National Security and Emergency Preparedness

Telecom News

2004, Issue 1

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

Table of Contents

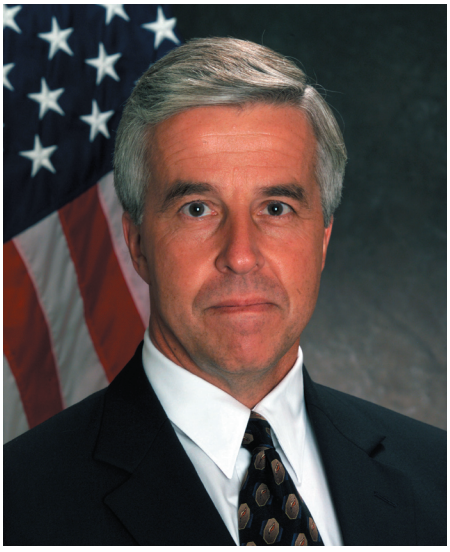
Homeland Security's Liscouski Named Manager of NCS

Homeland Security Secretary Tom Ridge announced on October 24, 2003, that the Department's Assistant Secretary for Infrastructure Protection, Mr. Robert P. Liscouski, would become Manager of the National Communications System (NCS). The announcement was published in the *Federal Register* on November 3, 2003.

Mr. Liscouski assumes the NCS position left vacant last March when the NCS transferred to the Department of Homeland Security from the Department of Defense. The position was last held by Air Force Lieutenant General Harry D. Raduege, Jr., currently the Director of the Defense Information Systems Agency (DISA).

The NCS, part of the Information Analysis and Infrastructure Protection (IAIP) Directorate, 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) communications infrastructure.

Mr. Liscouski became the Department's Assistant Secretary of Homeland Security for Infrastructure Protection in March 2003. He is responsible for the Department's efforts to identify our critical infrastructures and propose protective measures to keep them safe from terrorist attacks.



Mr. Robert Liscouski, Manager, NCS

Prior to his return to Government service, Mr. Liscouski was the Director of Information Assurance for The Coca-Cola Company.

Mr. Liscouski was a member of the Intelligence Science Board. His Government experience includes 11 years with the Diplomatic Security Service of the U.S. Department of State and five years criminal investigative experience as a homicide and narcotics investigator in Bergen County, NJ.

Mr. Liscouski received his bachelor of science degree in criminal justice from John Jay College of Criminal Justice in New York and his masters of public administration from the Kennedy School of Government, Harvard University.

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

NCS Slated to Get $141 Million of $31 Billion Homeland Security Bill

President George W. Bush signed legislation on October 1, 2003, providing $31 billion for Homeland Security purposes for fiscal year 2004.

During a signing ceremony at the Department of Homeland Security headquarters in Washington, D.C., the President noted the U.S. Congress-approved legislation, "commits $31 billion to securing our Nation, over $14 billion more than pre-Sept. 11 levels."

Nearly $840 million is targeted for the Department's Information Analysis and Infrastructure Protection (IAIP) Directorate – with $141 million earmarked for the National Communications System. Programs targeted for the funding include further development and deployment of the Wireless Priority Service, the Emergency Notification System, Back-up Dial Tone, and other national security and emergency preparedness telecommunications activities.

"Many of you have served your country for years, in agencies with proud histories and honored traditions. Some of you are new to the Federal service. All of us share a great responsibility," said President Bush. "Our job is to secure the American homeland, to protect the American people. And we're meeting that duty together."

Other IAIP projects include:

•$345 million for remediation and protective actions, which includes work with state and local governments, and industry, to identify and prioritize protective measures; and to develop objective protection standards and performance measures.

• $84.2 million for infrastructure vulnerability and risk assessment, which will develop and maintain a complete, accurate, and prioritized mapping of the nation's critical infrastructures and key assets including agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping, and monuments and icons.

•$52.3 million for information warnings and advisories, which will develop a comprehensive process to guide intelligence collection, assessment, evaluation, and prioritization; and ensure the required privacy protection related to the use, collection, and disclosure of private sector and personal information.

•$28 million for threat determination and assessment, which provides strategic assessments of our Nation's critical infrastructures and key assets, including 168,000 public water systems; 300,000 oil and natural gas production facilities; 4,000 offshore platforms; 278,000 miles of natural gas pipelines; 361 seaports; 104 nuclear power plants; 80,000 dams; and tens of thousands of other potentially critical targets.

•$20 million for the Departmental Command Center, which provides 24 hour a day, 7 day a week live watch for command, control, and monitoring capabilities of the Department.

The bill provides money, "for the key responsibilities at the Department of Homeland Security," the President pointed out, such as $5.6 billion earmarked for Project BioShield to develop methods to protect Americans against biological, chemical, and radiological threats.

Homeland Security Bill, page 16

NSTAC, OSTP, Georgia Tech Announce Findings from March Research and Development Exchange

By Steve Barrett
National Communications System

The President's National Security Telecommunications Advisory Committee (NSTAC), in conjunction with the White House Office of Science and Technology (OSTP) and the Georgia Institute of Technology's Information Security Center, released the findings of a research and development (R&D) exchange dealing with telecommunications and information systems impacting national security and emergency preparedness.

The report – *R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness (NS/EP)* – is the result of a two-day workshop conducted March 13 and 14, 2003, at Georgia Tech in Atlanta, Georgia. The fifth in a series of R&D exchanges conducted by NSTAC, this seminar was designed to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding the trustworthiness of NS/EP telecommunications systems.

Dr. John Marburger, Director, OSTP, presented the Keynote for the exchange, in which he said, "I am relying on this R&D Exchange to help me and my office give guidance to Office of Management and Budget and other White House policy organizations on the need for specific funding or programs to enhance the trustworthiness of the Nation's NS/EP telecommunications."

Dr. Carl Landwehr, Program Director, Trusted Computing Program for the National Science Foundation, introduces the Cyber 2 breakout session during the opening plenary session at the President's NSTAC Research and Development Exchange in Atlanta, Georgia. Behind Dr. Landwehr are Mr. Guy Copeland, Vice President, Information Infrastructure Advisory Programs for Computer Sciences Corporation (CSC) and a member of the NSTAC's Industry Executive Subcommittee, and Mr. Sami Saydjari of the Cyber Defense Agency (LLC). (Photo by Ms. Kiesha Miller)

Dr. Marburger demonstrated the strength of that conviction by personally moderating the closing plenary session of the Exchange in which the breakout session moderators reported their results.

Mr. F. Duane Ackerman, Chairman and CEO, BellSouth Corporation, addressed the Exchange attendees and highlighted three issues that will affect our ability to ensure trusted networks. First, "We need R&D to help us manage security as technology evolves. Keeping America safe and strong will require massive investment in innovation and R&D." Second, "I encourage all of us … to work on developing public policies that will help restore and protect the financial integrity of our national networks as we adapt to new threats and rapid technological change." Third, "In the Age of Networks, security and trust depend on a network of partners."

Mr. Guy Copeland, Vice President, Computer Sciences Corporation, and Chair of the NSTAC R&D Task Force, views the product of the Exchange as the beginning of a long-term collaboration of government, industry, and academia. He says, "This report lays out a series of challenges and describes general ways to begin addressing them. We now need to effectively use the community of interest – the "network of partners" – begun by this Exchange to flesh out the roadmap it offers and develop more detailed action recommendations for progress."

Dr. Seymour Goodman of Georgia Tech Information Security Center echoed Mr. Copeland's remarks. "We had an extraordinarily capable group

NSTAC R&D, page 13

FCC, NCS Spearhead a National Outreach Campaign to Secure Priority Phone Service Restoration to 9-1-1 Centers

The Federal Communications Commission (FCC) and the Department of Homeland Security's National Communications System (NCS) launched a campaign on April 24, 2003, to ensure that the Nation's 9-1-1 call centers, also known as Public Safety Answering Points (PSAP), are registered in the Telecommunications Service Priority (TSP) program to have their phone lines restored on a priority basis in the event of a national crisis or attack.

TSP is a Federal program that provides for priority installation and restoration of the telecommunications lines that are considered critical to the Nation's security and emergency preparedness, especially in times of disaster.

The FCC and NCS also announced that the national organizations that represent PSAPs – the National Emergency Number Association (NENA), the National Association of State 9-1-1 Administrators (NASNA), and the Association of Public-Safety Communications Officials International (APCO) – are joining the FCC and NCS in this nationwide campaign to increase PSAP participation in the TSP program.

The outreach campaign follows a joint letter to the national organizations from Mr. Brenton C. Greene, Deputy Manager of the NCS, and Mr. Edmond J. Thomas, Chief of the FCC's Office of Engineering and Technology, that called for a nationwide initiative to help educate PSAPs about the TSP program and to promote enrollment.

According to research conducted by the FCC and NCS, less than 10 percent of the Nation's approximately 7,500 PSAPs currently participate in the TSP program. PSAP administrators who operate the Nation's 9-1-1 centers readily qualify for inclusion in the TSP program because their services are essential to the health and safety of American citizens.

Mr. Greene and Mr. Thomas wrote in the letter, "PSAP administrators provide services that are essential to the protection of life and property of American citizens, and we believe they should avail themselves of the benefits of the TSP program. Lack of participation could jeopardize the restoration of essential service provided by the PSAP administrators during times of disaster and could put citizens at substantial risk of injury or loss of property at times when they are most vulnerable."

