National Security and Emergency Preparedness

Telecom News

2001, Issue 1

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

# Brenton C. Greene Becomes National Communications System Deputy Manager

By Steve Barrett, Customer Service Division, OMNCS

Brenton C. Greene, formerly Manager of Critical Infrastructure Protection Programs for Sandia National Laboratories, became the 10th Deputy Manager of the National Communications System (NCS) on April 2, 2001.

Brenton C. Greene became the 10th Deputy Manager of the National Communications System on April 2, 2001.

(Photo by John Kandrac, DISA)

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

Lt. Gen. Harry D. Raduege, NCS Manager and Director of the Defense Information Systems Agency (DISA), announced Greene's appointment on March 16, 2001. "I'm excited about the energy and background he brings to this challenging job," said Raduege. "His distinguished background as a career naval officer, his work with industry, and most recently, his experience as Manager, Critical Infrastructure Protection Programs for Sandia National Laboratories means he is well prepared for the NCS and NSTAC [the President's National Security Telecommunications Advisory Committee]."

See Greene Becomes NCS Deputy Manager, page 4

## TABLE OF CONTENTS

*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:

Stephen Barrett
Office of the Manager
National Communications
System

Customer Service Division
701 S. Court House Road,
Arlington, VA
22204-2198

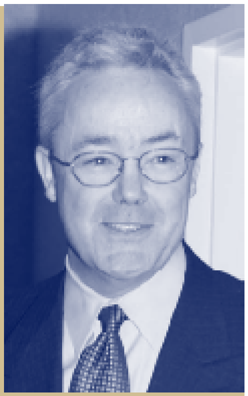
PHONE: (703) 607-6211
FAX: (703) 607-4826
e-mail:
telecomnews@ncs.gov

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

# *NSTAC Chairman Addresses, Praises Industry Executive Subcommittee*

**By Steve Barrett, Customer Service Division, OMNCS**

The Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC) told members of the NSTAC Industry Executive Subcommittee (IES) that their work was critical to NSTAC's effectiveness and thanked them for performing their duties on behalf of their companies and in support of the Nation.



Daniel J. Burnham, Chairman and CEO of Raytheon Company, and Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), addressed members of the NSTAC Industry Executive Subcommittee (IES) during their January 18 working session. (Photo by Donna Burton, Defense Information Systems Agency.)

Daniel P. Burnham, the Chairman and Chief Executive Officer (CEO) of Raytheon Company, also told the subcommittee that he is committed to supporting NSTAC to ensure that the combined efforts of the IES are highly visible to the Nation's leadership.

Speaking before the subcommittee's monthly meeting on January 18, Burnham assured the IES members that they are not working national security and emergency preparedness (NS/EP) communications issues in obscurity. He assured them that the communications industry and the Federal Government greatly recognize their efforts in researching and recommending critical infrastructure protection issues to the President.

"Your reports have received national recognition," said Burnham. Because of NSTAC's 17-year reputation as a leader in industry-Government cooperation and because previous NSTAC recommendations were enacted in past presidential administrations, Burnham said he has every reason to believe that the Bush Administration will take great interest in NSTAC's assessment on the threats to our national infrastructure—both cyber and physical.

The meeting between Burnham and the IES members was the first since Burnham assumed the NSTAC Chair on September 25, 2000. It provided the Chair a chance to tell IES members how involved he would be in NSTAC issues. "I told John (IES Working Chair John Grimes of

Raytheon) that if I'm going to take on the chairmanship, I'm going to be involved," said Burnham. He assured members he would be "engaged and visible" and would occasionally attend IES meetings to show that there would be no question to his active support of NSTAC initiatives.

Burnham added that he would make quarterly trips to the Washington area to meet with the President's National Security Council and "make sure that the new national security team is aware of our activities." He also said he would meet frequently with Lt. Gen. Harry D. Raduege, Jr., the Manager of the National Communications System (NCS) and Director, Defense Information Systems Agency (DISA), on NSTAC issues and NS/EP concerns.

