in depth' in the infrastructure upon which we the Government depend and upon which you and your customers depend."

In response to an NSTAC Principal's comment, Hamre agreed that the United States does not have a monopoly on the development of encryption technologies. He asserted that the key to the Nation's encryption policy is to achieve a balance so that markets are not closed to U.S. firms, but national security interests are protected. Hamre stated that he believed that a compromise could be reached between national security interests and those of multinational corporations based in the United States.

With regard to the transition to Y2K, Hamre was asked whether there were any indications that groups might exploit potential deficiencies in the infrastructure resulting from Y2K. Hamre explained that there were no identifiable state-sponsored groups seeking to exploit the Y2K problem and damage DOD information systems, and added that detection capabilities were in place for all DOD networks.

Hamre concluded his remarks by thanking the NSTAC member companies for their commitment and dedication to serving the Nation and for continuing to provide advice and expertise to the Administration on issues vital to the Nation's national security policies.❖

IES Recaps Accomplishments during NSTAC XXII Meeting

By Stephen Barrett, Customer Service Division, OMNCS

Guy Copeland, Computer Sciences Corporation's representative to the Industry Executive Subcommittee (IES) of the President's National Security Telecommunications Advisory Committee (NSTAC) recapped IES accomplishments to the audience at the NSTAC Business Session on June 10, 1999, at the U.S. State Department.

Copeland, who serves as the IES Working Session Chair, addressed the accomplishments of the IES during the 9-month NSTAC XXII cycle, concentrating on four issue areas. Each of those areas —infrastructure protection, network security, legislative and regulatory topics, and industry/ Government coordination and response—addressed national security and emergency preparedness (NS/EP) issues.

Infrastructure Protection

Copeland first reviewed the subcommittee's work in the area of infrastructure protection. Noting NSTAC's 17 years of successful industry/Government partnership and experience in joint planning for the telecommunications infrastructure, Copeland said the committee is uniquely qualified to share best practices and lessons learned with Government officials responsible for implementing Presidential Decision Directive (PDD) 63, "Protecting America's Critical Infrastructures."

Because of this experience, Copeland said the IES—at the request of the Critical Infrastructure Assurance Office (CIAO)—reviewed the contents of the draft National Plan for Information Systems Protection and provided comments on the plan to the CIAO.

Copeland stated that the IES had completed a Transportation Information Infrastructure Workshop, held March 3 and 4, 1999, in conjunction with the Department of Transportation. He said the workshop was well received by transportation officials from the public and private sectors.

The 2-day workshop also facilitated completion of the IES' Transportation Information Infrastructure Risk Assessment—the third and final risk assessment conducted by the NSTAC. Copeland said the assessment was carried out based on a Presidential request to NSTAC to examine the information-based risks to infrastructures identified as having strong interdependencies and a growing reliance on telecommunications and information systems.

NSTAC completed risk assessments for the financial services and electric power industries in previous work cycles.

The transportation risk assessment revealed that several industry-wide factors—including the globalization of transportation companies, the intermodal transport of goods and services, and increased reliance on information technology —are increasing the vulnerability of the transportation infrastructure to the large-scale effects from information system outages. The IES concluded that the industry could benefit from future Transportation Department-sponsored conferences and the timely dissemination of Government information on physical and cyber threats to the transportation infrastructure.

Copeland said the IES also completed its investigation of the national security and emergency preparedness (NS/EP) implications of electronic commerce (EC) use in the Federal Government and how EC could affect business operations and security processes within the NS/EP community. He reported that while the IES found that the NS/EP community's use of and dependence on EC is still modest, it will grow steadily, therefore heightening the need for a coordinated focus to address NS/EP requirements.

Toward that end, the IES recommended that the President, in accordance with Executive Order (E.O.) 12472, "Assignment of National Security and Emergency Preparedness Functions," designate a focal point to examine the NS/EP issues related to the widespread adoption of EC.

Copeland explained that on the basis of previous NSTAC findings, the IES also believes that the Global Information Infrastructure (GII) will present significant new opportunities, as well as vulnerabilities, for NS/EP communications in the future. Therefore, the IES began a study to postulate the GII for 2010, focusing on airborne and space-based communications systems, land-based communications systems, and emerging applications and protocols.

