National Security and Emergency Preparedness
Telecom News
2002, Issue 1

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

NSTAC Chair Recaps Committee's Recent Accomplishments At March Meeting

By Steve Barrett
National Communications System

In his final meeting as Chair of the President's National Security Telecommunications Advisory Committee (NSTAC), Daniel P. Burnham briefed industry and Federal Government leaders that NSTAC's work over the past year was greatly influenced by the terrorist attacks in New York and Washington.

"Since our last meeting — to say much has happened somehow doesn't quite say it all," explained Mr. Burnham to the 200 attendees present at the NSTAC XXV Business Session, held March 13 in Washington. "The terrorist attacks on September 11 changed our focus on national and homeland security. It affected everybody in this room and everybody in the country. Many of our companies were drastically impacted, of course, and those who were not directly affected stepped forward nevertheless to assist in any way possible."

Mr. Burnham, Chairman and Chief Executive Officer of Raytheon Company, said the NSTAC companies played a

Daniel P. Burnham (left), Chairman and Chief Executive Officer of Raytheon Company, receives a final update from John Grimes (right), Raytheon's Vice President for Command, Control, Communications and Intelligence, Washington Operations, before opening the Executive Breakfast at the 25th meeting of the President's National Security Telecommunications Advisory Committee (NSTAC), held March 13. Mr. Burnham concluded his term as the NSTAC Chair that afternoon. (Photo by Robert Flores, Defense Information Systems Agency.)

Table Of Contents

Chair Recaps, page 5

NS/EP Telecom News is published quarterly under the auspices of Mr. Brenton Greene, 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:

Steve 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
e-mail:
telecomnews@ncs.gov

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

Executive Order Establishes the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security

By Steve Barrett
National Communications System

Soon after completion of the NSTAC XXV conference last March, President Bush issued another Homeland Security Executive Order – an order that established a new presidential advisory council that will focus on developing ways to protect the United States from terrorist threat and attack.

The Executive Order (E.O.) signed March 19, 2002, created the President's Homeland Security Advisory Council (PHSAC), which will provide advice to the President – through the Assistant to the President on Homeland Security — on developing and coordinating the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.

According to the E.O., the PHSAC will consist of not more than 21 members appointed by the President — two of which will be designated as chair and vice chair. The E.O. dictates that the appointed members of the PHSAC shall be selected from the private sector, academia, professional service associations, federally funded research and development centers, nongovernmental organizations, State and local governments, and other appropriate professions and communities.

In addition to the appointed members, the President said that the Chair and the Vice Chair of the National Infrastructure Advisory Council (NIAC); the Chair of the President's National Security Telecommunications Advisory Committee (NSTAC); and the Chair of the Panel on the Science and Technology of Combating Terrorism, President's Council of Advisors on Science and Technology, will also serve as PHSAC members.

The PHSAC role will also include recommendations on ways to improve coordination, cooperation, and communication among Federal, State, and local officials and private and other entities, as well as providing a means to collect scholarly research, technological advice, and information concerning processes and organizational management practices both inside and outside of the Federal Government.

The council also advises the President on the feasibility of implementing specific measures to "…detect, prepare for, prevent, protect against, respond to, and recover from terrorist threats or attacks within the United States; and examine the effectiveness of the implementation of specific strategies to detect, prepare for, prevent, protect against, respond to, and recover from terrorist threats or attacks within the United States."

To assist the PHSAC in its mission, the President also ordered the establishment of four Senior Advisory Committees (SAC) for Homeland Security. These four committees will focus on:

State and local officials and their roles, academia and policy research, the private sector, and Emergency Services, Law Enforcement and Public Health and Hospitals. The Assistant to the President for Homeland Security will select not more than 17 individuals for each of the committees, as well as the chair and vice chair for each. The President may establish additional groups as required.

All PHSAC members shall serve without compensation for their work on the committee, the SACs, and any subcommittees. However, members shall be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service.

The President ordered

HS Advisory Council, page 9

Seven Corporate Leaders Take Oath to Become Members of NSTAC

As Richard Clarke (second from left), the President's Special Advisor for Cyber Security looks on, Lt. Gen. Harry D. Raduege, Manager of the National Communications System, administers the oath of office to seven new members of the President's National Security Telecommunications Advisory Committee (NSTAC). Those new members are (from left to right after Clarke): Joseph P. Nacchio, former Chairman and Chief Executive Officer (CEO) of Qwest Communications; Dr. Vance D. Coffman, Chairman and CEO of Lockheed Martin Corporation; F. Duane Ackerman, Chairman and CEO of BellSouth; Herbert W. Anderson, President of Northrop Grumman Information Technology Sector; Donald J. Obert, Group Executive, Technology Solutions Group, Bank of America; Lawrence A. Weinbach, Chairman and CEO of Unisys Corporation; and Clayton M. Jones, CEO and President, Rockwell Collins. The presentations were made during the NSTAC dinner held in Washington, D.C. (Photo by Robert Flores, Defense Information Systems Agency.)

