National Security and Emergency Preparedness

Telecom News

2003, 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

National Communications System Transfers to Homeland Security Department

By Steve Barrett
National Communications System

After a nearly 40-year relationship with the Department of Defense, the National Communications System (NCS) became part of the Department of Homeland Security during ceremonies held at the Defense Information System Agency's Skyline 7 Auditorium on March 5, 2003.

Lieutenant General Harry D. Raduege, Jr., the NCS Manager since June 2000, passed the NCS colors and responsibilities to Army Major General Bruce M. Lawlor, Chief of Staff for the Department of Homeland Security, who represented Secretary of Homeland Security Tom Ridge. Lt Gen Raduege remains the Defense Information Systems Agency Director (DISA). Pending nomination by the President and confirmation by the Senate, the Homeland Security Department's Undersecretary for Information Assurance and Infrastructure Protection will become the NCS Manager.

In his remarks, Lt Gen Raduege said it is his hope that the NCS will continue to maintain and build upon the synergy the agency has established over a distinguished 40-year history. "The NCS has accomplished each new mission it has received with unmatched excellence and great ability," said Lt Gen Raduege. "It will be no different as they take on their new mission with the Department of Homeland Security. The NCS will continue to demonstrate its great ability as its professional team members identify and assess threats to our homeland, map those threats against vulnerabilities, issue warnings, and provide the basis from which to organize protective measures."

Maj Gen Lawlor, in accepting the NCS colors, said the department is extremely proud that the NCS is part of the effort to defend the homeland. "You are an important and valued member of a new team," he said. "We appreciate your experience, understand your traditions, and acknowledge your

NCS Transfer, page 10

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

President Bush Welcomes Agencies to Homeland Security Department

By Steve Barrett
National Communications System

Stating that America is very grateful to the people who work day and night to protect the Nation, President Bush welcomed more than 20 Federal agencies to the Department of Homeland Security (DHS) during ceremonies conducted at the Ronald Reagan International Trade Center on February 28, 2003.

"[March 1] marks an historic day for our Government and for our country," the President said. "Around 170,000 people from more than 20 Federal agencies will officially join the new Department of Homeland Security, creating a more effective, organized, and united defense of our homeland. Every member of this new department accepts an essential mission to prevent another terrorist attack. Yours is a vital and important step in reorganizing our Government to meet the threats of a new era as we continue the work of securing this country."

The President said the agencies joining the department – including the nearly 100 members of the National Communications System – will retain their longstanding responsibilities in addition to their new responsibilities. "Each agency, with its own proud and honored tradition, will also gain a new mandate and must adopt a new mind set," said President Bush. "We created this Cabinet department in a time of war. Every professional in the Department of Homeland Security plays a valuable role in winning the first war of the 21st century."

Acknowledging that there is no such thing as "perfect security," the President told the audience of nearly 400 Federal workers that he is determined to do everything in his power to defeat this enemy and to defend our people against the hidden network of cold-blooded killers. "The world changed on September 11, 2001," said President Bush. "We learned that a threat that gathers on the other side of the earth can strike our own cities and kill our own citizens. It is an important lesson, one that we must never forget. Oceans no longer protect America from the dangers of this world. We are protected by daily vigilance at home, and we will be protected by resolute and decisive action against threats abroad."

The President detailed the tasks the new department will handle in protecting the homeland. The department is charged with analyzing the vulnerabilities of the Nation's critical infrastructure, from dams to banks to seaports, and will move quickly to take protective action. In meeting this responsibility, the President said DHS will partner with the new Terrorism Threat Integration Center that will integrate and analyze all threat information collected domestically and abroad in a single location. When fully operational, the President said the center will fully house a database of known and suspected terrorists that officials across this country will be able to access and to act upon.

The President is also tasking DHS with strengthening the country's defenses against

President George W. Bush delivers remarks to new employees of the U.S. Department of Homeland Security at the Ronald Reagan Building and International Trade Center in Washington, D.C., Friday, February 28, 2003. (White House photo by Paul Morse)

cyber-terrorism and the even greater dangers of biological, chemical, or nuclear weapons. To tackle this tasking, the President nominated Dr. Charles McQuerry to establish a science and technology directorate within the department to develop and deploy the technologies for detecting weapons of mass destruction. "As these technologies are deployed, border inspectors will have better tools to intercept dangerous materials before they enter our country," said President Bush. "Emergency services personnel will be able to identify biological or chemical weapons and agents so they can use the most effective decontamination methods available."

Noting that America's enemies can strike anywhere in the country, the President said DHS would also promote cooperation between the Federal Government and state and local governments. "Through the Homeland Security Advisory System, we have created a unified process for alerting Government officials and the public of current threats," said the President. "We are also providing more information about suspected terrorists to state and local law enforcement agencies. With this new department, state and local officials will now have a single point of contact to help them address the needs of the local area."

Another concern is safeguarding border and transportation systems. Acknowledging that September 11th taught the Nation that terrorists will try to use the country's openness against it, the President said the department is working to understand and correct vulnerabilities, and to better track those entering and exiting the country. To strengthen that effort, the President said the Transportation Security Administration (TSA) is assigning thousands of air marshals to commercial flights and deploying more than 50,000 newly trained airport screeners. "TSA is also screening all checked luggage at our airports – up from 5 percent before September 11, 2001," the President said.

Four different organizations that patrol and enforce laws at the borders will be integrated into a new Bureau of Customs and Border Protection. "This bureau will unify border inspection and enforcement functions," said the President, "so that legitimate visitors and goods can enter the United States, while giving us better tools to help deny entry to terrorists, drug traffickers, and dangerous materials."

Over the past 18 months, the President said the Nation has significantly enhanced the national stockpile of critical drugs, vaccines, and other medical supplies. He said supplies from this stockpile can be delivered wherever they are needed, anywhere in the country, within 12 hours. He also said the country has provided more than $900 million in support to help state and local responders and emergency managers prepare for terrorist attacks.

President Bush concluded that the Nation has both great challenges and advantages in securing the homeland. "We have people like you all who serve with skill and, frankly, do not get enough credit for the work you do," he said. "We have brave and honorable men and women serving in our military, including the Coast Guard, ready to accomplish any mission they are given. They will do so with courage, skill, and honor. Above all, we have the courage and character of the American people who are resolved to prevent further attacks on our homeland."

Ridge Confirmed as First Secretary of Homeland Security

By Steve Barrett
National Communications System

Thomas J. Ridge, the former Governor of Pennsylvania who returned to Washington in 2001 to lead President Bush's homeland security efforts, became the Nation's first Secretary of Homeland Security on January 24, 2003, during ceremonies held at the White House.