Copeland concluded the review of the current cycle's infrastructure protection activities by stating that at Attorney General Janet Reno's request, the IES facilitated a partnership between the Department of Justice (DOJ) and several industry associations called the "Cyber Citizen" Program.

Copeland said that during the next NSTAC cycle, the IES plans to work with DOJ to sponsor a round table between senior industry and Government officials to

See IES Recaps, page 12

discuss cyber security policy issues. He also stated that the IES plans to continue the ongoing projects that he had highlighted.

Network Security

Copeland discussed the subcommittee's network security projects, focusing first on its study of the NS/EP community's use of the Internet. He explained that due to concerns about the Internet's reliability and security, the NS/EP community's direct dependence on the Internet is limited to outreach, information sharing, and e-mail, while dedicated TCP/IP networks, or Intranets, are used for mission-critical functions. However, Copeland cautioned that the interconnected nature of TCP/IP networks could result in the disruption of service to those Intranets should the Internet infrastructure experience difficulties.

He also noted that the study concluded that NS/EP dependence on the Internet is expected to grow over the next several years as the Government continues to explore efficient ways of doing business.

Therefore, the NSTAC recommended that, in accordance with E.O. 12472, the President establish a permanent program within the Federal Government to address NS/EP needs specific to the Internet. In addition, the NSTAC recommended that the President direct the appropriate Government departments and agencies to use existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

Copeland then turned to other network security initiatives, including the Research and Development (R&D) Exchange Symposium, which addressed the growing convergence within the telecommunications industry and ways to improve collaboration among Government, industry, and academia. He reported that the NSTAC Network Security Information Exchange (NSIE) continued to meet with the Government NSIE. The two NSIE groups had produced two key documents—the After-Action Report on the Insider Threat Workshop and the 1999 Assessment of the Risk to the Security of the Public Network.

The latter report built upon a similar risk assessment completed in 1995 and identified three factors that have significantly affected the public network's vulnerability since then: the Telecommunications Act of 1996, the Year 2000 technology problem, and the changing business practices within industry.

Copeland then stated that the IES planned to conduct another R&D Exchange Symposium to continue to foster information exchange among industry, Government, and academia on network security R&D. The symposium would also examine the allocation of network security resources with respect to current operations and R&D initiatives and examine how

Guy Copeland, Working Group Chair for the NSTAC Industry Executive Subcommittee, briefs NSTAC Principals and others attending the NSTAC XXII Business Session on June 9, 1999, at the State Department's Loy Henderson Auditorium. (Photo by Robert Flores, Defense Information Systems Agency.)

the convergence of the public network with IP-based networks could have an effect on NS/EP telecommunications priority services.

Legislative and Regulatory Issues

The third issue area focused on NS/EP telecommunications legislation and regulation. Copeland stated that the primary focus of that area was information sharing, and in particular, information sharing between industry and Government in response to telecommunications outages and network intrusions. As a first step toward examining this problem, Copeland said the IES developed a report that illustrates the current and proposed information sharing process between industry and Government.

Based on comments by John Koskinen (Chair of the President's Council on Y2K Conversion) at last year's NSTAC meeting, Copeland said the NSTAC sent a letter to the President in September 1998 asking him to urge the Congress to quickly pass the Y2K Information Readiness and Disclosure Act. The Act was signed into law on October 19, 1998, and in January 1999, the IES conducted a survey of NSTAC companies on the success of the act. The survey results were shared with the President's Council on Y2K Conversion.

With regard to the NSTAC's next steps in the area of legislation and regulation, Copeland said the subcommittee planned to continue to examine options for eliminating barriers to information sharing. The subcommittee would also examine the definition of foreign ownership within the telecommunications industry and how it affects NS/EP communications, and continue to monitor the regulatory environment surrounding network convergence for any impact on NS/EP communications.

Government/Industry Coordination

Copeland discussed the NSTAC's work examining issues related to Government/industry coordination and response. He said the IES had worked closely with the National Coordinating Center for Telecommunications (NCC) to develop guidelines and reporting criteria for the NCC's new indications, assessment, and warning function. He added that the IES had begun assessing participation in the NCC in an effort to determine if additional entities are needed to help fulfill the NCC's expanded mission.

The IES report illustrates the current and proposed information sharing process between industry and Government.

Copeland also expressed NSTAC's support of the development of a memorandum of understanding between the Manager, National Communications System, and the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, formally establishing the NCC as an Information Sharing and Analysis Center for the telecommunications infrastructure.