Powell asks NSTAC to Keep Nation Inside the Information Loop

By Steve Barrett
National Communications System

The Nation's top diplomat told members of the President's National Security Telecommunications Advisory Committee (NSTAC) that in order to stay ahead of this Nation's allies and adversaries, the Nation's telecommunications industry must be able to keep the country's leaders "inside the information loop."

As the concluding speaker at the NSTAC XXV Business Session held March 13 at the U.S. State Department's Loy Henderson Auditorium, Secretary of State Colin L. Powell addressed over 200 conference attendees about the importance of state-of-the-art communications in his job and to the roles of thousands of diplomats serving around the world.

"Power to me now, as Secretary of State, is to be inside everybody else's information loop and decision loop," said Secretary Powell, the highest-ranking Bush Administration official attending the NSTAC XXV conference. "I have to be able to move faster and decide quicker than my friends, allies, and potential adversaries around the world. I have to be able to move faster than all of my European colleagues, all of my Asian colleagues. I have to know information constantly coming in, is constantly being updated, it has to be accurate."

In order to meet his rapid-fire requirements around the world, Secretary Powell called on the Nation's telecommunications industry leaders to make sure that he stays inside the information loop of the people he has to deal with. He said having the ability to talk to a foreign leader anywhere in the world instantaneously has become an essential part of his life. "I had called the President of Pakistan last Friday [March 8], to talk some business. And just as I was concluding I said, "I'm sorry to hear about the deaths that occurred in Karachi today". And he said, "What deaths?" I'm inside his information loop."

Secretary of State Colin Powell told members of the President's National Security Telecommunications Advisory Committee (NSTAC) that the Nation needs their help in keeping Federal Officials "inside the information loop" to better conduct the Nation's business. Secretary Powell concluded discussions at the NSTAC XXV Business Session, held March 13 at the Department of State's Loy Henderson Auditorium. (Photo by Robert Flores, Defense Information Systems Agency.)

The Secretary of State also indicated that this requirement to be "inside the loop" not be limited to him exclusively, but to all in the State Department. "All of them have to have that same ability to stay tight in my information loop so when I call them, they already know what I'm calling about, so that we are no longer sitting there 'tap, tap, tap, teletyping,'" he said. "We've got to have faster ways of getting the information out."

Secretary Powell said some of the State Department's technology needs are becoming more important with President Bush's national push to promote, establish and maintain homeland security. He said if the country is going to start checking everybody coming in for homeland security concerns, there needs to be a method of cross referencing information from all Federal agencies to ensure identities.

"Somebody shows up at a consular's office in Lisbon and says, 'I'm so-and-so,'" said Secretary Powell. "I've got to make sure that that consular officer — that person who has been in the State Department one year — can get onto a computer and access the entire system back here in the United States … to determine whether or not this is somebody we want to come into the country. That's the kind of goal we are marching

to, and I need your help to show us how best to do that so that we can get the size pipes we need, the connectivity we need, the security we need, how to protect ourselves from exploitation."

Secretary Powell also told of his personal experience following the September 11th attacks on New York's World Trade Center and the Pentagon in Washington. "I never felt more useless in my life than on the morning of the 11th of September," said the Secretary, who was in Lima, Peru attending a conference with nations of the Organization of American States when notified of the attacks. For most of his seven-hour return flight, Powell said he couldn't talk to anybody.

"Phones [were] gone because of what happened here and what happened to the [communications] system here in Washington," he said. "They couldn't get a phone line through. I was able to get some radio communications — two radio spots on the way back — but for most of that seven-hour period, I could not tell what was going on here in my Capital, and I'm the Secretary of State! Those are the kinds of challenges we face."

The Secretary thanked the members of NSTAC for the work they are doing and encouraged them to continue their support because they are serving "a noble purpose" that is in the interest of the American people. He encouraged the NSTAC Principals to continue finding ways to provide better and faster ways of communicating so that the Nation's elected and appointed leaders, diplomats and defense forces have "…everything they need to do the job that they need to do in the front line of diplomacy." v

As Air Force Lieutenant General Harry D. Raduege, Jr., Manager of the National Communications System, reviews the agenda, NSTAC Chair Daniel P. Burnham opens the Business Session for the 25th meeting of the President's National Security Telecommunications Advisory Committee (NSTAC). The meeting was held March 13 in Washington. (Photo by Robert Flores, Defense Information Systems Agency.)

Chair Recaps, continued from page 1

critical role in supporting America's response to the terrorist attacks. "The initiatives of the NSTAC companies were significant factors, we believe — and I think you believe — in the early restoral of telecommunication services," he said. This included the successful and quick reopening of Wall Street just days after the attack. "The extraordinary involvement by our member companies in the NCC [National Coordinating Center for Telecommunications] operations and in the [September 11] lessons learned analysis of industry's emergency response … was a significant part of the work of NSTAC and all of the people here during this cycle."