With the President by his side, Secretary Ridge took the oath of office administered by Vice President Richard Cheney. Secretary Ridge becomes the leader of the Federal Government's 15th executive department and will direct over 170,000 Federal workers tasked with protecting their fellow Americans.

The Department of Homeland Security will lead a comprehensive and unified effort to defend the country by analyzing threats, guarding the Nation's borders and airports, safeguarding critical infrastructure, and coordinating the Nation's response to future emergencies. Part of that effort will come from the National Communications System (NCS), which joined the new department on March 1, 2003. The NCS is located within the Department's Information Assurance and Infrastructure Protection (IAIP) Directorate.

As President George W. Bush watches, Vice President Richard Cheney swears in Tom Ridge as the Secretary of the Department of Homeland Security in the Cross Hall on January 24, 2003. Secretary Ridge's wife, Michele, and children, Tom and Lesley, hold the Bible during the administering of the oath. (Photo by Paul Morse at the White House.)

The President said he knew immediately that Secretary Ridge was the right man for the assignment. "[Secretary Ridge] is a decisive, clear-thinking executive who knows how to solve problems," said President Bush. "The American people can be certain that the mission of homeland security will be carried out with focus and resolve, with the resources the task requires. The American people can know, as well, that the department is under the command of a superb leader who has my confidence."

Secretary Ridge was twice elected Governor of Pennsylvania, serving from 1995 to 2001. He grew up in Erie, Pennsylvania, attended Harvard University on a scholarship, and received his undergraduate degree with honors from Harvard in 1967. Soon after graduation he postponed his academic career at Dickinson Law School to begin a combat tour in Vietnam, where he earned a Bronze Star for Valor.

After returning to civilian life, Secretary Ridge received his law degree from Dickinson in 1972 and went on to serve as an assistant district attorney before his first Congressional bid in 1982. He became the first Vietnam combat veteran to win a seat in the House of Representatives and was re-elected by an overwhelming majority six times before he left for the Pennsylvania Governor's mansion in 1995.

England, Hutchinson Confirmed

In addition to Secretary Ridge's confirmation by the U.S. Senate, two other Homeland Security Department nominees received Senate approval. On January 24, 2003, the Senate confirmed Asa Hutchinson as the Nation's first Under Secretary of Homeland Security for Border and Transportation Security and then approved the nomination of former Secretary of the Navy Gordon England as the Deputy Secretary of the new department on January 30, 2003.

Secretary England served as executive vice president

of General Dynamics Corporation from 1997 until 2001, when he accepted President Bush's nomination to become the Navy Secretary. Previously, Secretary England served as Executive Vice President of the Combat Systems Group, President of General Dynamics Fort Worth aircraft company (later Lockheed), President of General Dynamics Land Systems Company, and as a principal at a mergers and acquisition consulting company.

Secretary Ridge's top deputy also served as the Chair of the Defense Science Board and participated in a broad range of subjects dealing with the U.S. military and the industrial base.

Secretary England is active in a variety of civic and charitable organizations, including Goodwill International, where he served as Vice Chairman of the Board of Directors; the United Service Organizations' (USO) Board of Governors; and as a member of the board of visitors at Texas Christian University (TCU) and other universities.

A Baltimore native, Secretary England graduated from the University of Maryland in 1961 with a bachelor's degree in electrical engineering. In 1975, he earned a master's degree in business administration from the M. J. Neeley School of Business at Texas Christian University. He is a member of the following honorary societies: Beta Gamma Sigma (business), Omicron Delta Kappa (leadership) and Eta Kappa Nu (engineering).

Under Secretary Hutchinson will be responsible for securing the Nation's borders, ports, waterways, and transportation systems. He will oversee the functions now housed in agencies like the Immigration and Naturalization Service, the U.S. Customs Service, the Transportation Security Administration, and the Office for Domestic Preparedness.

"In our mission to protect America, we face the daunting challenge of improving border and transportation security, while at the same time facilitating the unimpeded flow of legitimate commerce and people across our borders and ports," said Secretary Ridge. "In his career, Asa Hutchinson, has demonstrated that he is up for big challenges. I congratulate him on his confirmation and look forward to working with him in this new mission."

Lieutenant General Winston D. Powers, Former NCS Manager, Dies

Air Force Lieutenant General Winston D. Powers, who completed his 37-year career as the Manager of the National Communications System (NCS) and Director of the Defense Communications Agency (DCA) from September 1983 to May 1987, died on February 5, 2003, in Northern Virginia. He was 72.

Funeral services were held on Tuesday, February 25, 2003, at the Fort Myer Post Chapel, followed by burial in Arlington National Cemetery.

General Powers, who retired from the Air Force following his NCS/DCA assignment, served as the seventh Manager of the NCS, succeeding Army Lieutenant General William J. Hilsman. He was also eighth director of the DCA – the forerunner of the Defense Information Systems Agency.

His military career began in 1950 as a 19-year old enlisted airman, and he served in a variety of assignments during his career. Prior to becoming the NCS Manager and DCA Director, General Powers commanded the Space Communications Division at Peterson Air Force Base, Colorado. While at Peterson, he also served as Chief of the Systems Integration Office, Headquarters, and Aerospace Defense Center; and Deputy Chief of Staff for Communications, Electronics, and Computer Resources for the North American Aerospace Defense Command and Aerospace Command.

During his career, General Powers received the Distinguished Service Medal, the Legion of Merit, the Meritorious Service Medal with two oak leaf clusters, the Air Medal with oak leaf cluster, and the Air Force Commendation Medal. He also accumulated over 4,000 flyer hours as a master navigator.

Lieutenant General Winston D. Powers, Former NCS Manager (Photo by Defense Information System Agency)

General Powers is survived by his wife, Jeanette, his daughter Diane (Powers) Nock, her husband Robert Nock and two grandchildren, and his son, Lieutenant Colonel Winston David Powers.

NCS Deploys Initial Wireless Priority Capability

By Steve Barrett
National Communications System

The first step toward a nationwide wireless priority service for national emergencies is now in place.

On January 13, 2003, the National Communications System (NCS) announced the implementation of the Wireless Priority System (WPS) to areas of the Eastern United States which it plans to expand to a full nationwide capability through 2003.

A limited WPS service has been operational in the Washington, DC and New York metropolitan areas since May 2002. The initial nationwide capability is now available in both New York City and Washington DC, as well as in metropolitan areas surrounding Atlanta, GA; Birmingham, AL; Boston, MA; Jacksonville, FL.; Louisville, KY; Memphis, TN; Miami, FL; Mobile, AL; Nashville, TN; New Orleans, LA; Norfolk, VA; Philadelphia, PA; and Richmond, VA. Additional markets will be added nationwide over the next few months, as will further enhancements to the capability.