APCO President Mr. Vincent R. Stile said, "APCO recognizes the importance of the TSP program to the quick and efficient restoration of critical infrastructure and encourages all public safety communications centers to be aware of and participate in this program."

NASNA President Ms. Evelyn Bailey said, "The National Association of State 9-1-1 Administrators recognizes that participation in the TSP program is a key component of homeland security. 9-1-1 operators were the first responders on September 11, 2001. We must not become complacent. We must not assume that our 9-1-1 service provider or the telephone company will automatically give priority to 9-1-1 circuits if we have not registered them with TSP. We urge 9-1-1 centers throughout the Nation to be proactive and ensure participation in TSP."

NENA President Mr. John Melcher said, "NENA supports TSP as desirable and essential for quick restoration of 9-1-1 network trunking, as well as other critical PSAP mission-related communications circuits. As 9-1-1 becomes even more important in today's world, this becomes critical."

The TSP program provides for priority installation and restoration of the telecommunications lines most necessary to promote the Nation's security and emergency preparedness functions, especially in times of disaster. The FCC established the program in 1988, and the NCS administers the program. The TSP program covers more than 50,000 of the Nation's most critical lines, and the program has been instrumental in the timely restoration of key telecommunications lines in many disasters. Most notably, the TSP program played a crucial role in the restoration of telecommunications services to lower Manhattan following the attacks on the World Trade Center on September 11, 2001, by prioritizing the restoration efforts of the telecommunications carriers.

Additional information on the TSP program, including how to enroll, may be found at http://tsp.ncs.gov. Information on how to obtain FCC sponsorship and how to enroll in TSP may be found at http://www.fcc.gov/hspc/emergencytelecom.html.

NCS Conducts First Successful Test of Backup Dial Tone Capabilities

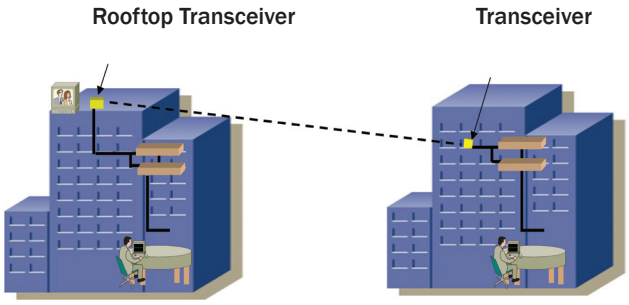
Officials with the National Communications System (NCS) announced that they successfully completed the first test of an initiative designed to study "Backup Dial Tone" capabilities in and around the National Capital Region.

The first tests, conducted with the Department of Energy (DOE) and Terabeam Corporation of Kirkland, Washington, involved deploying Free Space Optics (FSO) as a wireless transmission medium to connect two of their buildings using Voice over Internet Protocol (VoIP) technology. Officials with the DOE indicated that the VoIP service was the first phase in a multiphase plan to incorporate FSO technology at the Department. They said later phases would include implementing a videoconferencing service over the FSO link and using the FSO link to provide a diverse route between two private branch exchanges.

"...although the initial indications were that many Federal organizations already had a backup dial tone capability, some critical agencies did not."

The successful testing of Backup Dial Tone capabilities at the DOE began what NCS Deputy Manager Brenton C. Greene characterized as a multiphase study evaluating options for an alternative source of dial tone to critical Government facilities. "This is the type of capability that can play a vital national security and emergency preparedness (NS/EP) role following a disaster, such as the September 11, 2001, attacks in New York and Washington D.C.," said Mr. Greene. "The success of this pilot program with Terabeam is impressive and offers a promising option for Backup Dial Tone services."

Free space optics is a technology whereby voice and data signals are sent via a beam of light through the air, rather than through underground fiber optic cables. The light, using the same wavelength as a fiber optic cable light, is beamed directly through office windows or to building rooftops and allows high capacity for tremendous amounts of data transmission. FSO provides the transmission effectiveness of fiber optics but avoids the expense and manpower required to install underground cables.



Free Space Optics - Video Conference Service

The DOE is one of 23 Federal agencies that compose the NCS, an organization chartered to provide NS/EP telecommunications. The NCS, which moved to the Department of Homeland Security on March 1, 2003, oversees vital programs such as the Government Emergency Telecommunications Service, the Wireless Priority Service, and the Telecommunications Service Priority. Although these programs provide for priority queuing or priority provisioning of the public switched telephone network (PSTN) during emergencies, they do not address the problem of a loss of dial tone due to damage or congestion.

"This is the type of capability that can play a vital national security and emergency preparedness (NS/EP) role following a disaster, such as the September 11, 2001, attacks in New York and Washington D.C."

Brenton Greene

Soon after the September 11, 2001, attacks, the White House requested that the NCS evaluate the need for a backup dial tone capability to determine if it could have aided communications following the attacks. The White House also asked the NCS to evaluate various technical approaches to providing this service, with cost and time frame estimates.

NCS Backup Dial Tone, page 12

Mr. Thomas J. Falvey Named Chief of the NCS' Customer Service Division

On May 19, 2003, Mr. Thomas J. Falvey was named Chief, Customer Service Division for the National Communications System (NCS). The NCS is part of the Information Analysis and Infrastructure Protection Directorate (IAIP), Department of Homeland Security (DHS).

Mr. Falvey, who until recently served with the Department of Transportation (DOT) as Deputy Director of the Office of Intelligence and Security, replaced Air Force Colonel Wilson D. Crafton. Colonel Crafton remains with the NCS and serves as a military liaison officer assigned to address issues with the Department of Defense, the Joint Staff, Office of the Secretary of Defense, and DHS.

While at the DOT, Mr. Falvey served for more than 12 years leading Department actions to develop and implement national homeland security and critical infrastructure protection (CIP) policies, strategies, and processes. He led DOT CIP efforts in the areas of transportation security, critical infrastructure protection, key asset identification and protection, physical and information security, weapons of mass destruction, counter and anti-terrorism, consequence management, continuity of operations, and emergency planning and response.

His close, effective working relationship with the transportation sector and the establishment of Information Sharing and Analysis Centers led to the rapid, cooperative industry homeland security response to the September 11, 2001, attacks. Mr. Falvey also served with distinction as a commissioner on the President's Commission on Critical Infrastructure Protection from 1996 to 1997.

Before joining the Secretary of Transportation's office, Mr. Falvey held several civilian positions at the U.S. Coast Guard. A recently retired Captain in the Coast Guard Reserve, he commanded four Coast Guard reserve units, served in the Office of the Secretary of Defense, and led the Coast Guard Reserve response to the events of September 11, 2001, as the Reserve Chief of Staff, Commander, Coast Guard Atlantic Area.

Mr. Thomas J. Falvey, Chief, Customer Service Branch, National Communications System

Mr. Falvey graduated from the U.S. Coast Guard Academy and holds a master's degree in transportation management from the State University of New York.

New Members Named to NCS Committee of Principals

By DeJuan Stroman
National Communications System

The National Communications System (NCS) recently welcomed three new members to its Committee of Principals (COP). The new principals are **Mr. Stephen Cooper**, Department of Homeland Security (DHS); **Mr. W. Horton Tipton**, Department of the Interior; and **Dr. Linton Wells**, Department of Defense.

The COP and its subordinate working group, the Council of Representatives (COR), work in concert to explore the technical, regulatory, and legislative issues facing the national security and emergency preparedness (NS/EP) telecommunications community.

Mr. Cooper

In February 2003, President Bush appointed Mr. Cooper to be the DHS's first chief information officer (CIO). In this capacity, he supports the information technology resources of the 190,000 Federal employees from the 22 agencies that comprise DHS. Having worked in the private sector for over 20 years as an information

technology professional, Mr. Cooper has experience in both the public and private sectors. His previous positions include, Special Assistant to the President for Homeland Security and Senior Director for Information Integration in the White House Office of Homeland Security.

Mr. Tipton

Mr. Tipton has served over 21 years with the Federal Government. Prior to his appointment as the Interior Department's CIO in June 2002, Mr. Tipton worked as the Assistant Director for Information Resource Management, Energy, and Materials, and Resource Use and Protection within the Interior Department's Bureau of Land Management.

Dr. Wells

On August 20, 1998, Dr. Wells was appointed the Principal Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) and now serves in that capacity in the C3I successor agency, Networks and Information Integration. Additionally Dr. Wells also serves as the Acting Deputy Assistant Secretary of Defense for Spectrum, Space, Sensors, and Command, Control, and Communications.
Dr. Wells served 26 years in the U.S. Navy. From 1991 to 1998, he worked in the Office of the Under Secretary of Defense, serving most recently as the Deputy Under Secretary of Defense (Policy Support).

The NCS, now a part of the DHS, assists the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget with NS/EP communications issues.

COR Will Continue to Foster Cooperation and Information Sharing as Part of the DHS

On June 4, 2003, the Council of Representatives (COR) met at the National Communications System (NCS) in Arlington, Virginia to discuss and identify national security and emergency preparedness (NS/EP) issues that impact the full spectrum of Federal telecommunications assets and responsibilities.

To evaluate the most pertinent NS/EP telecommunications issues, the COR received a briefing on the NCS transition to the Department of Homeland Security (DHS), an update from the Critical Facilities Working Group (CFWG), a briefing on the NCS NS/EP Communications One-Stop Shopping Service (OSSS), and an update on the Wireless Priority Service (WPS).