As a follow-up to supporting the recovery efforts, Mr. Burnham said the White House requested NSTAC members establish an "ad hoc" group in coordination with the Federal Government to address lessons learned and share its views. He said a major point in the group's report was what the Chair called the increased coordination between industry and Government — highlighting a growing interdependence of the Nation's critical infrastructures. In particular, Mr. Burnham noted that many of the Nation's other critical infrastructures are highly dependent on the telecommunications industry to accomplish their missions.

In response to the White House, the NSTAC Chair said the ad hoc group identified some recommendations and follow-up actions that were forwarded in a letter to President Bush. The letter discussed such issues as how industry was denied access to the disaster site by law enforcement, causing a delay in service restoration. "Verizon, for example, encountered significant delays simply getting to their own facilities in New York City because of this," said Mr. Burnham. He then said NSTAC recommended some kind of standard

Chair Recaps, page 6

The Department of State's Loy Henderson Auditorium was the site of the 25th meeting of the President's National Security Telecommunications Advisory Committee (NSTAC). Over 200 people attended the Business Session, bringing corporate industry executives and Federal leaders to discuss telecommunications issues affecting national security and critical infrastructure protection. (Photo by Robert Flores, Defense Information Systems Agency.)

Chair Recaps, continued from page 5

access control procedure to be established across Federal, State and local government jurisdiction at the disaster sites.

He also noted how wireless and cell phone services, so essential obviously to emergency responders and support activities, were disrupted due to the congestion in the public network. "This experience highlighted the need for wireless priority service capability, an idea that the committee originally recommended in 1995," said Mr. Burnham.

The Chair also took time to praise the NCC and its Telecommunications Information Sharing and Analysis Center for its effectiveness and ability to react quickly to the emergency. The NSTAC Chair said the NCC effectively coordinated real-time industry and Government operational responses during and after the tragedy, specifically citing the NCC's work with the Federal Communications Commission and the White House Office of Science and Technology Policy in "...expediting regulatory and prioritization approval for industry service providers."

Other Taskings

In addition to reacting to September 11 requirements, the NSTAC was also asked to comment on the pervasive vulnerabilities uncovered in the Simple Network Management Protocol, what is referred to as SNMP. "The implication of the SNMP vulnerabilities, if exploited, could have significant ramifications for the nation's critical infrastructure and other computer network processes," said Mr. Burnham. He reminded attendees that SNMP provides the management or the handshake of, for, and between networks, and that NSTAC is working closely with the Government on this critical concern.

Although the events of September 11 absorbed a great deal of NSTAC's efforts, the committee also accomplished taskings assigned during the previous NSTAC conference held in June 2001. Mr. Burnham said areas examined over the past cycle included telecommunications recommendations for the national strategy on critical infrastructure protection, network security and convergence, and "last mile" bandwidth availability.

At the request of Mr. Richard Clarke, the President's Special Advisor for Cyberspace Security, Burnham said NSTAC worked with the Department of Commerce's information and communications sector coordinators to develop the national strategy for the protection of the critical telecommunications and information infrastructure. "Our recommendations for the strategy were reflected in our information-sharing analysis and dissemination report which we sent to the President," he said. "We recommended a national level capability to disseminate cyber attack warnings and information-sharing analysis processes between industry and Government."

The Chair also noted that over the past 20 years, NSTAC has been focused on sharing critical information

and advice with the Government. "The first recommendation of this committee in 1982 …resulted in the creation of the National Coordinating Center for Telecommunications," which Mr. Burnham said is a mechanism for sharing critical information and coordinating emergency responses between the industry and government. "Now, the outstanding industry-Government cooperation and emergency support during the September 11 events is a direct result of this 20-year relationship," he said.

Mr. Burnham then addressed convergence issues, saying that the committee examined the potential for widespread outages in the Nation's networks resulting from distributed denial of service attacks, and the convergence of telephony and Internet network services. "The work on network security and convergence over several cycles led to the White House Office of Science and Technology Policy request that we take a look at the potential for widespread network outages," he said. "Our research and exercises indicated that a widespread outage is unlikely at this time." However, the NSTAC Chair cautioned that industry remains concerned about the potential for widespread outage, especially in converged or

> "Now, the outstanding industry-Government cooperation and emergency support during the September 11 events is a direct result of this 20-year relationship,"

The final tasking from NSTAC XXIV was a request from the Manager, National Communications System, to address providing high bandwidth services in the "last mile" for NS/EP requirements in a timely manner. Mr. Burnham said the NSTAC examined the economic and technological factors impacting the provisioning of these services and what policy-based solutions are available for improvement. "Specific recommendations on how Government and industry could reduce provisioning time or to mitigate the effects of provisioning periods were identified," he said. "These recommendations were in three categories — to improve contracting and practices within the Government, for the Government to think about and establish realistic requirements for its own specific needs, and then to better forecast to industry the future broadband services." Mr. Burnham said some of these issues are already being addressed and improvements are being made. "Our findings identified numerous factors that impacted the provisioning of critical services to NS/EP users," he said, "and provided recommendations to the President for improving the availability of the last mile and requirements of the Government."