T-Mobile signed a contract on January 10, 2003, with the NCS through DynCorp, its Government Emergency Telecommunications Service (GETS) and Wireless Priority integration contractor, the initial carrier for the WPS service.

"We are very excited and proud that we now have the initial capability to provide the Nation's leaders, first responders, and key critical infrastructure personnel with wireless priority communications during periods of emergency," said Mr. Brenton C. Greene, Deputy Manager, NCS.

"We've worked hard withT-Mobile and all of our industry partners to develop a program that meets the President's request for an emergency wireless communications service. This is a major first step."

Mr. Greene indicated there are more steps to take and more telecommunications partners that will be involved in expanding WPS to cover the entire country. "T-Mobile is the first of what we hope will be a full slate of major wireless carriers ready to step up and support WPS nationwide," said Mr. Greene. "We are also working very hard to secure the funding and complete the work that will allow us to reach a full operating capability of WPS by the end of 2003."

"WPS is an important capability for U.S. NS/EP [national security and emergency preparedness]," said Mr. Gary Jones, Director of Standards Policy for T-Mobile. "The NCS, the FCC [Federal Communications Commission], and others in the Administration and Congress have worked hard to make WPS a top priority and to ensure it was implemented as soon as possible. With the initial stage of Nationwide WPS operational before the end of 2002, great progress has been made. T-Mobile is pleased to have been awarded a nationwide WPS contract, and we know that [WPS] is a capability that national security and emergence preparedness officials want and will adopt quickly."

"We've worked hard with T-Mobile and all of our industry partners to develop a program that meets the President's request for an emergency wireless communications service. This is a major first step."

NCS officials predict that within the next 2 years, there will be as many as 50,000 WPS users in the country, depending on carrier capacity. Mr. John Graves, program director for the GETS and the NCS manager for the WPS implementation, said that the number of users will increase as more carriers accept contracts to provide the service.

WPS is available only to designated leadership at all Government levels: national security personnel, emergency responders, and private sector critical infrastructure leaders and decision makers, as approved by Federal Communications Commission Rules and Requirements and the NCS. Further, WPS has been designed to have negligible

impact on regular cellular users, providing priority access to vital decision makers without restricting the public's ability to gain access to those same networks.

Mr. Graves said the NCS and its industry team designed the WPS capability to have minimal impact (about two percent) on normal consumers using cellular networks. He said this would balance emergency priority use and public customer access. The NCS hopes to add other global systems for mobile communications (GSM) carriers – such as AT&T Wireless, Cingular, and Nextel – in the near future. Plans also include adding code division multiple access (CDMA) carriers such as Verizon Wireless and Sprint PCS as soon as funding allows.

When trying to make a call in times of emergency or natural disaster, NS/EP users will have the ability to gain priority access to the next available cellular channel to place their call. Authorized users with T-Mobile WPS access need only dial *272 and then their destination numbers. Mr. Graves said this service would greatly enhance a caller's ability to complete wireless calls during critical times and communicate vital decisions and reports during emergency situations.

In concept, WPS is an extension of GETS, the NCS emergency communications program that currently provides wireline priority service to more than 70,000 users. Under GETS, eligible users with GETS calling cards can call a designated access number, input their GETS personal identification number, then dial the number they need during an emergency. Users would then receive "priority queuing" on the public network – a process that gives emergency responders the first available phone line without pre-empting calls already in progress.

GETS – available to eligible users since 1995 – saw its greatest success in the events following the September 11th attacks, during a time when the program was reaching full operational capability. Of the thousands of GETS calls attempted by national leaders and emergency responders, over 95 percent were completed on the first attempt.

"The goal is to provide emergency responders with priority access with a variety of standards that support a common goal – successfully completing emergency calls during an emergency. We believe all wireless carriers – GSM and CDMA – have a vital role in making wireless priority service a success."

Future Funding

Mr. Graves said the Federal Government is funding the initial WPS capability, with a small amount being funded through service charges with participating carriers. Money for the T-Mobile contract award originated from emergency funding following the September 11th attacks and has gone to research, development, and deployment of initial capabilities.

However, future funding for development and deployment of the full WPS operational capabilities was put in doubt last October when a Senate-House conference committee "zeroed-out" the NCS request for $73 million for WPS from the fiscal year 2003 Defense Appropriations Bill. With the NCS now moved to the Department of Homeland Security as of March 1, 2003, the WPS initiatives for fiscal year 2003 will rely on whether the NCS can obtain funding in the new department's budget.

Mr. Graves said the clock is ticking to obtain that funding, adding that funding cuts mean delays in the software development necessary to bring more carriers on board, as well as increased upgrades to begin the coast-to-coast full operating capabilities by the end of the year.

Although funding restrictions are delaying the CDMA development, Mr. Graves insists that WPS remains open and ready to develop CDMA technology for the WPS. "We've said all along that we want to have as many wireless carriers participating in the program as possible," said Mr. Graves.

"The goal is to provide emergency responders with priority access with a variety of standards that support a common goal – successfully completing emergency calls during an emergency. We believe all wireless carriers – GSM and CDMA – have a vital role in making wireless priority service a success."

New Members Named to NCS Council of Representatives

By Steve Barrett
National Communications System

Four Federal organizations of the National Communications System (NCS) member organizations have named new members to the NCS Council of Representatives (COR).

The new members are Mr. Paul B. Maison from the Federal Emergency Management Agency (FEMA), Mr. Kenneth Moran of the Federal Communications Commission (FCC), Ms. Anne E. Paulin of the Federal Reserve Board, and Mr. Gilbert Nolte of the National Security Agency (NSA).

The NCS Council of Representatives is the subordinate body of the Committee for Principals (COP). As the working group of the COP, the COR meets to consider national security and emergency preparedness (NS/EP) communications initiatives, study critical NS/EP areas, and provide reports to the COR for consideration.

Mr. Maison is a telecommunications management specialist working for the FEMA's Homeland Security Coordination Office. He also serves as FEMA's NS/EP telecommunications observer to the National Association of State Telecommunications Directors (NASTD), National Emergency Number Association (NENA), and the Association of Public Safety Communications Officers, Inc. (APCO).

In replacing Dr. Joseph Massa at FEMA, Mr. Maison is returning to the COR – he first served as the FEMA representative to the NCS from October 1989 to January 1995. Mr. Maison also serves on the Telecommunications Service Priority (TSP) Oversight Committee and on various NCS working groups defining and resolving NS/EP information systems issues.

Mr. Moran is the Director, National Defense and Security in the FCC's Office of Engineering and Technology. He is responsible for developing Commission policies on defense, emergency preparedness, intelligence, law enforcement, and telecommunications network protection and reliability.