Finally, Copeland discussed NSTAC's efforts to coordinate Y2K outreach and contingency planning by sponsoring a series of meetings with industry and Government entities responsible for Y2K preparedness. He explained that those meetings facilitated discussions that ensured that NS/EP aspects of the Y2K technology problem were being addressed.

Specific topics that were examined included the development of an international Y2K early warning system for telecommunications, and the domestic and international roles of the NCC as a national coordinating body for response to Y2K telecommunications events. Based on the study of the Y2K problem, the NSTAC recommended that the Federal Government take the necessary steps to ensure the timely dissemination of meaningful and accurate Y2K planning information to State and local governments, which will enhance the flow of information to the general public and community groups.

Copeland then recognized the group chairs and once again thanked the industry and Government participants who contributed to NSTAC's work during the NSTAC XXII cycle.❖

Cohen Listens, Answers Questions on NSTAC Concerns

Secretary of Defense William Cohen (left) answers questions by members of the President's National Security Telecommunications Advisory Committee (NSTAC) during the committee's Executive Session June 10, 1999. Listening to Cohen's response is Computer Sciences Corporation Chairman Van Honeycutt (far right), who chairs the NSTAC. Committee members and senior Government officials discussed issues dealing with critical infrastructure protection and the Year 2000 technology problem. Government officials attending included Richard Clarke, the President's National Coordinator for Security, Infrastructure Protection, and Counter-terrorism; Michael Powell, Defense Commissioner of the Federal Communications Commission; and Dr. Neal Lane, Assistant to the President for Science and Technology.❖

(Photo by Robert Flores, Defense Information Systems Agency.)

President Names AT&T's Armstrong as New NSTAC Member

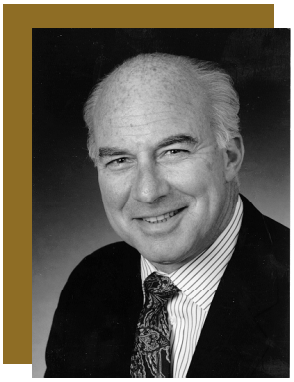
On September 17, 1999, President Clinton announced his intent to appoint C. Michael Armstrong of AT&T as a member of the President's National Security Telecommunications Advisory Committee.

Armstrong was appointed Chairman of the Board and Chief Executive Officer of AT&T in November of 1997. He was previously at Hughes Electronics, where he had been Chairman and CEO for 6 years. Prior to his tenure at Hughes Electronics, Armstrong was with IBM for more than 3 decades. He began as a systems engineer and ended as Chairman of the Board of IBM World Trade Corporation.

Armstrong received his Bachelor of Science degree in Business and Economics from Miami University of Ohio and completed the advanced management curriculum at Dartmouth Institute. He was awarded an honorary Doctor of Law degree from Pepperdine University.

The President's National Security Telecommunications Advisory Committee (NSTAC) provides the President with technical information and advice on national security telecommunications policy.❖

(Courtesy of the White House Press Office.)



C. Michael Armstrong, Chairman and CEO of AT&T, was named to the President's National Security Telecommunications Advisory Committee on September 17, 1999. (Photo courtesy of AT&T.)

President Renews NSTAC Through 2001

By Stephen Barrett, Customer Service Division, OMNCS

The President's National Security Telecommunications Advisory Committee (NSTAC) will continue its role of advising the President on matters regarding national security and emergency preparedness (NS/EP) telecommunications for at least two more years.

President Clinton signed an Executive Order (E.O.) on September 30, 1999, extending NSTAC's role to September 30, 2001. NSTAC was one of 16 committees, councils, commissions, and boards retained by the White House to advise the President under the provisions of the Federal Advisory Committee Act.

Seventeen years ago, President Reagan created the NSTAC by E.O. 12382 to advise him on matters regarding NS/EP telecommunications.

The NSTAC is composed of up to 30 Presidentially appointed industry leaders—usually chief executive officers. In its advisory role to the President, the NSTAC provides industry-based analyses and recommendations on a wide range of policy and technical issues related to information assurance telecommunications, infrastructure protection, and other NS/EP concerns.

Four issues provided impetus for the establishment of the NSTAC: divestiture of AT&T; increased Government reliance on commercial communications; potential impact of new technologies on NS/EP telecommunications; and growing importance of command, control, and communications to military and disaster response modernization.