Chair Recaps, page 16

President Creates Homeland Security Advisory System

By Linda D. Kozaryn
American Forces Press Service

Federal, state, and local authorities, law enforcement agents, and the American people, need to know about terrorist threats as quickly as possible.

To ensure that happens, President Bush signed a directive creating the Homeland Security Advisory System. White House officials say the system is the foundation for building an effective communications structure.

Part of a series of initiatives to improve coordination and communication in the fight against terrorism, the advisory system would provide a national framework for Federal, state, and local governments, and private industry, allowing officials to communicate the nature and degree of terrorist threats.

HS Advisory System, page 8

HS Advisory System, continued from page 7

Government officials would determine if a threat is credible and whether it has been corroborated. They'd also determine the gravity of the threat and whether it is specific and imminent.

Government officials would also characterize levels of vigilance, preparedness and readiness in a series of graduated threat conditions.

These threat conditions would help Federal, state and local government officials, law enforcement agents and citizens decide what action they could take to help counter and respond to terrorist activity.

Based on the threat level, federal agencies would then implement protective measures that the government and the private sector would take to reduce vulnerabilities. States and localities would be encouraged to adopt compatible systems.

The advisory system would also include public announcements of threat advisories and alerts and inform people about government steps to counter the threat. The announcements would also provide information to help people respond to the threat.

Heightened threat conditions could be declared for the entire nation, for a specific geographic area, or for a functional or industrial sector, White House officials said. Officials would use a color-coded system: conditions green, blue, yellow, orange and red.

Condition Green would indicate a low threat of terrorist attack. Government and law enforcement authorities would refine and exercise protective measure plans and regularly assess facilities for vulnerabilities and taking steps to reduce them.

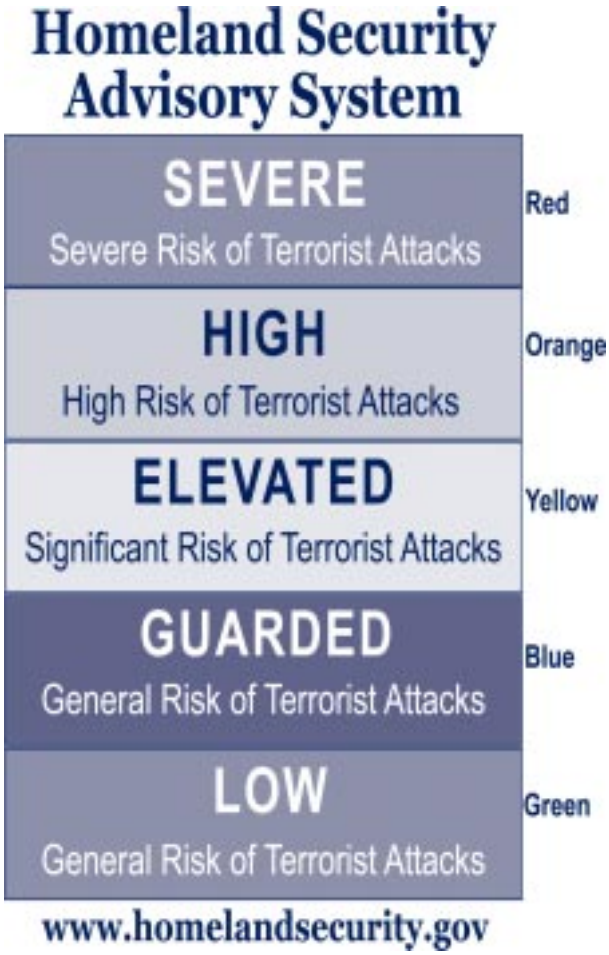
Condition Blue would indicate a general risk of terrorist attack. Among other precautions, authorities would check communications with emergency response and command locations. They would also review and update emergency response procedures and provide the public with necessary information.

Condition Yellow would indicate significant risk of terrorist attacks. Protective measures would include increasing surveillance of critical locations; coordinating emergency plans with nearby jurisdictions and implementing contingency and emergency response plans, as appropriate.

Condition Orange would indicate a high risk of terrorist attacks. Authorities would coordinate security efforts with armed forces or law enforcement agencies and prepare to work at an alternate site or with a dispersed work force and restrict access to essential personnel only. Additional precaution would be taken at public events.

Condition Red would indicate severe risk of terrorist attacks. In this case, emergency response personnel would be assigned and specially trained teams would be pre-positioned. Authorities would monitor, redirect or constrain transportation systems, close public and government facilities and increase or redirect personnel to address critical emergency needs.