Mr. Moran, replaces Mr. Douglas Kyle as the FCC COR member.

Ms. Paulin is a senior member of the Federal Reserve Board's Information Technology section, which has oversight responsibility for information technology planning and acquisitions within the Federal Reserve System. She is the section's primary analyst for Federal Reserve telecommunications and network planning efforts. In addition, she is responsible for leading projects related to oversight of Federal Reserve information security and disaster recovery planning.

Mr. Nolte is assigned to the NSA's Information Assurance (IA) Directorate – leading a highly technical organization to design, develop, produce, and deliver IA solutions for the U.S. Government, its allies, and coalition partners. He replaces Mr. Michael Green as the NSA COR.

The NCS consists of 23 Federal departments and agencies that assist the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget in the coordination of planning and provisioning of NS/EP communications for the Federal Government.

NCS, Canadian Representatives Tackle SNMP Issue

By Jacqueline Cookston
National Communications System

For over 14 years, the National Communications System (NCS) and its Canadian counterpart, Industry Canada, have benefited from their emergency telecommunications relationship. This relationship has helped both the United States and Canada to react to many natural disasters from the January 1998 ice storms that ravaged areas of Canada and New England to the December 1998 four-day storm that caused excessive flooding in many areas of the Pacific Northwest.

Recently, the NCS and Industry Canada expanded their cyber-related efforts, gathering information regarding a recent vulnerability discovered in the transmission of information across the Internet. In February 2002, the National Infrastructure Protection Center (NIPC) released an alert notifying the public that the Oulu University in Finland had reported multiple vulnerabilities in the Simple Network Management Protocol (SNMP). SNMP is the most popular protocol used to manage many core network devices, such as routers, switches, hubs, bridges, and wireless network access points. SNMP is a standard that transports information between these networked devices, but encoding errors were found throughout the SNMP code, leaving network elements vulnerable to the insertion of malicious code.

Due to years of planning and operational cooperation and the fact that SNMP was not a problem that could be solved by the United States alone, discussion between the United States and Canada was initiated to determine what level of collaboration could be attained to promote an effective partnership to combat this threat. Mr. Bernie Farrell, Manager of the National Coordinating Center for Telecommunications (NCC) in the NCS, spoke with Mr. Jan Skora, Director General, Radio and Broadcasting Regulations, Industry Canada and discussed options for sharing information on the vulnerability.

For SNMP operations, collaborative options included using encrypted e-mail, since the nature of the threat and response activities were extremely sensitive in the early response stage, conducting meetings, and detailing someone from Industry Canada to the NCC to be the conduit between Canada and the United States and to assist the NCC team as needed.

Mr. John Kluver, Emergency Telecommunications Officer, Industry Canada, volunteered to work in the NCC for a number of weeks and to work with the NCS on the SNMP vulnerability. The placement of a member of the Canadian Government within the NCC for an extended period of time represented an unprecedented step between the two countries. Over the years, there had been many meetings and much correspondence between Canada and the United States; however, never before had someone from another country physically worked in the NCC. Previously, the planning and operational interfaces created to monitor the "Year 2000 (Y2K)" rollover represented the closest partnership the two countries had forged.

Industry Canada is an agency within the Canadian Government responsible for supporting and developing business and the economy in Canada and can be compared to the U.S. Department of Commerce. It is led by a Minister, Mr. Allan Rock, and a Deputy Minister and comprises several departments including Policy, Telecommunications, Consumer Advocacy, and Industry Sector Development. At the onset of the e-commerce age, the Department of Communications within the Canadian Government merged with Industry Canada. This makes Industry Canada the most appropriate agency within the Canadian Government to work directly with the NCS on emergency

SNMP Issue, page 18

NCS Transfer, continued from page 1

incredible achievements over the past 40 years."

When the Office of Homeland Security began writing the plan that lead to the creation of the department, Maj Gen Lawlor said they thought about how they could link intelligence and critical infrastructure within a new organization. He said the department wanted an organization that could look at intelligence threats, assess vulnerabilities in critical infrastructure, identify those infrastructures that are most important, identify the security gaps, and propose and implement solutions. The department also wanted an organization that could inspire confidence in the private sector to collect and protect the information needed to accomplish this kind of mission.

He said the NCS quickly surfaced. "As we struggled to think about this new directorate, we found that what we were thinking about was not so new at all – that the NCS had been doing it for some time and doing it magnificently," he said. "We sought out the NCS as a model for how we might take what you have done and implement it across all 14 sectors of critical infrastructure that exist across the country. We also remembered what happened after 9-11 and we remembered your magnificent efforts of putting back into operation the communications systems that serve as the engine that drives this country."

Maj Gen Lawlor also cited the NCS accomplishments with the President's National Security Telecommunications Advisory Committee (NSTAC) – a model for industry/Government partnership in establishing national security and emergency preparedness communications. "With the NSTAC, you have created an unmatched standard of integrity that generates trust between the public and private sectors to look at critical infrastructures for the good of the country," he said.

Lieutenant General Harry D. Raduege, Jr., who became the Manager of the National Communications System (NCS) in June 2001, passes the NCS colors and responsibilities to Army Major General Bruce M. Lawlor, Chief of Staff for the Department of Homeland Security, during ceremonies held March 5. The ceremony marked the transfer of Executive Agent responsibilities from the Department of Defense to the Department of Homeland Security. (Photo by Donald W. Jordan, Defense Information Systems Agency.)

Maj Gen Lawlor said the department is committed to sustaining those NCS achievements, to moving forward, and to making the next 40 years as great as the first 40. "We look forward to your experience, your commitment, your sense of mission, and your professionalism, and we look forward to helping you help us," he said.

In his last action prior to transferring the NCS, Lt Gen Raduege presented a Joint Meritorious Unit Award to the NCS, and then attached the award streamer to the NCS colors. The award cited the NCS and DISA for "exceptional meritorious achievement" from September 11, 2001, to December 31, 2001, when the NCS "…consistently

displayed super leadership skills, managerial talent, and technical expertise, directly contributing to the overwhelming success of operational forces during the conduct of operations to assure homeland security, overthrow the Taliban regime, and liberate Afghanistan as part of the war on terrorism."

Although the transfer from the Department of Defense to the Homeland Security Department is complete, the NCS will remain at its current site – co-located with the DISA headquarters in Arlington, VA – until further notice. The NCS continues its mission of developing, deploying, and coordinating emergency communications with the Nation's telecommunications and information technology companies.