Transition to the DHS

Mr. Brenton C. Greene, NCS Deputy Manager and Chief of the Department of Homeland Security's Infrastructure Coordination Division (ICD), welcomed COR members to the meeting, noting that the Committee of Principals (COP)/COR will play an integral role in supporting the DHS mission and will be an example throughout the Department for interagency cooperation. He noted that the Manager, NCS, has not yet been determined and that the next COP meeting will be postponed until after the new Manager, NCS, is confirmed.

Mr. Greene mentioned that, in an effort to reenergize the COP process in the new DHS environment, he would be meeting individually with each COR member's Principal. He asked the COR members to provide their COP Principals with a list of critical topics/issues that can be addressed during the one-on-one visits. Mr. Greene also introduced Mr. Tom Falvey, the new Office of the Manager, NCS (OMNCS) Customer Service Division Chief, who worked previously at the Department of Transportation.

Critical Facilities Working Group Update

Mr. Kenneth Moran, Federal Communications Commission (FCC) and CFWG Chair, updated the COR on the working group's progress. He stated

COR Information Sharing, page 8

COR Information Sharing, continued from page 7

that the working group established goals, scrutinized telecommunications diversity definitions, examined Network Reliability and Interoperability Council (NRIC) best practices, and interacted with the President's National Security Telecommunications Advisory Committee's Industry Executive Subcommittee. Mr. Moran explained that the working group will be producing a report related to ensuring diversity for critical facilities that perform the most essential functions as diversifying the assets of these facilities is one of the primary methods to assure their survivability in the event of a physical attack.

Mr. Greene mentioned that, in an effort to reenergize the COP process in the new DHS environment, he would be meeting individually with each COR member's Principal.

With regard to CFWG work, COR members also discussed the Government's difficulty in verifying industry compliance with national level NS/EP telecommunications programs without Government defined requirements until the programs are stressed in emergency situations, similar to September 11, 2001. The working group members felt that program compliance should be continually reviewed, and in order to facilitate this review, the Government should provide sufficient guidelines to determine national level NS/EP telecommunications requirements, to ensure both industry and Government compliance.

COR members decided that the best way to improve NS/EP services would be to create a working group to review the national level telecommunications programs and NS/EP services to ensure they address the concerns expressed by the working group members in their requirements discussion.

Mr. Tom Sellers, Government Services Administration (GSA) and CFWG member, requested that the working group address the concerns and work to identify requirements to determine compliance. The working group would also examine the current NCS Issuance System to see where updates are required. The members also discussed a similar issue with regard to Continuity of Operations and NS/EP communications plans. The group decided that COR members should review and update Continuity of Operations Plan/Continuity of Government related communications plans to include systems and circuits that will be used during an NS/EP event. (For further information on CFWG activities, please see the CFWG article.)

NS/EP Communications One-Stop Shopping Service

Ms. Sarah Jane League, formerly the Special Assistant to the Chief, Critical Infrastructure Protection (CIP) Division, NCS, briefed the COR on the NS/EP One-Stop Shopping Service (OSSS), which provides a central point of contact for all NS/EP priority communications services. OSSS manages and supports the consolidated operations and user missions and functions of the Government Emergency Telecommunications Service, the Telecommunications Service

Mr. Brenton C. Greene, Deputy Manager, National Communications System

Priority System, the Emergency Notification System (ENS), Shared Resources (SHARES), High Frequency (HF) Radio Program, and the National Coordinating Center for Telecommunications (NCC).

To date, several capabilities for the identified program/service areas have been implemented including the first draft of the OSSS Concept of Operations, a virtual call center, and the NS/EP Communications Services portal page.

Wireless Priority Service

Mr. Vernon Mosley, NCS Technology and Programs Division, updated the COR on the progress of the wireless priority service (WPS) program and briefly explained the process to make an NS/EP call during congestion based on wireline and wireless priority capabilities.

Mr. Greene noted that WPS has a national footprint and service is available on a GSA schedule for $4.50 per month. He explained that the program has encountered a slowdown because of

decreased fiscal year 2003 allotted funds which will result in deployment delays for Global System for Mobile (GSM) carriers', the full integration of code division multiple access capabilities, and the program's full operational capacity by approximately one year.

As the NCS becomes integrated into the DHS, the missions of the COP and the COR will not change. These bodies will continue to work to strengthen the overall NS/EP mission and will serve a crucial role in supporting key objectives of the DHS mission. The protection and security of our Nation's critical telecommunications infrastructure remain the primary goals of the COP and the COR and their extensive knowledge of NS/EP efforts and experience with interagency and private sector cooperation will prove invaluable to the DHS and its efforts.

Critical Facilities Working Group Strives to Ensure Diversity of Facilities that Support NS/EP Functions

The Council of Representatives (COR) established the Critical Facilities Working Group (CFWG), a subgroup of the COR, at its October 30, 2002, meeting.

The working group's purpose is to develop a solution for telecommunications diversity issues, determine requirements to ensure adequate redundancy and diversity of critical telecommunications facilities that support national security and emergency preparedness (NS/EP) functions when service is provided by multiple carriers, and continue to support telecommunications diversity and redundancy as an ongoing customer service to the Federal Government.

Upon completion of its work, the CFWG plans to publish its findings and recommendations in a report that it ultimately hopes other Government agencies will use as a template when working with telecommunications carriers to develop their own contractually based diversity requirements. To accomplish its tasking, the working group established the following goals:

Develop a template to:

- Identify agencys' critical NS/EP functions for which telecommunications services are essential;
- Identify the critical telecommunications facilities that are used to provide the agency access to the public switched network (PSN);
- Assess whether these facilities contain sufficient diversity and redundancy to ensure the agency can support its NS/EP functions over the PSN at all times; and
- Ensure these facilities continue to contain adequate diversity and redundancy.

Develop a process that:

- Government agencies can use to purchase certain circuits for diversity;
- A sanctioning body can use to designate circuits as "diversity circuits;" and
- Carriers can use to implement operating procedures to ensure "diversity circuits".

Develop a process to:

- Ensure adequate redundancy and diversity of critical telecommunications facilities that support NS/EP functions when service is provided by multiple carriers; and
- Continue to support diversity and redundancy as an ongoing customer service to the Federal Government.

Since September 2002, the working group has invited representatives from MCI, Booz Allen Hamilton, Universal Access Inc., BellSouth, and WinStar to brief the CFWG on a variety of diversity topics. Representatives from MCI discussed the importance of 99.999 percent reliability for mission-critical networks, while personnel from Booz Allen Hamilton presented the capabilities of the Infrastructure Mapping and Analysis Tool, a tool that allows users to view local switch lines between nodes in a specific region.

Representatives from Universal Access Inc., presented information about the proprietary telecommunications facilities database from a communications integrator perspective, BellSouth personnel discussed managing and tracking telecommunications facility diversity, and the representative from WinStar spoke about "Line of Sight," a wireless diversity routing alternative.

As a result of the industry briefings, working group members gained valuable

CFWG Supports NS/EP, page 10

CFWG Supports NS/EP, continued from page 9

insight into diversity issues including the need to: (1) understand how service providers have diversified critical facilities; (2) ensure accurate record keeping; (3) clearly define diversity and maintenance provisions in contracts; and (4) understand the importance of the administrative support required to maintain and audit diverse critical facilities.

Mr. Kenneth Moran, Federal Communications Commission (FCC) and CFWG Chair, stated that the future activities of the CFWG include analyzing Network Reliability and Interoperability Council (NRIC) Best Practices, investigating General Services Administration (GSA) contracts that mandate diversity, exploring diversity maintenance provisions in Defense Information Systems Agency (DISA) contracts, and supervising critical facilities data calls to the COR to populate the Department of Homeland Security's National Communications System (NCS) critical facilities database.

Mr. Moran also stated that the CFWG's early findings show that the method to ensure diversity depends on the carrier's record keeping process and noted that ensuring diverse routing for critical NS/EP functions is difficult for telecommunication service providers to guarantee. Mr. Thomas Sellers, GSA and CFWG member, added that the GSA can stipulate diversity mandates in contracts; however, if the telecommunications service provider does not track routing, diversity mandates in the contract are unenforceable.

Currently, the CFWG has not set a date for report publication; however, the report will be used to evaluate and address communications diversity for the critical facilities identified in the NCS database. Working group members also hope that the final report will provide Government agencies with valuable knowledge needed to ensure that the Government's telecommunications networks as a whole are diverse enough to adequately support future emergency response activities.

Mr. Moran also stated that the CFWG's early findings show that the method to ensure diversity depends on the carrier's record keeping process and noted that ensuring diverse routing for critical NS/EP functions is difficult for telecommunication service providers to guarantee.

CIP Division Launches Outreach Program With New Trade Show Booth

By Lisa Phillips-Morris
National Communications System

The National Communications System (NCS), Critical Infrastructure Protection (CIP) Division officially launched its tradeshow and events program this past spring at the Emergency Medical Service (EMS) Today Conference in Philadelphia, Pennsylvania with a new touch – a new trade show booth.

Since then, NCS members have transported the booth through numerous events to promote the NCS, the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate, and the agency's priority telecommunications programs and services.

Designed and developed last winter, the tradeshow program has become a significant element of the more comprehensive strategy for the NCS to reach out to audience segments, which have a national security and emergency preparedness (NS/EP) mission. The CIP outreach program's goal is to bring pertinent information about the NCS and its priority telecommunications services to support NS/EP efforts across Federal, State, and local Government, critical infrastructure industries, and other authorized NS/EP organizations.