The President has given the Attorney General responsibility for developing, implementing and managing the Homeland Security Advisory System. Government and law enforcement officials and the public had 45 days to comment on the plan. Ninety days later, in coordination with the Office of Homeland Security, the Attorney General will present a system to the President for approval. v



Tom Ridge, the President's Director for Homeland Security, discusses details of the new Homeland Security Advisory System. (White House photo.)

HS Advisory Council, continued from page 3

that heads of Executive Departments and Agencies provide the PHSAC with homeland security information on their agencies upon the council's request. He also indicated that the PHSAC would have a government official as Executive Director, who would be appointed by the Assistant to the President for Homeland Security. Unless the Executive Order is extended by the President, the PHSAC, its subordinate SACs, and all subcommittees will conclude work on March 19, 2004.

E.O. 13231 Follow Up

The new Executive Order follows up on an E.O. the President signed last October: E.O. 13231, "Critical Infrastructure Protection in the Information Age." Executive Order 13231 highlights the President's efforts to "ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."

The E.O. established the Presidential Critical Infrastructure Protection (CIP) Board to coordinate and have cognizance of Federal efforts and programs that relate to protecting information systems. The NCS Manager — currently Lt Gen Harry D. Raduege, Jr. — has a seat on that board and serves with other senior government officials from the Executive Branch and other Federal agencies. In addition, the Manager is also a member of Board's Coordination Committee.

Section 11 of E.O. 13231 specifically contains language about the NCS and its critical role. President Bush said that changes in technology are causing the convergence of much of telephony, data relay, and Internet communications networks into an interconnected network of networks. "The NCS and its National Coordinating Center for Telecommunications shall support use of telephony, converged information, voice networks, and next generation networks for emergency preparedness and national security communications functions assigned to them in Executive Order 12472," said the President.

"All authorities and assignments of responsibilities to departments and agencies in that order, including the role of the Manager of NCS, remain unchanged except as explicitly modified by this order."

"All authorities and assignments of responsibilities to departments and agencies in that order, including the role of the Manager of NCS, remain unchanged except as explicitly modified by this order."

One key role the NCS plays under E.O. 13231 is chairing one of the CIP Board's standing committees – the Committee for National Security and Emergency Preparedness Communications (NS/EPC). The NS/EPC — formerly the NCS Committee of Principals — consists of Government telecommunications executives representing 22 Federal agencies. The NS/EPC, in addition to its responsibilities to the NCS in accordance with E.O. 12472 shall report fully and regularly on the activities of the NS/EPC to the President's Critical Infrastructure Protection Board.

The Board will also work with Presidential Advisory Panels — comprised of senior experts from outside of Government that advise the President. This includes the President's National Security Telecommunications Advisory Committee (NSTAC), a 30-member advisory committee that provides advice to the President on the security and continuity of communications systems essential for national security and emergency preparedness established by E.O. 12382. Administrative and staff support for NSTAC comes from the National Communications System. v

Eberhart Tabbed to Head United States Northern Command

By Gerry J. Gilmore
American Forces Press Service

The commander of the U.S. military's space and continental air defense assets has been chosen to lead the nation's premier military homeland defense organization.

Air Force Gen. Ralph E. Eberhart has been nominated by President Bush to command the soon-to-be established U.S. Northern Command, Defense Secretary Donald H. Rumsfeld said today in a Pentagon news briefing. The nomination requires U.S. Senate confirmation, DoD officials noted.

Northern Command will take the homeland security missions being performed by various combatant commanders and put them under a single command, Air Force Gen. Richard B. Myers, chairman of the Joint Chiefs of Staff, noted April 18 at a Pentagon press briefing.

The new organization is slated for activation October 1, at Peterson Air Force Base, Colorado Springs, CO., as part of changes to DoD's Unified Command Plan announced April 17.

Eberhart currently wears three hats as the commander in chief of both U.S. Space Command and the North American Aerospace Defense Command and as Defense Department manager for Space Transportation Systems Contingency Support, all at Peterson. He has served as head of Space Command since February 22, 2000.

Gen. Ralph E. Eberhart, USAF

A command pilot, Eberhart flew 300 combat missions in Vietnam. Other assignments during his career include tours as Air Force Vice Chief of Staff; Commander, Air Force Air Combat Command, Langley Air Force Base, VA.; and Commander of the 5th Air Force, Yokota Air Base, Japan. He is a 1968 graduate of the U.S. Air Force Academy, Colorado Springs, CO.