Established in 1963 by President John F. Kennedy to assure national telecommunications survivability following the Cuban Missile Crisis, NCS programs and activities currently include the Government Emergency Telecommunications System (GETS) and Telecommunications Service Priority (TSP) Programs – two programs successfully used by NS/EP officials during the September 11 attacks in New York City and Washington, DC. A recent NCS initiative – and a result of the September 11 attacks – is the initial deployment of a nationwide Wireless Priority Service (WPS), now available in 15 geographic areas. The NCS plans to expand this service across the country by the end of the year.

The NCS also runs the National Coordinating Center for Telecommunications (NCC) and its Telecommunications-Information Sharing and Analysis Center (ISAC), where telecommunications industry representatives from the Nation's major telecommunications companies and Government work together to coordinate emergency telecommunications response efforts following national crises, including natural disasters and terrorist events.

In addition to its programs, the NCS manages the activities of two major telecommunications committees. The NCS Committee for Principals (COP) – chaired by the NCS Manager – consists of representatives from each of the 23-member NCS Government agencies. The COP and its subordinate Council of Representatives currently addresses emergency communications issues and provides guidance and advice to the Executive Office of the President.

The other, the President's NSTAC, is a Federal advisory committee up to 30 executives from the telecommunications, information technology, banking, and aerospace industries. Created in 1982, the NSTAC provides advice and expertise to the President on a variety of emergency telecommunications issues – such as the creation of the NCC and its Telecom ISAC – and concerns pertaining to protection of the Nation's critical telecommunications infrastructure.

More information on the NCS can be obtained from its Web site at http://www.ncs.gov.

Mr. Brenton C. Greene (right), Deputy Manager of the National Communications System (NCS), accepts the citation for the Joint Meritorious Unit Award from Lieutenant General Harry D. Raduege, Jr., during March 5 ceremonies transferring the NCS from the Department of Defense to the Department of Homeland Security. (Photo by Donald W. Jordan, Defense Information Systems Agency.)

Science and Technology Key to Administration's Commitments

Courtesy of the Department of Commerce

During 2002, the Bush Administration and the U.S. Department of Commerce (DOC) were focused on the priorities of economic and homeland security and enacting the President's agenda for a safer, stronger, and better America.

"Science and technology have played essential roles in improving the economic and homeland security of all Americans," said Commerce Secretary Don Evans. "The Department of Commerce has furthered the President's call to marshal the Nation's technology resources to help the United States win the war on terrorism, strengthen homeland protections, revitalize the economy, and create new jobs."

"Technology remains an important and vibrant part of our lives and our economy," said Mr. Phil Bond, Under Secretary of Technology and Chief of Staff. "This Administration, and the DOC Technology Administration [TA] especially, remain committed to supporting policies that foster innovation, support research and development, and improve the quality of life for all Americans."

The Bush Administration has led the way in promoting innovation and competition – a few accomplishments include:

Increased Market Access. Signed legislation to grant the President Trade Promotion Authority – opening new markets for U.S. made products.

Promoted Research and Development (R&D). The President signed into law the largest Federal R&D budget in history and proposed broadening and making permanent the research and experimentation tax credit.

Enhanced Economic Security. Signed into law an economic security package that will speed depreciation schedules. Deploying the advanced telecommunications equipment and technologies needed for the high-speed Internet is capital intensive. Companies are more likely to make these important investments if they can depreciate the capital costs associated with broadband rollout over a shorter time period.

Expanded E-Government. The President signed H.R. 2458, the "E-Government Act of 2002." The Act, which builds on the President's E-Government initiative, will assist in expanding the use of the Internet and computer resources in order to deliver Government services.

The DOC's TA continues to serve as a portal to the technology community:

Promoted Homeland Security. The DOC TA hosted the first-ever Homeland Security Tech Expo that featured over 300 American inventors, small innovation companies, and large corporations from 36 states.

Lead the Homeland Security Effort. In 2002, National Institute of Standards & Technology (NIST) launched a major building and fire investigation into the collapse of the three World Trade Center buildings. NIST also issued a series of guidelines to help Federal agencies and the private sector improve the security of our information systems and critical infrastructures.

Fostered Broadband Deployment. The DOC continues to foster the development and rapid deployment of new technologies. The TA led a series of discussions with industry and consumer groups to promote effective and balanced approaches to digital rights management as part of a larger effort to understand the demand for broadband technologies and promote applications to stimulate deployment.

The National Telecommunications and Information Administration (NTIA), the U.S. Patent and Trademark Office (USPTO), the Bureau of Industry and Security (BIS), and the Economic Development Administration (EDA) have all been key leaders in the Administration's technology initiatives:

Enhanced Ultra Wideband Technology. The NTIA completed a technical study on ultra wideband technology that helped lay the foundation for the introduction of a promising, new communications technology that has the potential to save lives and create new jobs for Americans.

Increased Radio Spectrum. The NTIA issued a landmark plan to make more radio spectrum available in the future for deployment of advanced mobile (third generation) telecommunications services to meet an anticipated consumer demand for new wireless services in the next decade and beyond.

Modernized the Patent Office. The USPTO unveiled a revolutionary 21st Century Strategic Plan to make USPTO a quality-driven, information age, market-oriented, e-commerce based organization by 2008. This included a dramatically accelerated electronic Government in the processing of patent and trademark applications.

Increased Tech-Centered Economic Development. The EDA awarded $6.4 million, its largest economic investment ever under the Bush Administration, to Oakland Base Reuse Authority, Advancing California's Emerging Technologies (ACET) and California State University at Hayward, Alameda, California. The investment will become the nucleus of technology-led economic development in Alameda and Oakland, creating hundreds of jobs in the East Bay Region of the San Francisco Bay Area.

Established Bilateral High-Tech Trade. The BIS established a U.S.-India High Technology Cooperation Group composed of senior government officials of both countries. The group will develop a statement of principles governing bilateral cooperation in high-technology trade.

Incompatible Information Systems Pose a Homeland Security Challenge, White House Info Czar Says

By Gerry J. Gilmore
American Forces Press Service

According to Mr. Lee Holcomb, Director for Information Structure in the White House Office of Homeland Security, sorting through and integrating different computer information systems from the 22 agencies transferring to the new Department of Homeland Security (DHS) presents "a challenge" as these agencies will bring a variety of disparate, separate databases with them.

Prior to the September 11, 2001, terrorist attacks on America, a number of Federal agencies had developed technologies and systems to function within an agency setting, but in many cases did not address information sharing between the systems across multiple agencies," Mr. Holcomb said. "Such advanced capability," he added, "is a mandatory asset for the new DHS."

Many existing databases operated by DHS-designated agencies and systems administered by other organizations expected to work closely with the Homeland Security Department are currently "not mutually accessible," Mr. Holcomb added.

Additionally, he noted that much of the communications equipment now used by civic emergency first responders such as police, fire, and rescue workers, is either outdated or incompatible with Federal gear.