Van Honeycutt, President, Chairman and Chief Executive Officer of Computer Sciences Corporation, is NSTAC's current Chair. Solomon Trujillo, President and Chief Executive Officer of U S WEST, is nominated to become the NSTAC Vice Chair, pending White House approval.❖

ITAA Awarded Funding for Cybercitizen Partnership

By Tinabeth Burton, Information Technology Association of America

On September 29, 1999, the Information Technology Association of America (ITAA) announced it has entered into a Cooperative Agreement with the Department of Justice (DOJ) and has been awarded $300,000 to support the Cybercitizen Partnership.

This alliance is between the high tech industry represented by ITAA and the U.S. Government, and dedicated to promoting computer ethics and civic responsibility in the cyber age. The cooperative agreement will support the development of a major national public awareness campaign directed at children and young adults to educate, raise awareness, and teach responsible, lawful online behavior.

More funding from ITAA member companies and non-member sources such as foundations and vertical industries will be solicited to implement the awareness campaign, and industry and Government officials will work together to oversee the direction and message of the campaign.

"Read the headlines. Cyber crime is a growing concern of both

See ITAA Funding, page 16

industry and Government, as both are vulnerable to attacks," said Harris Miller, President of ITAA. "Industry can't afford to just sit back and watch the crime volume increase, and we believe this solution will help weed out some of the less meaningful system violations by curious children so that law enforcement can focus on the true criminals."

"This public awareness campaign should be a priority for every company—not just IT [information technology] companies—that owns an information infrastructure," Miller added. "We are delighted to play a leadership role by collaborating with the Justice Department on the Cybercitizen Partnership."

The Cybercitizen Partnership was mentioned in an August, 1999 report by the Attorney General to the Vice President of the United States on Cyberstalking. The Attorney General's report highlighted the Partnership as an "industry effort" to educate on cybercrime and boost cooperation between industry and Government, expand public awareness of computer crime issues among children and adolescents, and provide resources for Government to draw upon in addressing computer crime. The report is available at http:/www.usdoj.gov/ag/cyberstalkingreport.htm.

"Collaborative efforts like the Cybercitizen Partnership will aid law enforcement and industry in combating criminal activity in cyberspace," said Attorney General Janet Reno. "Partnering with industry will help ensure and promote safe and responsible use of computers."

One ITAA member company, Computer Sciences Corporation, has already committed funds and staff support to the Cybercitizen Partnership's public awareness campaign. The Partnership will now submit requests for proposals to public relations agencies to develop possible messages and deliverables for the campaign.

Harris Miller

"This public awareness campaign should be a priority for every company, not just information technology companies."

ITAA officials and Attorney General Reno announced the Cybercitizen Partnership at a press conference on March 15, 1999, in Washington, D.C. Another component of the partnership currently underway is a directory of information security providers scheduled for publication in October 1999 to help public and private sector organizations quickly and easily find the computer security resources they need to protect information assets.

Steps are also being taken to implement an information security professional fellowship program between industry and Government. For more information on the partnership, visit http://www.itaa.org/infosec/cyber.htm.

ITAA consists of 11,000 direct and affiliate members throughout the United States who 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 Sector Coordinators under Presidential Decision Directive 63.

Learn more about ITAA and its positions on the issues at its Web site at http://www.itaa.org.❖

Y2K Officials Say Canada, United States, Mexico are in Good Position Approaching 2000