Services represented in the booth include the Telecommunications Service Priority program, the Government Emergency Telecommunications Service, the Wireless Priority Service, the Shared Resources High Frequency Radio program, and the One-Stop Shop Services. The outreach program identifies the ways in which these services can benefit the various organizations and the importance of incorporating the services into their emergency response plans. The CIP Division services support the initiation, coordination, and restoration of NS/EP telecommunications during crises, emergencies, or national disasters.

Booth Design

The CIP Division booth has a contemporary design with light maple wood laminate, NCS-blue fabric sides, and striking red tabletops. The patriotic look of the booth is anchored by a dramatic, vibrantly colored, graphic with the American flag at the upper left corner. The graphic is a collage of photos that represents the functions of the division;

Priority Telecommunications Services; Planning, Training, and Exercise; Network Analysis and Design; and International Affairs.

The colorful backlit graphic is the focal point of the booth and its shear magnitude serves to draw attention and encourage people to stop and learn more about the NCS and its programs and services.

Public response has been extremely positive. Smaller graphics decorate the side panels and depict regional disasters to include the September 11, 2001, terrorist attacks in New York City and at the Pentagon.

Upcoming Events

The tradeshow outreach program is proving to be an effective way for the NCS to reach out to its current and future customers. The NCS will continue to deploy the booth around the country to provide critical information to NS/EP audiences about the NCS, DHS, and priority telecommunications programs and services.

For more information, please check the NCS Web site at http://www.ncs.gov for upcoming conference dates and locations.

The National Communications System (NCS) will have a presence at a variety of upcoming seminars and conferences with the deployment of the NCS outreach booth. NCS personnel will staff the booth, providing a variety of information on NCS programs involving national security and emergency preparedness communications. (NCS photo.)

Secretary Ridge Unveils Homeland Security Department Seal

Department of Homeland Security (DHS) Secretary Tom Ridge unveiled the Department's new seal while speaking to 200 DHS employees in Selfridge, Michigan on June 19, 2003. The seal is symbolic of the Department's mission – to prevent attacks and protect Americans on the land, in the sea, and in the air.

The Department developed the seal with input from DHS senior leadership, employees, and the U.S. Commission on Fine Arts. The Ad Council, which currently partners with DHS on its "Ready" campaign and the consulting company Landor Associates were responsible for graphic design and maintaining heraldic integrity.

In the center of the seal a graphically styled white American eagle appears in a circular blue field. The eagle's outstretched wings break through an inner red ring into an outer white ring that contains the words "U.S. DEPARTMENT OF" in the top half and "HOMELAND SECURITY" in the bottom half in a circular placement.

The eagle's wings break through the inner circle into the outer ring to suggest that the DHS will break through traditional bureaucracy and perform Government functions differently. In the tradition of the Great Seal of the United States, the eagle's talon on the left holds an olive branch with 13 leaves and 13 seeds while the eagle's talon on the right grasps 13 arrows.

Centered on the eagle's breast is a shield divided into three sections containing elements that represent the American homeland – air, land, and sea. The top element, a dark blue sky, contains 22 stars representing the original 22 entities that have come together to form the Department. The left shield element contains white mountains behind a green plain underneath a light blue sky. The right shield element contains four wave shapes representing the oceans alternating light and dark blue separated by white lines.

All 180,000 DHS employees are receiving a DHS lapel pin and a personalized certificate. NCS personnel received their pins and certificates in September. The personalized certificate signifies that the employee was part of the DHS at its inception. The seal will ultimately be used on Department materials, signage, credentials, badges, vehicles, sea vessels, and aircraft.

DHS Announces $165 Million in Grants to States

The Department of Homeland Security's (DHS) Emergency Preparedness and Response Directorate, also known as the Federal Emergency Management Agency (FEMA), recently provided $165 million in grants to help State and local Governments better prepare to respond to all hazards preparedness activities and emergency management. These funds are a result of a significant increase in funding for the Emergency Management Performance Grants (EMPG) program from the FY 2003 budget.

Homeland Security Secretary Tom Ridge noted, "This is an important step in getting essential funding to our State and local Governments to help them battle this national effort in the war on terror. We recognize the challenge that the states and localities face when planning to respond to a potential disaster and the Department is committed to providing them with the tools they need to be prepared."

The EMPG program provides states with the flexibility to allocate funds according to risk vulnerabilities and to address the most urgent State and local needs in the areas of all hazard mitigation, preparedness, response, and recovery. The effectiveness of State and local responder organizations is critical to the success of all aspects of the homeland security mission, but especially to disaster response operations.

Local emergency managers plan, train, exercise, and provide the facilities needed to coordinate all emergency services in response to major incidents. They also assume the leading role in mitigation program activities, those designed to reduce the vulnerability of communities to all hazards.

"The $165 million to State and locals for all hazards preparedness represents a 40 percent increase from fiscal year 2002 EMPG funding," said Mr. Michael D. Brown, Under Secretary for Emergency Preparedness and Response. "These grants are further evidence of this Administration's commitment to State and local Governments for all hazards emergency preparedness efforts."

The EMPG program, first awarded in fiscal year 2000, was intended to consolidate funding streams that FEMA provides to state emergency management departments and agencies.

NCS Backup Dial Tone, continued from page 5

Ms. Valerie Liles, the NCS Technology and Programs Division's technical lead on the project, said that although the initial indications were that many Federal organizations already had a backup dial tone capability, some critical agencies did not. "This study will identify agencies with an existing backup dial tone capability, agencies that should implement backup dial tone in the future, and which backup dial tone solution is optimum for that agency," she said.

Ms. Liles said the DOE test was only part of a series of tests under the initiative's third stage – a technology demonstration stage that could last a year per demonstration. She said that agencies such as the DOE were solicited to partner with the NCS and were given the option of selecting a particular technology to employ. "Once our volunteer partner agencies select the technical solution they are willing to help us demonstrate, we negotiate agreements with them and then our contractor arranges installation and conducts tests," Ms. Liles said. She added that after a year of testing, the partner agency could opt to have the capability removed, or they could negotiate with the supplier to retain it.

The NCS completed the first two phases of the three-phase study in June 2002, which consisted of analyzing generic and actual government architectures used to access the PSTN.

Recently, a fourth "physical routing diversity" phase was added to the Backup Dial Tone project. In this phase, the NCS will define an analysis methodology and develop criteria, metrics, and tools to analyze critical facilities' telecommunications, specifically public network accesses, which may be disrupted by natural disasters, violent incidents, or terrorist acts.

Free space optics is a technology whereby voice and data signals are sent via a beam of light through the air, rather than through underground fiber optic cables.

NSTAC R&D, continued from page 3

of people from industry, Government, and the universities who were largely in agreement on what work needs to be done," said Dr. Goodman, who studies impacts of information technologies on international affairs, national security, and defense policy. He said the group agreed that this work should have started long ago and that the conference "…will serve as a real stimulant in this regard."

In its executive summary, the R&D report indicates that the Nation's leadership is placing an increasing reliance on the public switched network, the Internet, and computer applications to support national, homeland, and economic security; emergency preparedness; and public safety places a premium on "trusted" systems and networks.

"The September 11, 2001, terrorist attacks demonstrated the critical importance of networked information systems in supporting national crisis management and response." The report indicates that "...ensuring that national leaders, first responders, infrastructure owners and operators, and the general public receive timely, accurate, and complete information through trustworthy NS/EP telecommunications – and the underlying networked information systems – is crucial to meeting national security and homeland security objectives."

The report also indicated that a majority of the research studies and activities on the trustworthiness of network information systems have focused on vulnerabilities in cyberspace. However, achieving and sustaining trustworthiness in those systems is jeopardized by a host of threats, such as exploitation by insiders, physical destruction that extends beyond cyberspace. As a result, the sponsors chose to adopt a broad perspective for the R&D Exchange, exploring the full range of trustworthiness issues as they pertain to NS/EP telecommunications systems.

Specifically, exchange attendees examined four aspects of trustworthiness:

•Cyber Security and Software: defending against the threat of malicious software attacks, distributed denial of service attacks, and other forms of intentional or unintentional corruption of software;

•Human Factors: ensuring that humans at all stages of the security

NSTAC R&D, page 23

Loy Becomes Deputy DHS, England Returns to Navy Position

By Steve Barrett
National Communications System

The Department of Homeland Security's Deputy Secretary has returned to the Pentagon and the former Commandant of the Coast Guard is nominated to replace him.

President George W. Bush announced on October 23, 2003, his intention to nominate Admiral (ret.) James M. Loy as Deputy Secretary of Homeland Security. Admiral Loy was sworn in as Deputy Secretary of Homeland Security on December 4, 2003. Admiral Loy, formerly served as the Administrator for the Department of Homeland Security's Transportation Security Administration, would replace Gordon England, who recently returned to the Pentagon as Secretary of Navy.

Admiral Loy previously served as Under Secretary of Transportation for Security and was Commandant of the Coast Guard and Coast Guard Chief of Staff. He graduated from the U. S. Coast Guard Academy in 1964 and holds masters degrees from Wesleyan University and the University of Rhode Island.

In a statement released by Department of Homeland Security Secretary Tom Ridge, the Secretary said, "Gordon England is an exemplary public servant and true patriot." He said Mr. England's experiences with mergers and the establishment of complex management and organizational systems ,"…have been critical to the effective start of the new department. One of his legacies of service will be his effort to lay the foundation for this new department. We wish him well as he continues his service to this Administration and our country."