"In many cases, police officers are operating 1970s analog radios," Holcomb said. Such discrepancies will be solved, he emphasized, by testing and selecting a model emergency-response setup, complete with modern, interoperable communications equipment.

Under a key initiative called Project Safecom, Mr. Holcomb noted that firefighters, police officers, and emergency medical technicians will gain the ability to communicate quickly and seamlessly to help preserve life and property during a disaster. "It is very critical that we are giving them the tools they need to protect communities to the maximum extent possible," Mr. Holcomb said.

NS/EPC Addresses Critical Infrastructure Issues

Highlights of the September 25, 2002, meeting of the Committee for National Security and Emergency Preparedness Communications (NS/EPC), included new emergency telecom pilot program, cyber and physical security of the Nation's cyber assets, and updates on the National Coordinating Center for Telecommunications (NCC) Information Sharing and Analysis Center (Telecom-ISAC), and the National Communication System (NCS) transition to the Department of Homeland Security (DHS).

The NS/EPC provides advice and recommendations to the President on critical emergency telecommunications issues. Chaired by the Manager of the NCS—the NS/EPC consists of senior telecommunications officials representing 22 Federal departments and agencies.

Emergency Notification System: Alerting the Public in Times of Crisis

The ability for national security and emergency preparedness (NS/EP) leaders and public safety officials to communicate in times of national crisis is crucial. It is equally important that the general population be informed of crisis information as well. The NCS is developing a national system to provide emergency notification or alerts to the general public.

Known as the Emergency Notification Service (ENS), the program is designed to facilitate interoperability across existing systems, provide for data collection across infrastructures, and use multiple communication technologies for notification.

Mr. Dale Barr, who is heading the ENS program out of the NCS Technology and Programs Division, briefed the NS/EPC members on the pilot program now underway. "The pilot program will include approximately 2,000 ENS users within three target areas," Mr. Barr stated, "providing a two-way link to other alerting systems technologies."

"Eventually," Mr. Barr confirmed, "the ENS notification will include approximately 2,000-6,000 critical NS/EP personnel at the top levels of Government as well as between 50,000-250,000 Federal, State, and local government and other public health and safety personnel. Individuals and organizations will be identified for ENS, including Federal operations centers, States, and appropriate NS/EP individuals."

Mr. Barr told the NS/EPC that there are three phases for the ENS Pilot. The first phase was recently completed user trial with a limited number of test users. The second phase expands the number of users to 2,000 in three target areas. The third phase will add capabilities based on needs and early pilot experiences. These phases will be completed between October 2002 and October 2003.

"ENS notification will include approximately 2,000-6,000 critical NS/EP personnel at the top levels of Government as well as between 50,000-250,000 Federal, State, and local government and other public health and safety personnel. Individuals and organizations will be identified for ENS including Federal operations centers, States, and appropriate NS/EP individuals."

National Strategy to Secure Cyberspace

Mr. Marcus Sachs, Director for Communication Infrastructure Protection, Office of Cyberspace Security, briefed the NS/EPC on the National Strategy to Secure Cyberspace. Mr. Sachs discussed the protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support these systems.

Mr. Sachs noted, "The Office of Cyberspace Security issued the initial draft of the National Strategy in September and asked members of the Federal Government and the general public for comments and

recommendations." The NCS, the NS/EPC, and the President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee provided comments and recommendations to the NCS concerning the strategy.

Telecom-ISAC: Sharing Information to Mitigate National Threats

NS/EPC members received a briefing from Mr. Bernie Farrell, Manager of the NCC on the Telecom-ISAC. He announced that several new members joined the ISAC since the last briefing to the NS/EPC, including the Cellular Telecommunications and Internet Association (CTIA), Motorola, and the Federal Reserve Board.

The Telecom-ISAC supports Executive Order 12472 and national Critical Infrastructure Protection (CIP) goals by facilitating voluntary collaboration and information sharing. In addition, it gathers information on telecommuncations vulnerabilities, threats, intrusions, and anomalies from multiple sources, and performs analyses to avert or mitigate any impact upon the telecommunications infrastructure. The NCC Watch and Analysis Operation, staffed by senior level information assurance analysts, operates around-the-clock. In addition, it is developing the requirements and design for the Global Early Warning System (GEWIS), a cyber warning tool that monitors the performance of the Internet and provides warnings to industry and Government users of threats that could degrade services. "The center processes a great deal of information sharing traffic that requires analysis and assimilation." Mr. Farrell stated, "The Watch Daily Analysis leverages available data sources and on-site talent to analyze suspected malicious logic, tools, and exploit methodologies as well as to monitor specialized sites."

NCS in Transition: Moving to the Department of Homeland Security

As the NCS maintains and builds upon its current programs it is also preparing for its role in the DHS. During the September 25 NS/EPC meeting, Mr. Frank Cilluffo, the Special Assistant to the President for the Office of Homeland Security (OHS) and Executive Director of the President's Homeland Security Advisory Council, provided an update on activities pertaining to the establishment of the new DHS. "This has been an extraordinary undertaking because it is the first time since 1947 that the President has created such a Department in the Executive Branch," he said. The OHS identified Federal and State partners as well as other stakeholders who could participate in developing an improved national security strategy.

As a follow up to Cilluffo's presentation, NCS Deputy Manager, Mr. Brenton C. Greene, presented an update on the transition of the NCS to the DHS. He stated that Government agencies and departments began meeting months ago to address the transition of the various agencies to the DHS and to identify how each of these agencies most appropriately fits into the new organizational structure. He said the goal was to leverage existing capabilities to enhance the capabilities of the combined agencies within the new department once it becomes operational.

Future Issues

During the meeting, Mr. Greene emphasized the important work of the NS/EPC's subordinate body, the Council of Representatives (COR). "The COR has been an extremely active body during the development of the transition plan exerting a great deal of effort to complete action items aimed at mitigating risks for failure to identify all necessary elements for the transition," Mr. Greene said. He observed that there are three areas of particular COR interest at this time: bandwidth issues, especially in reference to the Continuity of Operations Plans (COOP) sites; cyberspace and the Federal Response Plan to protect information security; and the NCS efforts to integrate the concerns of State and municipal linkages as required for national level events. He indicated that the COR would continue to work within these three areas to facilitate planning to meet all national security needs.

Building on the results of the NS/EPC, highlights of the meeting of the COR held October 30, 2002, at the NCS in Arlington, Virginia, included the establishment of a working group on communications diversity, Project SAFECOM, the Wireless Priority Service (WPS) transition, and the Department of Veteran Affairs (VA) cyber security program.