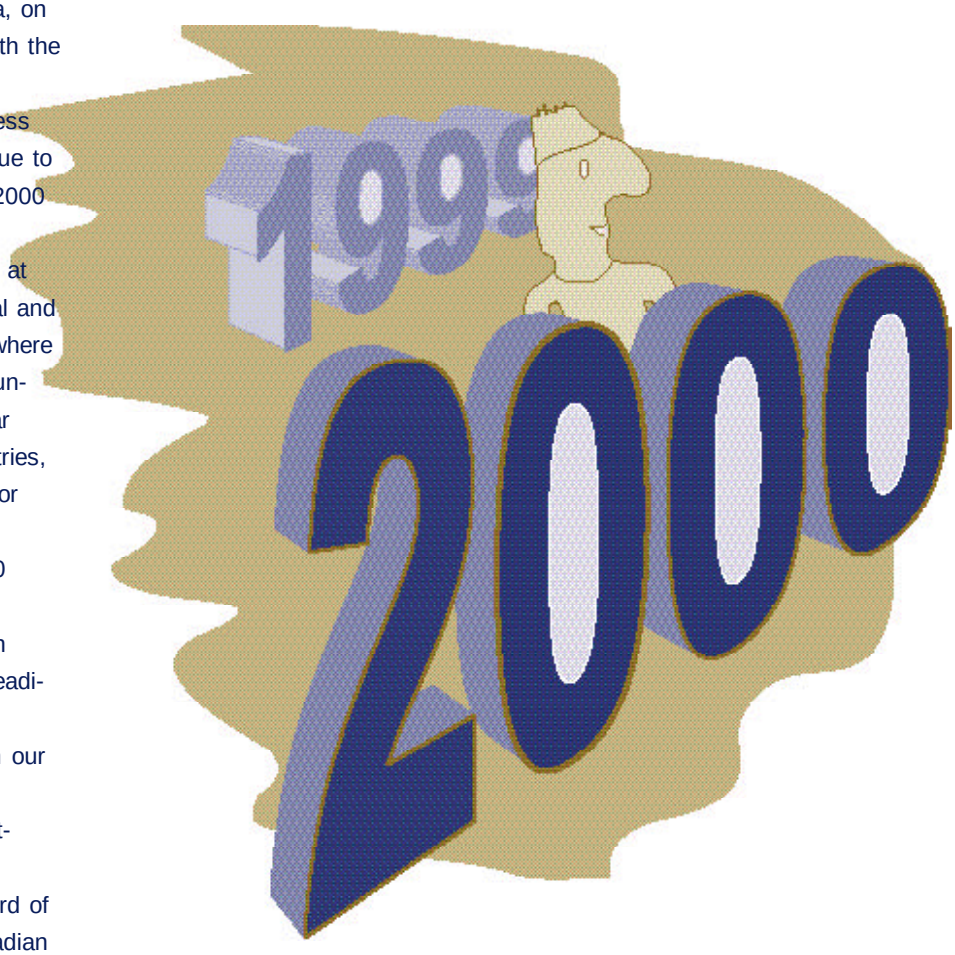
Top Year 2000 (Y2K)officials from the governments of the United State, Canada, and Mexico announced in Ottawa, Canada, on October 5 they are pleased with the progress being made in North America on Year 2000 readiness and confirmed they will continue to collaborate through the Year 2000 rollover period.

The announcement came at the end of two days of bilateral and trilateral meetings in Ottawa where delegations from the three countries discussed remaining Year 2000 challenges in their countries, including outstanding issues for cross-border cooperation and management of the Year 2000 transition period.

"Interdependencies are an important part of Year 2000 readiness. Canada has given high priority to our relationship with our NAFTA [North American Free Trade Agreement] trading partners," said V. Peter Harder, Secretary of the Treasury Board of Canada and head of the Canadian delegation. "During this most recent set of meetings, my colleagues and I have reconfirmed our commitment to work together through the Year 2000 date change to minimize any potential disruptions that could arise."

"Canada and Mexico have been leaders in meeting the Y2K challenge. As a result, we believe North America will be well-prepared for the Year 2000," said John Koskinen, Chair of the President's Council on Year 2000 Conversion and head of the American delegation. "We have all benefited from the partnership on Y2K that has developed among our respective countries and I look forward to

See Approaching 2000, page 18



DOD Conducts Largest Y2K Test Ever

By Paul Stone, American Forces Press Service

It was actually July 13, 1999. But as far as the Pentagon was concerned the date was March 4, 2000, as the Department of Defense (DOD) was wrapping up a test of the military's logistical systems in what was billed as the largest Year 2000 (Y2K) test ever conducted.