Mr. England has also served as Executive Vice President of General Dynamics Corporation. Throughout his career, Mr. England has served as a member of the Defense Science Board and has received awards from the National Defense Industrial Association and the National Management Association. He is also a member of the Aviation Heritage Hall of Fame. Mr. England received his bachelor's degree from the University of Maryland and his master's from the M.J. Neeley School of Business at Texas Christian University.

Secretary Ridge Announces Homeland Security Advisory Council Members

Secretary of Homeland Security Tom Ridge announced the appointment of 18 individuals who will serve as members of the Homeland Security Advisory Council (HSAC). The Council will provide advice and recommendations to the Secretary on homeland security related issues. The HSAC convened for the first time as a Department of Homeland Security (DHS) entity on June 30, 2003, at the Mayflower Hotel in Washington, D.C.

"I am grateful that these accomplished and experienced citizens are willing to serve and provide valuable insights on critical homeland security issues," said Secretary Ridge. "By bringing together members from diverse public and private sector backgrounds, the Council will provide recommendations that will help DHS more effectively integrate our efforts to make the homeland more secure."

A detailed *Federal Register* notice regarding the meeting was posted on June 13, 2003.

HSAC Leadership

Secretary Ridge selected **Mr. Joseph J. Grano, Jr.,** of New Jersey to serve as Chair of the HSAC. He is currently the Chairman and Chief Executive Officer (CEO) of UBS Paine Webber and a veteran of the U.S. Special Forces. He received a Bronze Star for his service in Vietnam, the Ellis Island Medal of Honor, and the United Service Organizations' Gold Medal Award for Distinguished Service. Mr. Grano previously served as Chair of the President's Homeland Security Advisory Council (PHSAC), which was dissolved on March 31, 2003.

Judge William H. Webster of the District of Columbia will serve as Vice Chair. In 1977, Judge Webster became Director of the Federal Bureau of Investigations after serving as a judge on the U.S. Court of Appeals for the Eighth Circuit. In 1987, Judge Webster became the Director of the Central Intelligence Agency (CIA), which he led until 1991. Since then, Judge Webster has practiced law for the Washington, D.C. firm of Milbank, Tweed, Hadley, and McCoy. Judge Webster served as Vice Chairman of the PHSAC from 2002-2003.

Other Members of the HSAC

Mr. Richard A. Andrews of California is the Senior Director, Homeland Security Projects, for the National Center for Crisis and Continuity Coordination. From 1991 to 1998, he served as the Director of the Governor's Office of Emergency Services for the State of California and was the President of the National Emergency Management Association from 1995 to 1996.

Ms. Kathleen M. Bader of Michigan is a Business Group President with Dow Chemical Company and the Corporate Vice President for Quality and Business Excellence. She joined Dow in 1973 and has held a variety of positions in sales and operations.

Mr. David Arthur Bell of New York is Chairman and CEO of the Interpublic Group of Companies, the world's largest marketing, communications, and services company. Mr. Bell is the current Chairman of the Ad Council.

Dr. Jared Cohon of Pennsylvania is the President of Carnegie Mellon University. Dr. Cohon is a national authority on environmental and water resource systems analysis. He served as a member of the Nuclear Waste Technical Review Board and was named Chairman of the Board in 1997. In 1992, he was named to the position of Dean of the School of Forestry and Environmental Studies at Yale University.

Dr. Ruth David of Virginia is presently President and CEO of ANSER, Inc., an independent, not-for-profit, public service research institution. From 1995 to 1998, she was Deputy Director for Science and Technology at the CIA. Dr. David began her professional career at Sandia National Laboratories. She has previously served on the Defense Science Board, and, among others, currently serves on the National Security Agency Scientific Board and the National Research Council Naval Studies Board.

The Honorable Lee Herbert Hamilton of Indiana is the Director of the Woodrow Wilson International Center for Scholars. Prior to being named Director of the Wilson Center, Representative Hamilton served for 34 years as a U.S. Congressman from Indiana's 9th District. While in Congress, he served as a member of the Committee on Foreign Affairs where he was the ranking Democrat for 10 years and the committee Chairman during the 103rd Congress. Representative Hamilton also served as Chairman of the Joint Economic Committee and as a member of the Permanent Select Committee on Intelligence, the Joint Committee on the Organization of Congress, and the Select Committee to Investigate Covert Arms Transactions with Iran.

Governor Michael Leavitt is the 14th governor of the State of Utah. He was first elected in 1992, reelected in 1996, and

then became only the second governor in Utah history to be elected to a third term in 2000. Governor Leavitt is also a past Chairman of the National Governors' Association.

Mr. James T. Moore of Florida is currently Commissioner of the Florida Department of Law Enforcement and serves as Governor Jeb Bush's homeland security advisor. He was first confirmed as Commissioner in 1988, after serving with the Department since 1973. During his tenure, Mr. Moore served as a Standards and Training specialist, the Director of the Division of Staff Services, and Deputy Commissioner.

Mr. James Rodney Schlesinger of Virginia has a long and distinguished record of public service. He has served as Secretary of the Energy, Secretary of Defense, Director of Central Intelligence, and Chairman of the Atomic Energy Commission. Mr. Schlesinger is currently the Chairman of the Board of Trustees of the MITRE Corporation.

Mr. Sidney Taurel of Indiana is the Chairman, President, and CEO of Eli Lilly and Company. He joined the Lilly subsidiary Eli Lilly International Corporation in 1971 and has held various positions in Brazil, France, Eastern Europe, and London. In 1986, he became President of Eli Lilly International Corporation and then Executive Vice President of the Pharmaceutical Division in 1991.

Dr. Lydia Waters Thomas of Maryland is President and CEO of Mitretek Systems, Inc. She was previously Vice President and General Manager responsible for the company's Center for Environment, Resources, and Space. Dr. Thomas served two terms on the Environmental Advisory Board to the Chief of Engineers, U.S. Corps of Engineers and was chairperson of the Chemicals Regulation Sub-Group of the United States Energy Association. In February 2003, Dr. Thomas was recognized as "Black Engineer of the Year" by the Black Engineer Selection Panel.

Mayor Anthony Williams was elected Mayor of the District of the Columbia in 1998. Before becoming Mayor, he was Chief Financial Officer of the District of Columbia and of the U.S. Department of Agriculture. His additional past positions include Deputy State Comptroller of Connecticut, Executive Director of the Community Development Agency in St. Louis, Assistant Director of the Boston Redevelopment Authority, and adjunct professor at Columbia University.

Ex Officio Members

Ex officio members of the HSAC serve in order to bridge efforts with other key Federal advisory boards. HSAC ex officio members will include:

Secretary of Homeland Security Tom Ridge (left) swears in Mr. Joseph J. Grano, Jr., (center) as the Chair of the Homeland Security Advisory Council and Judge William H. Webster as Vice Chair during the council's first meeting on June 30, 2003, in Washington, D.C. (Department of Homeland Security Photo.)

Mr. Norman R. Augustine of Maryland is currently a member of the Board of Directors of Conoco Phillips, Black & Decker, Procter & Gamble, and Lockheed Martin and a member of the Board of Trustees of Colonial Williamsburg, MIT, and Johns Hopkins University. Mr. Augustine served as Chairman and Principal Officer of the American Red Cross for nine years and is a former Chairman of the National Academy of Engineering, the Association of the United States Army, and the Defense Science Board. Mr. Augustine represents the President's Council of Advisors on Science and Technology's Science Technology of Combating Terrorism Panel on the HSAC.

Dr. Vance D. Coffman of Maryland is Chairman of the Board and CEO of Lockheed Martin Corporation. Dr. Coffman also serves as the Chairman of the Aerospace Industries Association for the year 2003 and represents the President's National Security Telecommunications Advisory Committee on the HSAC.

Mr. Richard K. Davidson of Nebraska has been the Chairman and CEO of Union Pacific Corporation since January 1, 1997. He joined Union Pacific Railroad in 1982. He also serves as a Trustee and Director of the Malcolm Baldrige National Quality Awards Foundation. Mr. Davidson represents the National Infrastructure Advisory Committee on the HSAC.

Secretary Ridge also announced the appointment of **Mr. Christopher J. Furlow** as Executive Director of the HSAC. Mr. Furlow previously served the Bush Administration as Director for State Affairs in the White House Office of Homeland Security and as Deputy Assistant Secretary of Commerce for Legislative and Intergovernmental Affairs.

Homeland Security Bill, continued from page 2

President George W. Bush signs the Department of Homeland Security Appropriations Bill during ceremonies held in Washington, D.C. on October 1, 2003. (White House photo)

Additionally, the President noted that $4 billion goes to police, fire, medical and other emergency first responders nationwide. More than $700 million of that money, he said, will be targeted for use in urban areas where it is most needed.

President Bush said $40 million is earmarked for volunteer groups that will work with local first responders to prepare for emergencies. "We're ensuring that America's firefighters and police officers and emergency medical personnel have the best possible training and equipment and help they need to do their job," Bush emphasized.

Money will also be provided to beef up security at the Nation's airports and along America's borders, the president said. The bill, he continued, also provides the Coast Guard with, "the resources to deploy additional maritime safety and security teams and patrol boats and the sea marshals to protect our ports and waterways."