In recognizing a part of the IES' ongoing work, Burnham was quick to cite efforts in network convergence. "No doubt that convergence of telephone and Internet networks are going to continue to be a big, big issue," said Burnham, who referred to the need for "assured" NS/EP for telecommunications services during national emergencies. He said that former White House Science Advisor Neal Lane specifically asked NSTAC to address the potential for widespread outage of converged networks and next generation networks. "I know that the IES is taking it on," said Burnham, "and I really look forward to your initial findings that we will all here about in June."

Burnham briefly touched on the creation of a new IES effort–-the Last Mile Bandwidth Availability Task Force. The new task force—formally approved by the IES during its business session—will examine the root causes of provisioning delays and how the provisioning process is affected by economic and technical factors. The task force also hopes to recommend how the Government might work with the communications industry to reduce provisioning times or otherwise mitigate the effects of delays, and examine what policy-based solutions could be applied to provisioning of high-bandwidth circuits for NS/EP services.

Burnham then praised IES efforts to become more responsive to requests from the Government on NS/EP telecommunications issues. "I'm sure that you're all going to agree that we need to stay ahead of these fast-changing threats," said Burnham. He added that the NSTAC must not only respond to requests quickly, but also anticipate the next request so they can "provide clear and unambiguous information and advice."

He also praised the efforts of the men and women of the Office of the Manager, National Communications System for their unfailing support to the activities of NSTAC and the IES.

In closing, Burnham told the IES members that there is a very clear set of priorities facing them. "Once those priorities are set—and I think they are largely set—we need to stick to them … and that communications [about the priorities] are clear and unambiguous," he said. "You deserve that, the White

Raytheon Company's John Grimes, Working Session Chair for the President's National Security Telecommunications Advisory Committee's Industry Executive Subcommittee (IES), welcomes Raytheon Chairman and CEO Daniel P. Burnham, and Lt. Gen. Harry D. Raduege, Jr., Manager, National Communications System, to the January 18 IES working session. (Photo by Donna Burton, Defense Information Systems Agency.)

## Burnham, Ruhl Swear In as NSTAC Principals

Lieutenant General Harry D. Raduege, Manager of the National Communications System and Director, Defense Information Systems Agency, administers an oath of Federal Service to Daniel Burnham and G. William Ruhl as they officially become members of NSTAC. Burnham, who serves as the NSTAC Chair, is Chairman and CEO of Raytheon Company. Ruhl serves as the NSTAC Principal representing the United States Telecom Association. (Photo by Donna Burton, DISA)

House deserves that, and I'm going to strive to work with you to achieve that."

Following his remarks to the subcommittee, Lt. Gen. Raduege presented Burnham with his NSTAC appointment certificate, signed by former President Clinton, plus a framed photograph of the NSTAC gavel exchange ceremony held last September at the White House. The general also presented an NSTAC appointment certificate to G. William Ruhl, the United States Telecom Association Principal to NSTAC who also attended the meeting.

Following the certificate presentations, Burnham, Ruhl and the IES listened to a briefing by MG James D. Bryan, Vice Director of DISA and Commander of U.S. Space Command's Joint Task Force-Computer Network Defense. Burnham and Ruhl were then were escorted by Lt. Gen. Raduege on tours of the National Coordinating Center for Telecommunications (NCC) and the Defense Information Systems Agency's Global Network Operations and Security Center.❖

## Greene Becomes NCS Deputy Manager *(continued from page 1)*

Greene replaces Diann L. McCoy, who was selected to be the DISA Deputy Director for Information Engineering (D6) and Commander, Joint Information Engineering Organization. Ms. McCoy served as the NCS Deputy Manager since November 1999.