See DOD Test, page 18

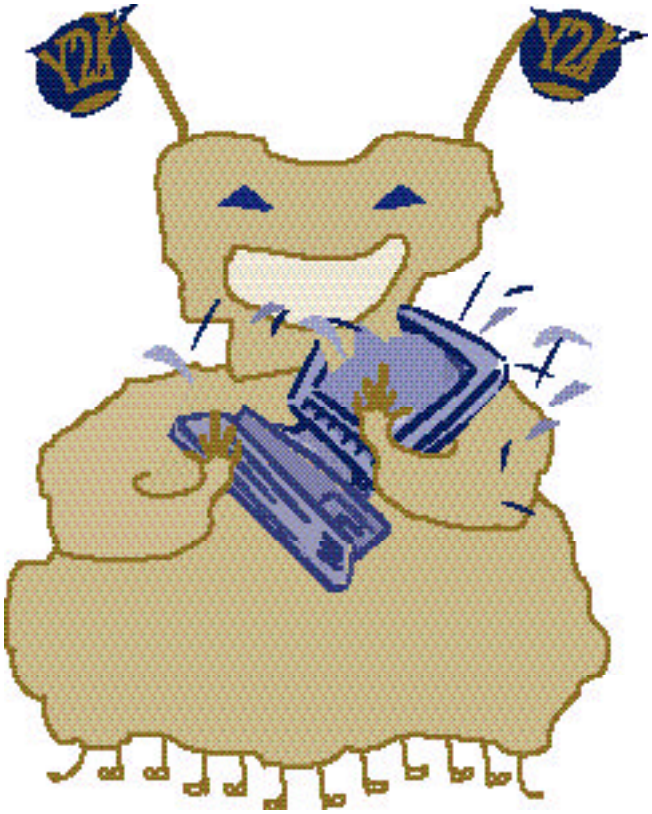
Approaching 2000, cont'd from page 17

continuing these constructive working relationships through the date rollover."

"Mexico believes that international co-operation plays a key role to minimize Y2K related risks and improve country readiness worldwide," said Norma Samaniego, Special Advisor to the Year 2000 National Conversion Commission of Mexico and head of the Mexican delegation. "This Third Trilateral Meeting between Canada, Mexico and the U.S. on Y2K cooperation issues represents one important step ahead in an effort to share experiences, take advantage of common approaches and undertake joint actions to increase the state of preparedness of the North American region."

In addition, Harder and Koskinen announced that a bilateral agreement had been reached to have Canadian observers on-site in Washington and American observers on-site in Ottawa over the Year 2000 transition period. Arrangements will be made for contact points to coordinate public communications between the two countries. Further, Ms. Samaniego and Koskinen have agreed to establish a special communications link between the United States and Mexico during the rollover period.❖

(Courtesy of the President's Council on Y2K Conversion.)



DOD Test, cont'd from page 17

The test involved more than 1,000 civilian and military personnel and DOD's 44 most critical logistics systems, spread out over 22 locations. It was designed to ensure that Year 2000 problems will not prevent delivery of supplies to troops as the millennium approaches.

The Year 2000 problem, nicknamed "Y2K" and "millennium bug," refers to a past computer industry practice of programming years with just two digits—1999 would be "99." The shorthand means some computer systems and equipment on January 1, 2000, might read "00" as "1900." The error could generate more inaccurate data and even cause systems to shut down. Systems that won't handle the year change correctly must be fixed or replaced; those that will work correctly are called "Y2K-compliant."

Test participants included the Office of the Secretary of Defense, Defense Logistics Agency, Defense Information Systems Agency, the U.S. Transportation Command, and all four services. The Joint Interoperability Test Command provided independent verification and validation of the tests.

The 44 systems tested conduct about $80 billion worth of

DOD business annually, said Zach Goldstein, DOD's Director of Logistics Information Systems. He said they process over 2.5 billion transactions—by some estimates, twice the electronic commerce conducted on the Internet by the rest of the entire country last year.

Goldstein said testing was vital because the systems support almost 2 million service members and civilian employees by processing requests for almost everything from buttons to bullets, from food to spare parts. If service members use it, shoot it, eat it, or wear it, chances are it's ordered through the complex networks of computer systems tested July 13, he said.

During the tests, technical experts built a duplicate network often referred to as a "parallel processing environment." Then they rolled their computer clocks forward to simulate the week following February 28, 2000.

February 28 through March 1, 2000, are key Y2K dates because many computer programs were not written to recognize 2000 as a leap year. DOD already successfully tested the systems for other key Y2K dates, such as the fiscal year rollover on October 1, 1999, and the millennium change itself.

Goldstein called the tests the culmination of more than 7 months of identifying problems, analyzing them, and fixing the individual systems. "Now we're seeing how the systems work together, because that's how we do military operations," he said. Analysts were watching to see whether the systems communicated correctly during the date changes and whether they produced accurate information in their final databases.