Infrastructure Issues, page 16

Infrastructure Issues, continued from page 15

NCS Working Group Established

The COR established a working group to address critical facilities issues, including the need for routing diversity, to ensure effective NS/EP communications. Under the leadership of Mr. Ken Moran of the Federal Communications Commission (FCC), and Mr. Tom Sellers of the General Services Administration (GSA), the working group will look at physical as well as carrier diversity, and the operational implications for Federal facilities if implementing both types of diversity. Other agencies, including the Departments of Interior, Energy, and Treasury, the Nuclear Regulatory Council, the National Telecommunications and Information Administration (NTIA), the Federal Emergency Management Agency (FEMA), and the NCS volunteered to participate in the working group.

Project SAFECOM

The events of September 11, 2001, emphasized the importance of crisis notification among first responders, public safety personnel, and citizens. Project SAFECOM, established by the FEMA after September 11, 2001, will enable public safety personnel to communicate with other Federal, State, and local public safety personnel in the event of an emergency or other public safety response event. The program is concentrated on developing interoperable communications for Federal, state, and local emergency safety personnel.

Ms. Susan Moore, FEMA SAFECOM Program Manager, told members of the COR that, "implementing interoperable wireless public safety communications raises a number of issues given the more than 53,000 public safety entities and their different radio networks." Ms. Moore said that among these issues are requirements for cross-jurisdictional and cross-disciplinary communications, as well as the evolving next generation wireless solutions that must be included in future plans.

Acknowledging the challenges Project SAFECOM faces, Mr. Brenton C. Greene, the NCS Deputy Manager, affirmed, "NCS will continue to support this program," and he urged the COR to "participate as possible, including detailing agency experts to encourage cross-pollination in an effort to enhance interoperability communications."

Wireless Priority Service Transition

The WPS is an NCS program that provides priority access to wireless services for key national security and emergency preparedness telecommunications users. Air Force Major David Tuteral of the NCS Technology and Programs Division, the COR received an update on the Wireless Priority Service (WPS) program.

There are two phases for the implementation of WPS: the immediate solution and the nationwide solution. According to Maj Tuteral, "The immediate solution was designed to utilize available technologies and services to quickly implement wireless priority usage in three markets: Washington, DC; New York, NY; and Salt Lake City, UT (specifically for the Olympics)." He emphasized that special attention has been paid to minimizing the impact of WPS on public use. In addition, there has been a focus on joint industry and Government specification development, software code development, joint testing, and standardized network implementation.

"The WPS nationwide technical approach will provide for software priority service enhancements to commercial software for mobile switching centers and base station subsystems and will attain initial operating capability at the end of 2002," Maj Tuteral stated. He also added, that the Immediate Wireless Priority Service users in the Washington, D.C. and New York metropolitan areas would be transitioning to nationwide WPS. This transition will include T-Mobile Network testing; new dialing procedures to enable the user to invoke a priority call; and transferring responsibility of payment for usage from the NCS to the individual organizations using WPS.

Department of Veterans Affairs Reorganizes Cyber Security Program

Given the heightened importance on protecting cyber security, NCS Deputy Manager, Mr. Brenton C. Greene, invited members of the Department of Veterans Affairs (VA) cybersecurity staff to share the success and learning points of the VA's cyber security program with NCS. Two years ago, the VA came under fire from Congress, the General Accounting Office, and the Inspector General for widespread deficiencies with regard to its information security. Because

of this criticism, the department revamped its cyber security operations with the goal to become the, "model cyber security program in the Federal Government."

Mr. Bruce Brody, Associate Deputy Assistant for Cyber Security for the VA, highlighted three programs in particular, the Central Incident Response Capability (CIRC) program, the Enterprise Cyber Security Infrastructure Project (ECSP), and Cyber Security Practitioner Professionalization, Certification and Credentialing. The CIRC provides continuous operations for incident management and response. Through the Security Operations Centers (SOCs), which configure and monitor all VA cyber security systems, the CIRC provides threat analysis, forensics, and technical help desk support.

Mr. Brody noted that "Under the Enterprise Cyber Security Infrastructure Project, the VA combined more than 200 gateways and modems and consolidated them into four hardened gateways under centralized VA management." These centralized and managed security services include intrusion detection monitoring, anti-virus management, vulnerability scanning, compliance monitoring, and firewall management.

The third program, the Cyber Security Practitioner Professionalization Certification and Credentialing program, established a standard for VA cyber security professionals. According to Mr. Brody, "The certification, which is required every three years and can be revoked by the VA Office of Cyber Security, is based on training, test results, and an ethics agreement." With the establishment of this program, only certified and credentialed individuals may serve as information security practitioners at the VA.

The COR will continue to examine the issues assigned to its working groups and will meet again in early March.

NIST Offers a Non-Traditional UWB Antenna Measurement Approach

Courtesy of the National Institute of Standards and Technology

Traditional ultra-wideband (UWB) antenna characterization and measurement facilities, such as anechoic chambers, are expensive to build and operate. Consequently, researchers in the National Institute of Standards and Technology (NIST) Radio Frequency Technology Division have designed and implemented an approach for acquiring such measurements without an anechoic chamber.

The new NIST antenna measurement facility is a 7.3-meter by 7.3-meter (24-foot by 24-foot) ground-plane with a +/- 0.1 flatness specification. A 4-meter (13-foot) tall cone is used to generate a precisely characterized field. The cone and ground planer are located in a high-bay room with a 5-meter (17-foot) ceiling and concrete walls.

The facility is capable of generating standard fields down to approximately 20 megahertz. To enhance performance of the facility, broadband pulsed and swept-frequency sources, along with time-gating techniques, have enabled mathematical removal of room reflections and other unwanted effects.

Tests conducted by NIST researchers produced measurements that are comparable to those obtained from computer models. Encouraged by these results, the researchers will perform additional tests including far-field extrapolation measurements and compare them with computer models.

For a copy of paper 32-02 detailing the new facility, contact:
Sarabeth Harris
MS104, NIST
Boulder, Colorado 80305-3328
(303) 497-3237
sarabeth@boulder.nist.gov

For technical information on this development, contact:
David Novotny
MS813, NIST
Boulder, Colorado 80305-3328
(303) 497-3168
novotny@boulder.nist.gov

SNMP Issue, continued from page 9

preparedness communications issues.

Mr. Farrell and Mr. Skora believe that the close-knit working relationship between the NCS and Industry Canada could be the beginning of an important information sharing relationship essential to protecting the world's critical infrastructures.

"It is a model for international and cross-border relations in the communications sector," said Mr. Kluver. He added that the established relationship enables each country to act or react to any type of disaster, manmade or natural, physical or cyber. Mr. Kluver noted that recent events have proven that this kind of partnership is just what the emergency preparedness community needs to share information in order to prevent or mitigate the effects of some kind of large-scale emergency event.