Prior to his arrival at the NCS, Greene led Sandia's significant analytical, research and development, and assessment competencies into national critical infrastructure protection initiatives. He was a member of the Defense Science Board 2000 Task Force on Defensive Information Operations.

From 1998 to 1999, Greene served as Vice President for Electronic Commerce at CAMP, Inc., a non-profit corporation advancing electronic commerce in support of the Department of Defense (DOD) and small and medium size manufacturing enterprises.  Greene managed five Electronic Commerce Resource Centers (ECRC) ($24 million annual revenue) as part of DOD's National ECRC program.

During 1996 and 1997, Greene was a Commissioner on the President's Commission on Critical Infrastructure Protection, developing national policy and strategy recommendations to the President, which led to Presidential Decision Directive 63 (PDD-63) and its range of national critical infrastructure initiatives.  He was instrumental in the Commission's establishment and its results, and for this work was awarded the Secretary of Defense Medal for Outstanding Public Service.

He frequently lectured on infrastructure and information assurance issues to a wide range of Government, industry, and academic organizations and audiences.

From 1992 through 1996, Greene was a leader in National and DOD initiatives that explored a wide range of military and non-military options through the leveraging of national infrastructures and information networks.  He created DOD's Infrastructure Policy Directorate, serving as its first Director within the office of the Under Secretary of Defense for Policy.  His office was charged with developing policy, plans, programs, guidance and oversight for infrastructure assurance policy, information and infrastructure warfare concepts.

Greene served in other key DOD positions within the offices of the Under Secretary of Defense (Policy), the Under Secretary of Defense (Acquisition & Technology), the Director, Program Analysis and Evaluation, and the Chief of Naval Operations.  In these roles, he coordinated and managed leading edge technology and affordability issues, pertaining to information operations, nodal analysis, modeling and simulation, intelligence collection, counter-terrorism, satellite capabilities, system security issues, and a broad range of special program technology areas.

A 1971 graduate of the U.S. Naval Academy in Annapolis, Maryland, Greene completed nuclear propulsion training and served a career in submarines, including tours as commanding-officer of the nuclear attack submarines USS Skipjack and USS Hyman G. Rickover.  He retired as a Navy captain in 1995 to continue infrastructure-related initiatives within the Government.

His military awards include the Defense Superior Service Medal, the Legion of Merit, the Defense Meritorious Service Medal, two Meritorious Service Medals, three Navy Commendation Medals, and the Navy Achievement Medal, as well as various campaign and service awards.❖

# *Ultra-Wideband Technology Could Improve Wireless Communications*

**By Dale Barr, Technology and Programs Division, OMNCS**

Ultra-wideband (UWB) technology is a revolutionary wireless technology used to transmit large amounts of digital data short distances (up to 230 feet) over a very wide bandwidth (from 1 gigahertz [GHz] up to 10 GHz) and at very low power levels (less than 0.5 milliwatt).

Unlike typical radio broadcasts that use continuous high frequency oscillations to launch electromagnetic waves to transmit data, UWB uses precisely positioned pulses across a wide spectrum at specific time intervals to transmit the signals.  This effort is accomplished by coordinating a transmitter and receiver to send and receive pulses with an accuracy of within trillionths of a second.

Promoters of UWB technology claim that it provides a low-powered signal that is almost indistinguishable from background noise and uses a wide area of the spectrum without significant interference to other systems. Promoters believe that using UWB technology not only will improve the performance of radar, positioning, and wireless communications, but also will present new possibilities in those areas. Opponents claim that this system could potentially interfere with critical radio signals, such as those emitted from global positioning system (GPS) satellites.

### Applications Of UWB

With UWB, radio signals can penetrate nearby surfaces while reflecting off surfaces that are farther away. This capability would allow radar-type applications to detect objects, such as people or weapons, behind walls or under surfaces, such as a collapsed building. UWB technology also can precisely measure distance and movement to within one inch. Precision geolocation systems can locate a person or vehicle by attaching locator beacons that send out signals to receivers so that a precise location can be determined. Beacons could be inserted into pagers, cellular phones, or a vehicle.