More than $900 million is allocated for science and industry projects, "including a major effort to anticipate and counter the use of biological weapons," the president pointed out. The bill also provides more than $800 million to assess potential vulnerability across the Nation's critical infrastructures. And, if vulnerabilities are discovered, "we'll take action to protect them," the President declared.

President Bush said the U.S. armed forces and other agencies continue to take actions abroad to confront terrorism wherever it may be. And, "we've been charged to protect our homeland, as well," he said, noting that the bill he signed is, "a major step forward" in that ongoing effort.

(Editor's Note: Gerry Gilmore of the American Forces Press Service contributed to this article.)

DHS Creates a New Division To Combat Cyber Threats

The Department of Homeland Security (DHS), in implementing the President's National Strategy to Secure Cyberspace and the Homeland Security Act of 2002, has created the National Cyber Security Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate.

The NCSD will provide 24/7 functionality, including conducting cyberspace analysis, issuing alerts and warnings, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. This division represents a significant step toward advancing the Federal Government's interaction and partnership with industry and other organizations in this critical area.

"Cyber security cuts across all aspects of critical infrastructure protection. Most businesses in this country are unable to segregate the cyber operations from the physical aspects of their business because they operate interdependently," said DHS Secretary Tom Ridge. "This new division will be focused on the vitally important task of protecting the Nation's cyber assets so that we may best protect the Nation's critical infrastructure assets."

The NCSD will build on the existing capabilities transferred to DHS from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System. The creation of the NCSD both strengthens Government wide processes for response and improves protection of critical cyber assets through maximizing and leveraging the resources of these previously separate offices.

Combat Cyber Threat, page 24

United States and United Kingdom Announce Joint Anti-Terrorism Working Group

By Gerry J. Gilmore
American Forces Press Service

The United States (U.S.) and the United Kingdom (U.K.) will partner to establish a joint anti-terrorism working group, the two Government's top civil security officials announced at a press briefing in Washington D.C., on April 1, 2003.

"The U.K. has extensive experience in battling the challenge of terrorism at home," U.S. Homeland Security Secretary Tom Ridge told reporters after meeting with British Home Secretary David Blunkett. "This relationship will benefit the strong homeland security partnership that our countries have developed since the attacks on our country on September 11th."

Secretary Ridge noted that he and Secretary Blunkett discussed, "strengthening the partnership between our two countries in fighting the war on terror" and "ideas that will benefit both of our countries in the area of homeland security."

Secretary Ridge said topics of discussion included the sharing of best practices related to countering terrorism at home and abroad, joint training exercises, cyber and physical infrastructure security, border and transportation security, research and development, and science and technology.

The U.K., "has been a critically important ally in bringing our attackers to justice," Secretary Ridge said, noting that the U.S. looks forward to continuing to work with the U.K., "to battle terrorism at home and abroad."

Secretary Blunkett also praised the Anglo-American partnership against terror, noting, "the unprecedented level of cooperation we now have, which has been built up over the last 18 months."

America and the U.K. have shared, and will continue to share, counter-terrorism intelligence, the two officials said. The working group, they pointed out, would go a step further in U.S. – U.K. collaboration.

Secretary Blunkett said the group, "will involve officials from the Homeland Security Department and our own Department." Such collaboration would facilitate cross learning, he said, which would enhance the development of similar methods to protect the two Nations' populations.

"All of us know that we have never faced a threat like the one that has developed since the 11th of September 2001," Secretary Blunkett said. "Because we are partners, including [in] the conflict in Iraq, we need to be more vigilant and we need to be more aware."

The two countries will be conducting joint training exercises, Secretary Blunkett said so that, "we can look at what might formulate the necessary steps to protect us from simultaneous attacks, from joint attacks." The first joint exercises will be conducted online, the British official said, "then physical exercises."

"The U.K. has extensive experience in battling the challenge of terrorism at home," U.S. Homeland Security Secretary Tom Ridge told reporters after meeting with British Home Secretary David Blunkett. "This relationship will benefit the strong homeland security partnership that our countries have developed since the attacks on our country on September 11th."

Secretary Blunkett said the U.S. and the U.K. will also brainstorm such issues as border protection, surveillance, biometrics and identification, Visa and passport controls, and the pooling of research and training.

Establishing joint facilities, he added, would assist the two countries in dealing with the threat, "of chemical, biological, radiological, and nuclear imports and the danger that people are transferring the capability across the world."

Secretary Blunkett said the U.S. – U.K. partnership will also seek ways to thwart the threat of cyber and electronic attack, "which would disrupt our commerce."

The two Nations are also, "collaborating closely on the development of new assessment techniques," he said. Secretary Blunkett noted that the United States had its Terrorist Threat Integration Center, which started operations

U.S./U.K., page 20

The House of Representatives Establishes Select Committee to Coordinate Homeland Security Activities

After Congress passed legislation in November 2002 creating the new Department of Homeland Security (DHS), the true challenge of standing-up the new Department began. The House of Representatives had the significant task of consolidating oversight responsibilities for the new Department. Prior to the creation of the DHS, 88 House committees and subcommittees had partial responsibilities to oversee the 22 agencies that entered the DHS.

In early January 2003, House leadership considered the rules package for the 108th Congress, and decided to establish a select committee for the next two years to coordinate the activities of the various committees with jurisdiction over the DHS. Rep. Christopher Cox (R–CA) was quickly identified as the Chairman of the full committee and Rep. Jim Turner (D–TX) was picked as the ranking minority member. Full committee membership and subcommittee leadership were announced on March 28, 2003.

Representative Cox's experience as Chairman of a select committee that investigated technology transfer to China by American companies in 1999 made him a good candidate for the position. In addition, House Speaker Dennis Hastert (R–IL) also thought it was important to have a member of the Congressional leadership in the position. His colleagues and the media have portrayed Representative Cox as studious, methodical, and cerebral in his approach to educating himself on issues and running committees.

Representative Cox selected Mr. John Gannon, former Deputy Director of the Central Intelligence Agency and former Chairman of the National Intelligence Council as the Committee's staff director. Immediately prior, Mr. Gannon served as the Team Captain for the development of the DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate. One of the major tasks ahead for Mr. Gannon will be to help coordinate with other committees, reach an understanding on jurisdiction, and determine the areas that the Select Committee can lead.

Representative Cox sees the role of the Federal Government in homeland security issues as not to increase the number of first responders to respond to events, but to prevent attacks from occurring by investing in intelligence

House Select Committee on Homeland Security

Republicans	Democrats
Christopher Cox (CA) – Chairman	*Jim Turner (TX) – Ranking Member*
Sherwood Boehlert (NY)	*Robert Andrews (NJ)*
Dave Camp (MI)	*Benjamin Cardin (MD)*
Lincoln Diaz-Balart (FL)	*Donna Christensen (VI)*
David Dreier (CA)	*Peter DeFazio (OR)*
Jennifer Dunn (WA)	*Norman Dicks (WA)*
Jim Gibbons (NV)	*Bob Etheridge (NC)*
Robert Goodlatte (VA)	*Barney Frank (MA)*
Porter Goss (FL)	*Charles Gonzalez (TX)*
Kay Granger (TX)	*Jane Harman (CA)*
Duncan Hunter (CA)	*Sheila Jackson-Lee (TX)*
Ernest Istook (OK)	*James Langevin (RI)*
Peter King (NY)	*Zoe Lofgren (CA)*
John Linder (GA)	*Nita Lowey (NY)*
Harold Rogers (KY)	*Ken Lucas (KY)*
James Sensenbrenner (WI)	*Edward Markey (MA)*
Pete Sessions (TX)	*Karen McCarthy (MO)*
John Shadegg (AZ)	*Kendrick Meek (FL)*
Christopher Shays (CT)	*Eleanor Norton (DC)*
Lamar Smith (TX)	*Bill Pascrell, Jr. (NJ)*
Mark Souder (IN)	*Loretta Sanchez (CA)*
John Sweeney (NY)	*Louise Slaughter (NY)*
Billy Tauzin (LA)	*Bennie Thompson (MS)*
Mac Thornberry (TX)	
Curt Weldon (PA)	
C.W. Bill Young (FL)	
Don Young (AK)	

and improving the process for sharing intelligence across the different intelligence organizations. The House Select Committee on Homeland Security will initially focus on getting the DHS up and running as quickly and efficiently as possible. It also has legislative jurisdiction over all matters related to the Homeland Security Act of 2002. For example, one of the first acts of the Committee was to address technical corrections to the Act, which the committee held hearings on in March 2003.

The Committee's organizational structure includes five subcommittees: (1) infrastructure and border security; (2) rules; (3) emergency preparedness and response; (4) cyber security, science, and research and development; and (5) intelligence and counterterrorism. During its first few months of activity, the committee has focused primarily on the organizational set-up of each of the DHS directorates, trying to identify budgetary requirements and major issues. Recent hearings covered bio-terrorism, homeland security technology development, lessons learned from the TopOff II homeland security exercise, and the National Critical Infrastructure Strategy.

Of particular interest to the telecommunications community is the work of the Subcommittee on Cybersecurity, Science, and Research and Development. The subcommittee, chaired by Representative Mac Thornberry (R–TX), has legislative jurisdiction and relevant oversight over the security of computers, telecommunications, information technology, and the prevention of injury to civilian populations and physical infrastructure caused by cyber attack.

Congress Continues Efforts to Secure the Nation Through Legislative Activities

Over the past two years, Congress and the Executive Branch have focused heavily on homeland security policy initiatives, culminating in the passage of the Homeland Security Act of 2002 last year.