Although all results were not scheduled to be in until late July, only a few minor glitches had occurred by July 1999. In two cases, the year on some supply requests incorrectly read the year 2000 as 100, and, in another instance, a system failed to recognize February 29, 2000. Goldstein said those would be easily fixed problems. "The key is to know they exist so we can fix them now," he said.

"We feel very confident, based on what we've seen here and what we've demonstrated, that we've got a system that works and works well," said Roger Kallock, Deputy Undersecretary of Defense for Logistics. Despite all the efforts by DOD, however, Y2K still could pose some undetected minor glitches, he warned.

Y2K is a first-time problem not only for DOD, but the entire world, Kallock said. "We don't know what we don't know, so there could be some surprises down the road," he said. "I think, however, that we will be prepared to handle situations in a way that's unparalleled as result of the effort being given to Y2K."

John Koskinen, Chairman of President Clinton's Council on Year 2000 Conversion, praised the DOD effort as "the ultimate in testing" and said the results have far-reaching consequences. "The outcome for the Defense Department is that logistics services, which support American war fighters, are in fact on their way to completion, not only internally, but across all the services," Koskinen said. "Beyond that, it demonstrates no matter how large or complicated the system is, if you pay enough attention to them and do the work, you can in fact complete the (Y2K remediation) process."

DOD was scheduled to release results of the testing by the end of July.❖

President Signs Executive Order Creating National Infrastructure Assurance Council

By Stephen Barrett, Customer Service Division, OMNCS

In an effort to promote partnership between the Federal Government and the private industry that owns the Nation's critical infrastructures, President Clinton, through an Executive Order signed July 14, 1999, established the National Infrastructure Assurance Council (NIAC).

Once the President approves the nominees, the NIAC will meet periodically over the next 2 years,

See NIAC, page 20

focusing on enhancing public and private sector partnerships in protecting critical infrastructures. The Council will provide the President with reports on infrastructure protection and will propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes.

In addition, the NIAC will monitor development of Private Sector Information Sharing and Analysis Centers (PSISACs) and provide recommendations to the National Coordinator and the National Economic Council. These recommendations will determine how these organizations can best foster improved cooperation among the PSISACs, the National Infrastructure Protection Center (NIPC), and other Federal Government entities.

Although the President has not yet announced any of the NIAC members, its membership will consist of not more than 30 individuals, selected from private sector entities representing the Nation's critical infrastructures identified in Executive Order 13010, and from State and local governments. Those critical infrastructures include telecommunications, electric power, transportation, oil and gas delivery, financial services, Government services, water distribution and purification, and nuclear resources.

Although the President has not yet announced any of the NIAC members, its membership will consist of not more than 30 individuals from the private sector, representing the Nation's critical infrastructures, and from State and local governments.

The Executive Order specifies that NIAC members have expertise relevant to NIAC functions. Individuals appointed by the President will serve for 2-year terms and may serve no more than 3 consecutive terms. The President will designate a Chair and Vice Chair from among the NIAC members. NIAC members serve without compensation for their work on the Council.

Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism will serve as the Executive Director of the NIAC. Dr. Jeffrey Hunker, the Senior Director for Critical Infrastructure Protection, will serve as the NIAC's liaison to other Federal agencies.

The NIAC will report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Policy. The NIAC will also advise the lead agencies with critical infrastructure responsibilities, sector coordinators, the NIPC, the PSISACs, and the National Coordinator on the subjects of the NIAC's function in a manner to be determined by the NIAC Chair, the National Coordinator, and the senior official of the affected entities.

Subject to the availability of appropriations, the Department of Commerce, through the Critical Infrastructure Assurance Office, will provide the NIAC with administrative services, staff, and other support services. The Department of Commerce will perform these functions under the Federal Advisory Committee Act

To the extent permitted by law, the NIAC may hold open and closed hearings, conduct inquiries, and establish subcommittees as necessary to complete its business. The President ordered that all executive departments and agencies shall cooperate with the NIAC and provide assistance, information, and advice to the NIAC as it may request.

While engaged in council work, the Executive Order permits NIAC members to collect travel expenses, including per diem in lieu of subsistence. Federal law allows this payment for persons serving intermittently in the Government service or on Federal Advisory bodies.

Although chartered until July 14, 2001, the President has the authority to renew the NIAC's charter.❖