As for SNMP, both the NCC and Industry Canada agreed that assigning a Canadian telecommunications specialist to the NCC for this project was an excellent idea. However, it was not as easy to implement as was originally thought. First, there was the issue of security. For Mr. Kluver to receive an NCS/Defense Information Systems Agency (DISA) security badge, a formal request had to be routed through the Canadian Embassy, the Defense Intelligence Agency, and DISA security. The process can be a very lengthy; however, once the proper procedures were determined, Mr. Kluver's security clearance was granted within a week.

"It is a model for international and cross-border relations in the communications sector," said Mr. Kluver. He added that the established relationship enables each country to act or react to any type of disaster, manmade or natural, physical or cyber.

Mr. Kluver also discovered that acceptance of his presence in the NCC was not immediate. Even after all of the communication between the two organizations, trust was an element that was not immediately present. Mr. Kluver felt that the individuals working in the NCC were hesitant about speaking freely in his presence.

Mr. Farrell felt this could happen and waited to see how the relationship would evolve. Although classified information on SNMP was discussed between NCC staff and their industry partners, it took time to include Mr. Kluver as a trusted NCC team member. Mr. Kluver remarked that these surprising, initial stumbling blocks were overcome within a matter of days, but served as a lesson learned for any similar situation between countries where sensitive information is discussed.

As the relationship grew, Mr. Kluver soon became a conduit of information for Industry Canada and its efforts to secure the Canadian telecommunications infrastructure. Mr. Kluver worked under Mr. Farrell's direction from February 20, 2002, to March 16, 2002, participated in daily teleconferences with Industry Canada, and helped the NCS effectively interface with the telecommunications industry in Canada. He also attended meetings with NCC industry representatives during his tenure in the NCC and was exposed to private sector information sharing that was sanitized and then sent to Industry Canada to assist with telecommunications issues. Mr. Kluver said, "all together, it was a great experience."

Since his physical departure from the NCC, the working relationship between Industry Canada and the NCC has continued to grow stronger. Ms. Maren Hansen, Director, Canadian Office of Cyber Infrastructure Protection Emergency Preparedness (OCIPEP), replaced Mr. Kluver as the conduit to Industry Canada, thus providing a direct link to the interagency and cross- sector aspects of the Canadian Government. In addition, a process has been established where OCIPEP personnel can be used if similar coordination is required.

Mr. Skora believes these relationships can only help each country understand the others' needs. "The sharing of timely information can alert industry and Government entities of possible

threats and vulnerabilities," said Mr. Skora, who is very satisfied with how the relationship between the NCS and Industry Canada is progressing. "Industry Canada has been able to better view and understand the efforts that are under way in the U.S. concerning threats to the Nation's critical infrastructures," he said.

Mr. Skora is now working to help Industry Canada establish a telecommunications Information Sharing and Analysis Center (ISAC) similar to the one in the United States. Mr. Skora explained that the emergency preparedness functions and the physical protection of the telecommunications infrastructure in Canada is "pretty well organized" within the Canadian Government; however, the cyber aspect is not as well organized. In addition, Mr. Skora said the industry-to-industry and Government-to-Government communication and information sharing relationship works well, but that industry-to-Government communication needs work. He said that Industry Canada's relationship with the NCC is helping Canada to establish its own telecommunications ISAC and is offering much insight and knowledge into information sharing between industry and Government. "These kinds of benefits are invaluable in the fight against threats and vulnerabilities in the physical and cyber world, and in the effort to combat terrorism," he said.

"The sharing of timely information can alert Government and industry entities of possible threats and vulnerabilities," said Mr. Skora, who is very satisfied with how the relationship between the NCS and Industry Canada is progressing.

FCC Chairman and Assistant Secretary of Commerce for Communications and Information Meet to Plan and Coordinate Spectrum Policy

Courtesy of the National Telecommunications and Information Administration

Federal Communications Commission (FCC) Chairman Michael K. Powell and Assistant Secretary of Commerce for Communications and Information Nancy J. Victory met on December 10, 2002, to plan and coordinate the efforts of the FCC and the National Telecommunications and Information Administration (NTIA) to improve U.S. spectrum policy.

The meeting, which included senior spectrum policy teams from both organizations, was scheduled to institutionalize and elevate the coordination of spectrum issues between the two agencies given the importance of spectrum management to the Nation today.

Spectrum users and industry participants at last spring's NTIA Spectrum Summit and public forums, which were hosted by the FCC's Spectrum Policy Task Force, emphasized the need for the FCC and NTIA to work together to develop spectrum policy for an era of technological convergence. As an immediate step

FCC Chairman Michael K. Powell

Spectrum Policy, page 20

Spectrum Policy, continued from page 19

Assistant Secretary of Commerce for Communications and Information Nancy J.Victory

to address this concern, the FCC and the NTIA announced that in the near future they will execute a new Memorandum of Understanding (MOU) detailing the terms of their interaction. Since the execution of the original MOU in the 1940s, the FCC and the NTIA have managed spectrum without updating that document.

In the meeting, the FCC and NTIA explored areas of common focus and priority in their efforts to maximize the value of a critical national asset. They discussed:

- The existing process for coordinating commercial and Government use of the spectrum;
- A mutual interest in fostering intensive use of the spectrum while diminishing the potential for harmful interference to existing spectrum users and new entrants;
- Emerging technologies with the potential to address a variety of spectrum access and interference concerns;
- Alternative licensing regimes and the success of the unlicensed model in promoting innovation; and
- Strengths and weaknesses of various licensing models, and the factors that should be weighed when considering adoption of particular licensing regimes, with a particular focus on sharing best practices to speed reform.

Both Chairman Powell and Assistant SecretaryVictory acknowledged that progress in spectrum reform will only come through a sound technical foundation. "The pace of development in spectrum-based services is such that remarkable breakthroughs quickly seem mundane," said Chairman Powell. "Our spectrum policies need to reflect this dynamic marketplace and to be flexible enough to keep up with innovation. I am pleased that Assistant Secretary Victory has made spectrum policy one of her top priorities. The NTIA and the FCC are essential partners on the frontier of spectrum policy reform, and I look forward to working closely with Assistant Secretary Victory on these important initiatives."

"Spectrum is the rocket fuel for the next wave of technological innovation," Assistant Secretary Victory said. "New spectrum technologies are moving from science fiction to the shelves of electronics stores and the cockpits of F-22 fighter jets. We need to boost the growth spectrum provides to our economy. The leadership of the FCC and the Administration are focused on the common objective of maximizing the value of the spectrum resource to the American people."

Chairman Powell and Assistant Secretary Victory agreed to schedule the next formal spectrum leadership meeting for early summer 2003.