NCS IMAs Support 2002 Winter Olympics

By Lieutenant Colonel Eugene Bonos
U.S. Army Reserve Individual Mobilization Augmentee
(IMA) National Communications System

From February 8 through 24, fans of sport from all over the world focused their attention to the 2002 Salt Lake City Winter Olympic Games. Military, civilian and contractor members of the National Communications System (NCS) team were there behind the scenes to provide support and the means for response personnel to communicate in the

National Communications System Individual Mobilization Augmentees staffed Federal Emergency Management Agency's emergency communications center at Camp Williams, Utah, in support of the Olympic Winter Games last February. The NCS military contingent consisted of LTC Eugene Bonos (Region III – Mid-Atlantic), COL Elizabeth Lippmann (Capital Region), COL Anne Walsh (Capital Region), Lieutenant COL Craig Knapp (Region IX-Pacific Rim) and LTC Steve Mainger (Region X – Northwest/Arctic). All five are Army Reserve officers. (Photo courtesy of NCS IMA Office.)

event of an emergency. Fortunately, there were no emergencies or incidents that made it necessary to progress from readiness to action.

Unlike deploying on short notice to respond following a natural disaster, planning NCS support for the 2002 Winter Olympic Games began a year in advance. Planners from the NCS worked with the Federal Emergency Management Agency (FEMA) to define the mission and the concept of operations.

The FEMA plan was to establish an operations center in the vicinity of Salt Lake City. This Olympic Watch Operations Center would become a Disaster Field Office (DFO) in the event of a natural or man-made disaster. Camp Williams, an installation of the Utah Army National Guard located south of Salt Lake City, was selected as the ideal location with facilities, space and security to accommodate a DFO.

Planners from the NCS and the General Services Administration (GSA) participated in surveying the site. The NCS planners determined that four Individual Mobilization Augmentees (IMAs) and one Regional Manager serving as the Federal Emergency Communications Coordinator could support the plan. They also coordinated with FEMA to obtain leased housing in Salt Lake City and with the Salt Lake City GSA Vehicle Fleet Management Center for two four-wheel vehicles.

To fulfill personnel requirements, the NCS selected Lieutenant Colonels Eugene Bonos and Craig Knapp to deploy on January 31, 2002 for 16 days to conduct the set-up phase and initiate telecommunications operations in the FEMA Olympic Watch Operations Center. Colonels Anne Walsh and Elizabeth Lippmann were selected for the deployment's second phase to continue operations and manage mission completion.

Edwin "Dave" Vest of the GSA Rocky Mountain Region was the Regional Manager responsible for continuity of operations throughout the mission and the designee prepared to assume the responsibilities as the Federal Emergency Communications Coordinator in the event of an actual disaster. A new member of the NCS IMA team, LTC Steve Mainger, was added to the deployment to provide continuity between the two phases.

The events of September 11 and the congestion on the public switched network presented the NCS with a challenge to overcome for future disasters. The NCS, in concert with industry and assisted by contractors, developed a solution to avoid the network congestion that ensued following the attacks of September 11th. The 2002 Winter Olympics served as a test bed for the concept.

Army Reserve LTC Craig Knapp, a National Communications System Individual Mobilization Augmentee (IMA) from Region IX (Pacific Rim Region), processes information while staffing FEMA Emergency Support Function-2 activities during the Olympic Winter Games in Salt Lake City last February. LTC Knapp was one of five NCS IMAs supporting the Games. (Photo courtesy of NCS IMA Office.)

The solution included use of GETS access cards with dual mode cellular/satellite handsets. These phones were distributed by NCS contract personnel to hundreds of law enforcement and emergency responders throughout the State of Utah, to personnel directly affiliated with Olympic operations, and to each IMA. A satellite phone base station was also installed on the FEMA Emergency Support Function (ESF)-2 desk at the Olympic Watch Operations Center.

During the deployment to Salt Lake City, the hours of pre-planning were evident. Vehicles and lodging more than met expectations and the absence of an actual emergency made the duty day less stressful than an actual deployment. FEMA made use of available time with classes provided by the various FEMA sections and orientation briefings provided by each ESF including the ESF-2/NCS briefing by Colonel Walsh. There were also several training exercises involving the entire operations center including an earthquake and a weapons-of-mass-destruction exercise.

Overall, the NCS deployment was a complete success. IMAs were given the opportunity to receive valuable training and also afforded the opportunity to attend various Olympic competitions. They represented both the NCS and the Army in a very positive light. v

Five Individuals Named to the NS/EPC

By Steve Barrett
National Communications System

WASHINGTON – Five new members have been named to the President's Critical Infrastructure Protection (CIP) Board's Committee for National Security and Emergency Preparedness Communications (NS/EPC), a 22-member body of Government communications experts that advise the White House on critical infrastructure protection issues involving telecommunications and information technology.

Joining the NS/EPC are Karen S. Evans, the Department of Energy's Chief Information Officer; Steven Price, Deputy Assistant Secretary of Defense, (Spectrum and C3 Policy); Edward Francis Meagher, Deputy Assistant Secretary for Information Technology Management and Deputy Chief Information Officer for the Department of Veterans Affairs; Ronald E. Miller, Associate Director of the Information Technology Services Directorate, Federal Emergency Management Agency; and Frederick Wentland, Director of Spectrum Plans and Policies, and Acting Associate Administrator, Office of Spectrum Management for the National Telecommunications and Information Administration.