In 2003, the policy community continues its efforts to secure the Nation by further examining homeland security policies, especially those that would implement the Homeland Security Act, fund homeland security efforts, enable first responders, and enhance cyber security. In coming years, these policies will shape the environment in which the national security and emergency preparedness (NS/EP) telecommunications community will continue to operate.

Homeland Security Act of 2002

The Department of Homeland Security (DHS) recently took steps to implement the *Homeland Security Act* provisions that extend *Freedom of Information Act (FOIA)* and liability protections to critical infrastructure information voluntarily shared with the DHS. These provisions are collectively referred to as the *Critical Infrastructure Information (CII) Act*.

On April 15, 2003, the DHS issued a Notice of Proposed Rulemaking (NPRM): *Procedures for Handling Critical Infrastructure Information (CII)*, which would implement the CII Act's provisions. The NPRM sets specific guidelines for the receipt, care, and proper storage of CII information. These rules will be important for the NS/EP community because they will determine the exact processes and procedures for sharing CII with the DHS and how this information will be protected. The NPRM was open for comment until June 16, 2003.

As the DHS has taken steps to implement the CII Act, Congress has also introduced bills that would modify some of the CII Act's provisions. The bill, S.609, the Restoration of Freedom of Information Act of 2003, was introduced on March 12, 2003, and awaits review by the Senate Judiciary Committee. The House also introduced a companion version, H.R.2526, on June 16, 2003, which was referred to the House Committees on Homeland Security and Government Reform. The two bills protect information from release under FOIA only if:

(1) The provider would not customarily make the record available to the public; and

(2) The record is designated and certified by the provider as confidential and not customarily made available to the public.

A similar provision was included in a Senate bill, S.6, introduced on January 7, 2003, which has been referred to the Senate Judiciary Committee.

The President's National Security Telecommunications Advisory Committee (NSTAC) also addressed the issue of information sharing by reviewing the CII Act and the NPRM, and making suggestions for improving the information sharing process.

Homeland Security Funding

Congress supported increased funding for homeland security efforts. As the Nation went to war in Iraq, the

Legislative Activities, page 22

U.S./U.K., continued from page 17

May 1, 2003, while the U.K. had its Joint Terrorism and Assessment Center.

Secretary Blunkett said the U.S. – U.K. partnership will also seek ways to thwart the threat of cyber and electronic attack, "which would disrupt our commerce."

Secretary Blunkett said that with the help of these two centers, "We can better pull together the information we have from the lessons we have learned in terms of dealing with terror."

The Home Office is the British Government department responsible for internal affairs in England and Wales. According to the Department's Web site, "The [British] Home Office works with individuals and communities to build a safe, just, and tolerant society enhancing opportunities for all and in which rights and responsibilities go hand in hand, and the protection and security of the public are maintained and enhanced."

Secretary Ridge became the first U.S. Secretary of the Department of Homeland Security (DHS) on January 24, 2003, and 22 separate agencies transferred to the new agency on March 1, 2003. The DHS Web site indicates that its, "first priority is to protect the Nation against further terrorist attacks. Component agencies will analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our Nation for future emergencies."

According to the DHS Web site, "Besides providing a better-coordinated defense of the homeland, DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions."

"Cryptoberry" Provides Wireless E-mail Solution for Government

By Major Maryann D'Alessandro,
U.S. Army Reserve
National Communications System

Wireless e-mail access can be achieved over personal data assistants (PDA) such as the Palm Pilot, Pocket PC, and BlackBerry. However, the secure capabilities of these commercial off the shelf (COTS) devices are limited and do not comply with the Department of Defense (DOD) Public Key Infrastructure (PKI) Policy and the DOD Overarching Wireless Policy that govern the use of wireless e-mail by Government workers.

The Secure/Multi-purpose Internet Mail Extension (S/MIME) enhanced BlackBerry product, or "cryptoberry," developed by Research in Motion (RIM), Inc. of Waterloo, Ontario, Canada, is the only wireless device available that provides true writer-to-reader security for wireless e-mail approved to protect up to sensitive but unclassified (SBU)/For official use only (FOUO) e-mail.

With the recent NCS transition to the Department of Homeland Security (DHS), ensuring secure communications throughout our missions is vital. Assuming coverage is available, the cryptoberry devices could provide a solution for secure data communications. Ideally, the BlackBerry Model 5810 which operates over a Global Systems for Mobile Communications/General Packet Radio Service (GSM/GPRS) will incorporate the S/MIME standard to provide secure data and voice communications during operations.

The S/MIME enhanced 957-8MB BlackBerry wireless e-mail solution for Microsoft Exchange is the only device that meets the DOD wireless e-mail standards and is available via a variety of contract vehicles. It is a wireless handheld device powered by an Intel 386 32–bit processor with integrated e-mail/organizer software, optimized keyboard, thumb – operated track wheel, and an easy–to–read screen.

E-mail is sent and received with guaranteed confidentiality, authentication, and data integrity. Users can read, compose, forward, reply, file, or delete messages from the device while maintaining a single, existing e-mail address and mailbox. By setting e-mail filters that monitor key words and message fields, individuals can control which messages they receive on their own devices. The BlackBerry displays 16 or 20 lines of text with a backlight to enable viewing in low-light conditions and includes an integrated wireless modem with a two-watt transmitter. The user is always connected to the network

and never has to dial in, thereby allowing discreet notification as new e-mail arrives.

The S/MIME enhanced device has 1 megabyte (MB) of static random access memory (SRAM) plus 8 MB of flash memory. The upgrade allows the user to send signed or signed and encrypted e-mail in approximately 12 seconds. The S/MIME upgraded device can hold up to approximately 100 certificates and runs on a rechargeable lithium battery with a lifetime of approximately one week when on continuously.

Data sent from a COTS BlackBerry handheld and the BlackBerry enterprise servers are encrypted using United States (U.S.) Government approved, Triple-Data Encryption Standard (DES) algorithm for symmetric encryption/ decryption. The same algorithm is favored by the banking industry to electronically transfer confidential financial data.

No successful invasions on this encryption method have been found; however, this algorithm alone does not meet the DOD requirements, according to Mr. Robert Nowak, a contractor with the National Security Agency's (NSA) Wireless Applications Group at Fort George G. Meade, Maryland. The S/MIME enhanced BlackBerry device provides an extra layer of security using S/MIME encryption. This enhancement incorporates the ability to securely transfer, store, forward, and authenticate messages to ensure writer to reader security and is completely compatible with the DOD X.509 Class 3 PKI. S/MIME encryption of the e-mail message is used in addition to the Triple DES encryption of the wireless network connection.

There are two versions of the COTS BlackBerry: the Internet version and the enterprise edition. The enterprise edition is the only version available with the S/MIME enhanced BlackBerry. A BlackBerry Enterprise Server (BES) is necessary to centralize e-mail redirection and wireless calendar synchronization for all BlackBerry users in an organization. This provides a secure, two-way link between a user's Exchange accounts and a user's BlackBerry handheld device. The server decrypts, then decompresses the message, and should be on the same domain as exchange.

While a dedicated BES is not required, Mr. Nowak said it is recommended for backup, security, and account management purposes. It is possible to use a BES located at U.S. Army Reserve Command for example. The server is only a redirector of messages to and from Microsoft Exchange. It stores no messages and therefore has no access to messaging or organizational information of any kind.

Mr. Nowak highly recommends the purchase of a BES rather than routing e-mail to a remote server to control our own infrastructure. A BES can be purchased for approximately $5,000.00. Another option is to purchase a one-year free upgrade with any BlackBerries purchased, which includes the BES and the maintenance. The upgrade can be purchased for $2,100.00. Mr. Nowak added that since antivirus software is not bundled with the product, it is important to keep it current for the desktop and the systems that host the BES.

There are limitations to consider before purchasing any BlackBerry device. The maximum message size of the standard BlackBerry device is 32K, and additional software is required to add an attachment to a message. The S/MIME device has the same 32K limitation, and currently, NSA has not authorized any third party software to permit attachments from the cryptoberry.

Another limitation is the national coverage of the devices. The United States does not have 100 percent coverage; however, expanded coverage is expected over time as tower owners increase the functionality of their towers and as tower population and dispersion increase. Currently, dead zones should be expected. The cost of one BlackBerry device on the General Services Administration (GSA) schedule is $1250.00, which includes a flat-rate wireless e-mail service for the first year. Follow-on service is $476.00 per device per year. Affiliated Computer Services Defense, Inc., headquartered in Dallas, Texas is the only authorized trusted third party to load S/MIME BlackBerry software for the Government.

The S/MIME enhanced 957-8MB BlackBerry wireless e-mail solution (cryptoberry) for Microsoft Exchange is the only device that meets the DOD wireless e-mail standards and is available via a variety of contract vehicles.

RIM currently does not plan to incorporate a cell phone capability in the BlackBerry 957-8MB. However, the company is developing an S/MIME version of the 5810, which includes cell phone as well as wireless e-mail capability. NSA officials will evaluate this model when the company incorporates the S/MIME capability. The U.S. Army requirements to comply with DOD policy as of this writing are not in place therefore, buyers should comply with the DOD PKI Policy and the DOD Overarching Wireless Policy when making any standard BlackBerry or cryptoberry purchase.