This technology could aid emergency responders in locating victims, team members, and medical supply trucks, for example. Unlike GPS, this geolocation system could operate indoors, underground, in foliage, in noisy environments, and through bad weather.

| APPLICATION | COMMERCIAL USE | GOVERNMENT USE |
|---|---|---|
| Asset tracking - locators/beacons to track mobile inventory and emergency 911 positioning | 4 | 4 |
| Surveillance radar - radar imaging, precise enough to distinguish specific features on aircraft/marine craft, bringing real-time intelligence to the battlefield | | 4 |
| Ranging - commercial/industrial "ranging" applications to determine precise distances between objects | 4 | |
| Security systems - imaging intrusion systems for alarming and tracking of movement | 4 | 4 |
| Through-wall and underground imaging and radar - detection of objects and conditions through structures | 4 | 4 |
| "Smart" home - wireless links to cable, TV, Internet, computer, and applicances | 4 | |
| Wireless Local Area Networks (LANs) - indoor, short range, high-bandwidth data and video communicatiosn where many channels are needed simultaneously (i.e., rural last mile, home server, in-building wireless LANs, and in-building communications) | 4 | |
| Portable wireless LANs - easy set-up wireless links for data and video transmission to give greater mobility | | 4 |
| Covert communications - radios for squad-level operations that allow anonymous communications without identification | | 4 |

Some of these Ultra-Wideband applications could be used in the commercial and Government sectors. (NCS illustration)

With the use of time-modulated digital pulses, UWB allows the use of very low-powered and relatively inexpensive equipment to broadcast signals at very high rates over a large part of the spectrum. This technology may enable the use of public safety devices and wireless communications in areas that suffer from severe multipath and/or high levels of industrial noise and interference. UWB could conceivably be used to provide high-speed Internet access similar to today's wireless modems.

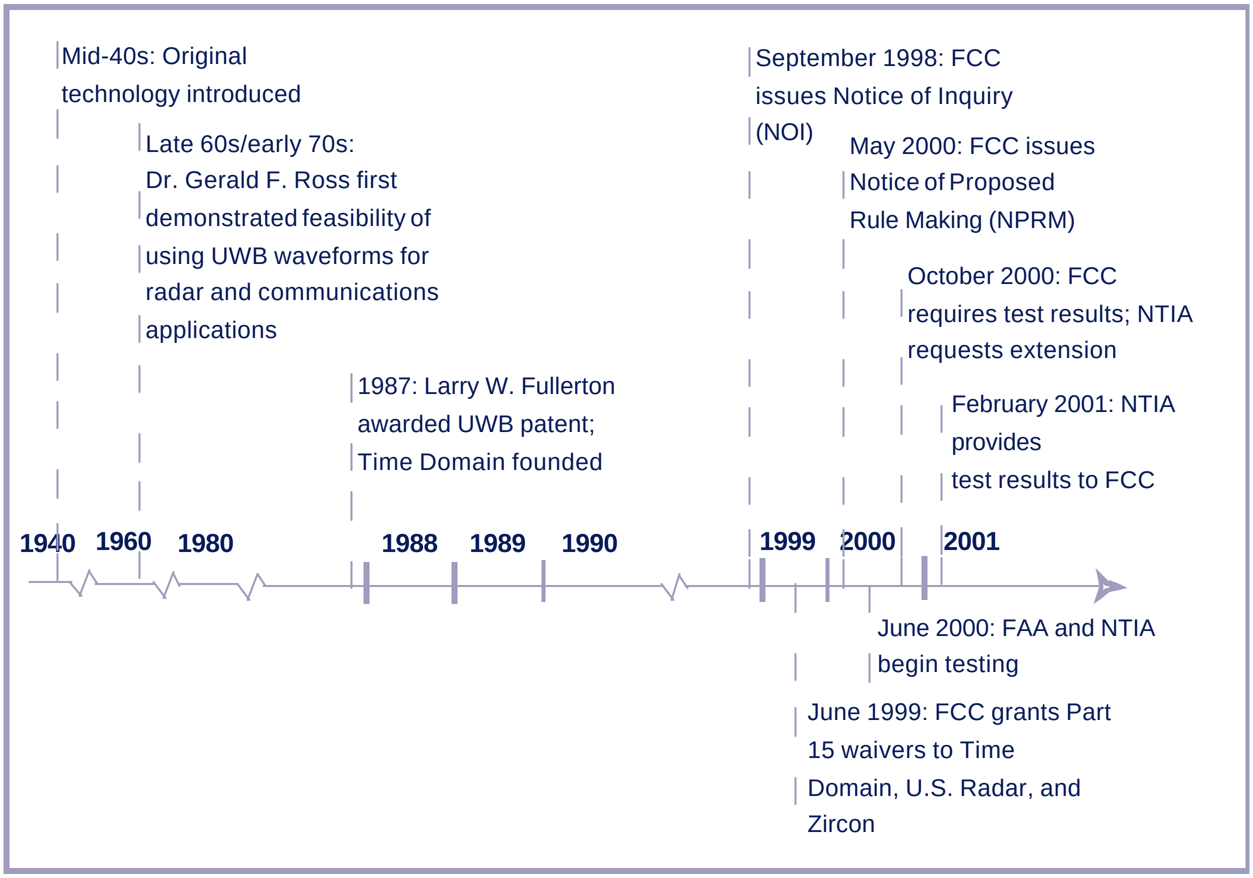
Additionally, low-power UWB devices may be noninterfering, which could increase its market potential. This technology has led to rapidly growing commercial and government interest in UWB development.