Karen S. Evans, Department of Energy's member of the Committee for National Security and Emergency Preparedness Communications (NS/EPC). (Photo courtesy of the Department of Energy.)

The NS/EPC, renamed and made a standing committee of the CIP Board by Executive Order 13231, "Critical Infrastructure Protection in the Information Age," advises the President and the CIP Board on issues involving the Nation's emergency telecommunications capabilities and assets. Formerly known as the National Communications System (NCS) Committee of Principals and chaired by the NCS Manager, the NS/EPC investigates, researches, and addresses critical infrastructure protection communications issues that would affect the Nation in the event of a Federal disaster or national emergency.

Ms. Evans replaces Howard Landon as the Energy Department's NS/EPC committee member. Before joining Energy, she was Director, Information Resources Management Division, Office of Justice Programs (OJP), U.S. Department of Justice, Washington, D.C., where she was responsible for the management and successful operation of the Information Technology program. She is a 20-year veteran of Government service, working with several agencies, including the National Park Service, the Office of Personnel Management, and the Farmers Home Administration (FmHA) of the Department of Agriculture.

Prior to joining OJP, she served as the Assistant Director for Information Services at Justice Department headquarters, where she successfully managed Internet resources for the Department, including electronic mail services and security. While at FmHA, she served as the

Steven Price, Department of Defense's member of the NS/EPC. (Photo courtesy of the Department of Defense.)

acting Deputy Assistant Administrator for Management Information Systems, Deputy Director for the Applications Management Division and the Chief of Emerging Technology, where she managed the implementation on a nationwide basis, from inception to continuing operations of several critical automation systems.

She holds a bachelor's degree in Chemistry and a master's of business administration degree from West Virginia University.

Price replaces Navy Rear Admiral Robert Nutwell on the NS/EPC Committee. Prior to joining the Bush Administration in November 2001, Price served as President and Chief Executive Officer of LiveWire, a 2,500 person provider of mission critical software products and outsourcing services for communications, media and utility companies, which he founded.

Price was formerly the President and Chief Executive Officer of PriCellular Corporation, a publicly traded cellular telephone operator that was sold in June 1998 for $1.4 billion. Prior thereto, he was an attorney with Davis Polk & Wardwell. Previous to practicing law, he served in the U.S. State Department as Special Assistant to the U.S. Ambassador to the Strategic Arms Reduction Treaty (START) Talks and also worked in the mergers and acquisitions department of Goldman, Sachs & Co.

He is a Phi Beta Kappa, magna cum laude graduate of Brown University and earned a Juris Doctorate degree from Columbia University School of Law.

Edward Francis Meagher, Department of Veterans Affairs member of the NS/EPC. (Photo courtesy of the Department of Veterans Affairs.)

Meagher replaces Robert Bubniak as the Veterans Affairs representation to the NS/EPC Committee. He is responsible for administering the information technology, cyber security, and telecommunications programs across the Department. Prior to his appointment, Meagher served as a member of the Secretary of Veterans Affairs senior staff and principal advisor to the Secretary on all information technology issues.

Most recently, Meagher has run his own consulting practice working with technology-based start up companies. Prior to that, he served as a Principal at American Management Systems in its Department of Defense business unit; General Manager for Telecommunications and Healthcare at SSDS, Inc.; and Executive Vice President at Comprehensive Technologies, Inc. In addition, Mr. Meagher held the position of General Manager of Capital Systems/Systemshouse, Telecommunications Systems Integration business unit.

Ronald Miller, Federal Emergency Management Agency member of the NS/EPC. (Photo courtesy of FEMA.)

He attended the University of Dayton (Ohio) and served in the United States Air Force from 1966 to 1970 with tours of duty in The Philippines and Vietnam.

Ronald E. Miller replaces Clay Hollister as FEMA's NS/EPC Committee representative. Miller manages and operates FEMA's information technology and telecommunications systems, and provides information technology and telecommunications services to FEMA and other federal, state and local agencies when required. He joined FEMA in June 2001 as the agency's Deputy Chief Information Officer and Deputy Assistant Director for the Information Technology Services Directorate.

continued next page

Five Individuals, continued from page 13

Prior to joining FEMA, Mr. Miller was a team leader and information technology project manager at PricewaterhouseCoopers in Tampa. He also spent eight years with SAIC in such positions as senior requirements analyst, project manager and division manager at various sites, including Satellite Beach and Tampa, Florida, and Stuttgart, Germany.

Miller also served in the U.S. Air Force, assigned as an air intelligence officer and attaining the rank of captain. His awards include the Meritorious Service Medal, and the Air Force Commendation Medal. A native of Lake Charles, Louisiana, Miller holds a bachelor's degree in political science from Texas Tech University in Lubbock, Texas, and a master's degree in international relations from Troy State University.