Legislative Activities, continued from page 19

President signed into law on April 16, 2003, the *Emergency Wartime Supplemental Appropriations Act of 2003*, which allowed for additional defense and homeland security spending. The Act included $3.9 billion for the DHS, including funds for an Interoperable Communications Technology Program and for States and localities to improve communications within and among law enforcement agencies.

Assistance to First Responders

Congress is also discussing first responders' issues. The recently passed House version of the Homeland Security Appropriations bill, H.R. 2555, gives $4.4 billion in grants to first responders, a $900 million increase over President Bush's budget request. During the debate, Homeland Security Committee Chairman Christopher Cox (R–CA) announced his intent to introduce legislation that would help overhaul the formula for homeland security grants. States would then receive money based on their threat level instead of on their population. A similar bill, S.1245, was introduced in the Senate on June 12, 2003, and was referred to the Senate Committee on Governmental Affairs. The bill was placed on the Senate legislative calendar on September 5, 2003.

Enhancements to Cyber Security

In other homeland security news, the DHS is increasing its focus on cyber security. On June 6, 2003, the DHS announced the creation of the National Cyber Security Division (NCSD), which is a new office, dedicated to cyber security efforts. Mr. Amit Yoran is leading this new division, which will be housed in the DHS' Information Analysis and Infrastructure Protection Directorate under Assistant Secretary for Infrastructure Protection, Mr. Robert Liscouski. The NCSD will work to identify, analyze, and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning.

Throughout the year, Congress and the Executive Branch will likely continue to engage in policy discussions about homeland security issues, especially as the DHS matures.

As the DHS rules are implemented and new initiatives are established, the NS/EP community would benefit by staying abreast of these developments. These policy initiatives will in turn provide a policy framework in which the NS/EP telecommunications community must operate and a guideline for cooperation.

Dr. McQueary Sworn In as Homeland Security Undersecretary

Dr. Charles E. McQueary became the Department of Homeland Security's Undersecretary for Science and Technology during ceremonies held April 9, 2003, in Washington D.C.

Dr. McQueary, who before assuming his new role was President of General Dynamics Advanced Technology Systems division in Greensboro, N.C., said there were two reasons why he accepted Homeland Security Secretary Tom Ridge's offer to serve.

"First, the opportunity to build the Science and Technology organization held enormous appeal because I had had experience in building successful teams before," said Dr. McQueary. "The second – and perhaps the more important reason – was that this country has provided me with a lifetime of incredible opportunities – and leading the office of Science and Technology would be my great chance to give something back. There can be no doubt that having a role in the development of this vitally important new Department at this particular moment in our great Nation's history is extraordinary. I pledge to you all that I will do my best."

Before his work at General Dynamics, Dr. McQueary served as President and Vice President of business units for AT&T and Lucent Technologies and as a Director for AT&T Bell Laboratories.

Dr. Charles E. McQueary, DHS Undersecretary for Science and Technology

In addition to his professional experience, Dr. McQueary has served his community in many leadership roles – Chair of the Board and Campaign Chair of the United Way of Greensboro; Member of the Board of Trustees of the North Carolina Agricultural and Technical State University; Member of the Guilford Technical Community College President's Chief Executive Officer Advisory Committee; Member of the Board of the World Trade Center North Carolina; Chair for the Action Greensboro Public Education Initiative; and Member of the Board of Guilford County Education Network.

Dr. McQueary holds both a master's degree in mechanical engineering and a Ph.D. in engineering mechanics from the University of Texas in Austin. The University of Texas also named Dr. McQueary a Distinguished Engineering Graduate.

NSTAC R&D, continued from page 13

chain, from systems designers to users, are cognizant of and able to take appropriate actions to ensure trustworthiness;

- **Physical Security:** protecting physical assets, such as facilities, and equipment, from damage, destruction, and/or exploitation; and

- **Integration:** managing and integrating innovative R&D to build trusted tools and systems to support future NS/EP telecommunications infrastructures and applications.

Participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, seven issues regarding the trustworthiness of NS/EP telecommunications and information systems emerged, including:

- ***A strong sense of frustration and urgency.*** Participants noted the R&D Exchange was but one of many conferences and events focused on issues of trustworthiness and security. They commented that each event produced similar results and recommendations, but that action and implementation were fleeting. At the same time, however, they conveyed a strong sense of urgency about trustworthiness topics. Participants agreed that, given the global nature and increasing proliferation of distributed denial of service attacks and computer viruses, grappling with how to prevent and mount effective responses to such types of attacks was a pressing national issue requiring senior-level attention and commitment in industry, Government, and academia.

- ***A need to clarify the definition of NS/EP telecommunications in the post 9/11 world.*** An issue frequently discussed at the event was the changing nature of NS/EP telecommunications. Participants noted the changing threat environment (from Cold War to distributed threats posed by rogue states and international terrorist groups), evolving technologies (from the traditional public switched network to a converged network composed of traditional voice services, wireless services, the Internet), and creation of new Government institutions (the Department of Homeland Security) all generated a need to clarify the meaning of NS/EP telecommunications in the post-September 11 environment. They also agreed that a better understanding of NS/EP telecommunications might serve as a catalyst for and offer a rationale for prioritizing R&D in key security technology areas.

- ***Major challenges on driving technology innovation into NS/EP systems and functions.*** The complexity derives from the lack of an overall system architecture that incorporates trust in each system layer, starting from devices, components, systems software, and working through all the applications layers. Research needs to be vertically integrated across these layers and mechanisms developed to identify and integrate technologies related to trust. Consensus on the unprecedented needs and capabilities indicates a need for rapid prototyping and testbeds to assure the desired integration into future NS/EP systems.

- ***Partnerships are essential for R&D integration.*** Government funding is a critical component to success, but it is not the overriding factor. The most important factor is adopting an R&D strategy that will attract participation from all the technology, industry, and user sectors to drive the integration into the real systems. The challenge is to attract the operations elements of industry to provide resources and assets, including most importantly people, access to real systems, and funding to conduct tests in collaborative and innovative research projects, pilots, and testbeds. Economic incentives need to be created for all sectors to cooperate and interoperate on R&D.

- ***A need to influence business drivers for security.*** Historically, public research was the primary driver for technology innovation and development in the United States. During the Cold War, the research community relied in the main on U.S. Government funding and direction. In the 1990s, however, this model evolved with private funding of research and technology development equaling and exceeding Government investment. Recognizing the shortage of available resources (Government R&D funds and grants, capital investment in industry, budget cutbacks at universities), participants discussed the need to collaborate on ways to stimulate and leverage market forces as a catalyst for developing the next generation of security tools and products.

- ***A need to improve threat definition and analysis and, equally important, identify methods to share and analyze that information to influence R&D.*** Participants agreed that understanding the evolving capabilities and intent of

NSTAC R&D, page 24

NSTAC R&D, continued from page 23

Mr. Phil Lacombe (right), President of the Security Solutions Sector for Veridian, along with Mr. Scott Charney of Microsoft, introduces the Cyber 1 breakout session during the opening plenary session at the President's National Security Telecommunications Advisory Committee (NSTAC) Research and Development Exchange in Atlanta, GA. (Photo by Kiesha Miller)

potential adversaries (nation-states, terrorists, hackers, insiders) was an important element in developing security tools and products that would meet the future needs of industry, Government, and academia. Participants noted that it was crucial to future R&D to develop a baseline of existing telecommunications and computer networks and to invest in enhancements to the Internet that would allow for regular and more real-time monitoring of Internet health, modeling, simulation, analysis, and testing of new vulnerabilities.

•A need to strike a better balance between better engineering of software and hardware with efforts to improve human factors. Participants noted the importance of having a well-trained and educated workforce, consistent and enforced policies, and a better understanding of the motivations and actions of insiders. A concern regularly expressed at the event was that every action taken in one realm (cyber, human factors, physical, integration) had both visible and often hidden impacts on the other.

Copies of the R&D Exchange findings can be obtained from the NSTAC R&D Exchange Website at http://www.ncs.gov/NSTAC/r&d2003.htm.

NSTAC, established by President Ronald Reagan in 1982 by Executive Order 12382, provides industry-based analyses and recommendations to the President regarding policy affecting national security and emergency preparedness (NS/EP) telecommunications. Up to 30 senior executives (usually chief executive officers) from the telecommunictions, information technology, aviation and banking industries – appointed by the President – make up the NSTAC membership. Dr. Vance D. Coffman, Chairman and Chief Executive Officer of Lockheed Martin Corporation, is the current NSTAC Chair.

Combat Cyber Threats, continued from page 16

Mr. Robert Liscouski, the Assistant Secretary of Homeland Security for Infrastructure Protection, will oversee NCSD and Mr. Amit Yoran will serve as the director of the NCSD. With 60 employees, the division is organized around three units designed to:

- Identify risks and help reduce the vulnerabilities to the Federal Government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets;
- Oversee a consolidated Cyber Security Tracking, Analysis, & Response Center, which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cyber security and incident response with Federal, State, and local Governments, private sector, and international partners; and
- Create, in coordination with other appropriate agencies, cyber security awareness and education programs and partnerships with consumers, businesses, Governments, academia, and international communities.

Consistent with law and policy, DHS's NCSD will coordinate closely with the Office of Management and Budget and the National Institute of Standards and Technology regarding the security of Federal systems and with Federal law enforcement authorities, as appropriate. NCSD will leverage other DHS components including the Science and Technology Directorate, the U.S. Secret Service, and the Department's Privacy Officer, as necessary, to support its mission.