Wentland takes over NTIA's seat on the NS/EPC Committee from William Hatch. Wentland has been with NTIA for the past 22 years and has worked in all facets of spectrum management. His Spectrum Plans and Policies Directorate office is responsible for spectrum plans and policies domestically and internationally with direct participation in World Administrative Radio conferences, continuity of Government operations in emergencies, spectrum allocation planning, public safety, satellite coordination and improvement of spectrum management processes through automation.

Prior to his employment with the NTIA, Wentland spent 22 years with the Air Force as an officer and worked in the area of communications and satellites of which he spent over seven years with the Department of Defense Joint Spectrum Center. One of his major achievements with the Air Force was his participation directly in NASA's Gemini/Apollo programs as a flight controller at Houston and also on the first lunar landing in July 1969. v

New Congressional Joint Economic Committee Compendium Examines Cyberterrorist Threat

A variety of security issues related to high technology is examined by leading experts in a new Joint Economic Committee compendium released today, Security in the Information Age: New Challenges, New Strategies.

The compendium contains contributions by many involved with the National Communications System (NCS) and the President's National Security Telecommunications Advisory Committee (NSTAC). Those authors include: John Tritak, Director of the Critical Infrastructure Assurance Office (CIAO); William Gravell, TRW's NSTAC Industry Executive Subcommittee (IES) representative; Scott Charney, Microsoft's IES representative; George Washington University's Dr. Jack Oslund, former chair of NSTAC's Legislative and Regulatory Group; Lee M. Zeichner, former senior counsel with the President's Commission on Critical Infrastructure Protection; and Mark Montgomery, former Director of Transnational Threats with the President's National Security Council.

"These studies build on previous JEC hearings on a number of security issues related to high technology," Chairman Jim Saxton said. "These studies examine how cyber security has become such an important component of our economic and national security, and the implications for economic and security policy. I would like to thank Senator Robert Bennett for his interest in this issue, and for his role in assembling the compendium of papers the Committee is releasing today," Saxton concluded.

"I commend Governor Ridge for his outstanding work to develop a national strategy and his recognition of the importance of the private sector in this process. I hope our report from the JEC will be of value in this effort," said Bennett.

"Just as mechanization was responsible for the Industrial Revolution, technology is the foundation of our new economy," Congressman Lamar Smith said. "The advantages of technology are obvious and so are the disadvantages. The Web is a fount of information, but also a tool for hackers, software pirates, child pornographers and cyber terrorists. To sustain our economic growth, we must secure our information networks and ensure that technology grows, not crime."

For a copy of the study, please visit the JEC website at www.house.gov/jec.

(Courtesy of Congressional Joint Economic Committee.) v

Chair Recaps, continued from page 7

Looking ahead

The Chair said that only a few of those gathered for the NSTAC meeting had heard the term "homeland security" seven months ago, but that is clearly the operative term as NSTAC looks forward. "Our role is not only affected by new security needs following September 11, but also the new policies and operational changes," said Mr. Burnham. "Since telecommunications and information is one of the critical infrastructures of Homeland Security, this committee will continue to play a critical role in advising the President on national security cyber issues."

The NSTAC Chair highlighted the enactment of Executive Order (E.O.) 13231, "Critical Infrastructure in the Information Age," which dictates that the President's Critical Infrastructure Protection Board — chaired by Mr. Clarke — will work with NSTAC on critical infrastructure protection issues. The Executive Order also created the National Infrastructure Advisory Council (NIAC) that will address cross-infrastructure concerns and State and local government roles.

The Chair also referenced E.O. 13228 – the Homeland Security document – that puts emphasis on the physical security of the nation's critical infrastructures. "This committee is going to continue to address physical as well as cybersecurity matters for NS/EP and Homeland Security," said Mr. Burnham. "Future work of NSTAC will have to take into consideration the thrust and functions of Homeland Security as outlined in this Executive Order." He added that the NCC and the Telecom-ISAC provide the model of successful industry Government partnership for information sharing as called for in this EO.

With the new emphasis toward homeland security, the Chair said the NSTAC work plan for the next cycle requires a shorter cycle in providing advice to the President. However, he added that both industry and Government must focus on the efficient and effective use of scarce industry and Government resources.

"There are now lots of committees addressing the same issue — NSTAC, NIAC and PCIS [Partnership for Critical Infrastructure Security] and the ISACs," said Mr. Burnham. "It does put a multiplicity of demands on us and we have to think that through. Since many of our members are supporting other Government and industry initiatives in cybersecurity, the Government must review the various venues and assist in prioritizing the critical issues to be addressed by each group, and we have a role to play in helping them think that through."

Mr. Burnham concluded by praising the work of the NSTAC Industry Executive Subcommittee and the NCS staff for the work they accomplished during the year. He also thanked the members of the NSTAC for their service to the Nation and their participation in NSTAC meetings. v

"Our role is not only affected by new security needs following September 11, but also the new policies and operational changes."