## The UWB Marketplace

Currently, three companies are influencing the future of the UWB marketplace: Time Domain Corporation; Zircon Corporation; and U.S. Radar, Inc.

Time Domain, headquartered in Huntsville, Alabama, is home to Larry Fullerton, who is credited with patenting time-modulated UWB technology in 1987, although the original technology dates back to the 1940s. Time Domain has developed the PulsON® chip, a high-speed chip that blends silicon and germanium to provide the time-modulated UWB technology. This chip can be inserted into many different devices to provide UWB technology to the user.

Currently, Time Domain is supplying police departments with a system that enables law enforcement officers to covertly communicate with each other. It is also providing a radar system that will enable fire and rescue squads to precisely locate persons trapped inside damaged, burning, or smoke-filled buildings.


Mid-40s: Original technology introduced
Late 60s/early 70s: Dr. Gerald F. Ross first demonstrated feasibility of using UWB waveforms for radar and communications applications
1987: Larry W. Fullerton awarded UWB patent; Time Domain founded
September 1998: FCC issues Notice of Inquiry (NOI)
May 2000: FCC issues Notice of Proposed Rule Making (NPRM)
October 2000: FCC requires test results; NTIA requests extension
February 2001: NTIA provides test results to FCC
1940
1960
1980
1988
1989
1990
1999
2000
2001
June 2000: FAA and NTIA begin testing
June 1999: FCC grants Part 15 waivers to Time Domain, U.S. Radar, and Zircon

The timeline depicts the recent increase in development and testing activity surrounding UWB since the founding of Time Domain and Mr. Fullerton's patented time-modulated UWB technology. (NCS illustration)

Zircon, headquartered in Campbell, California, has been working with UWB since 1980. It is developing a surface probing impulse radar system. Used primarily by the construction industry, this system can detect features such as electrical wiring conduit, water pipes, and gas lines, behind walls and other surfaces. Zircon will also manufacture and sell electronic hand tools, such as stud locators that can detect wood and metal density differences behind walls, above ceilings, and under floorings.

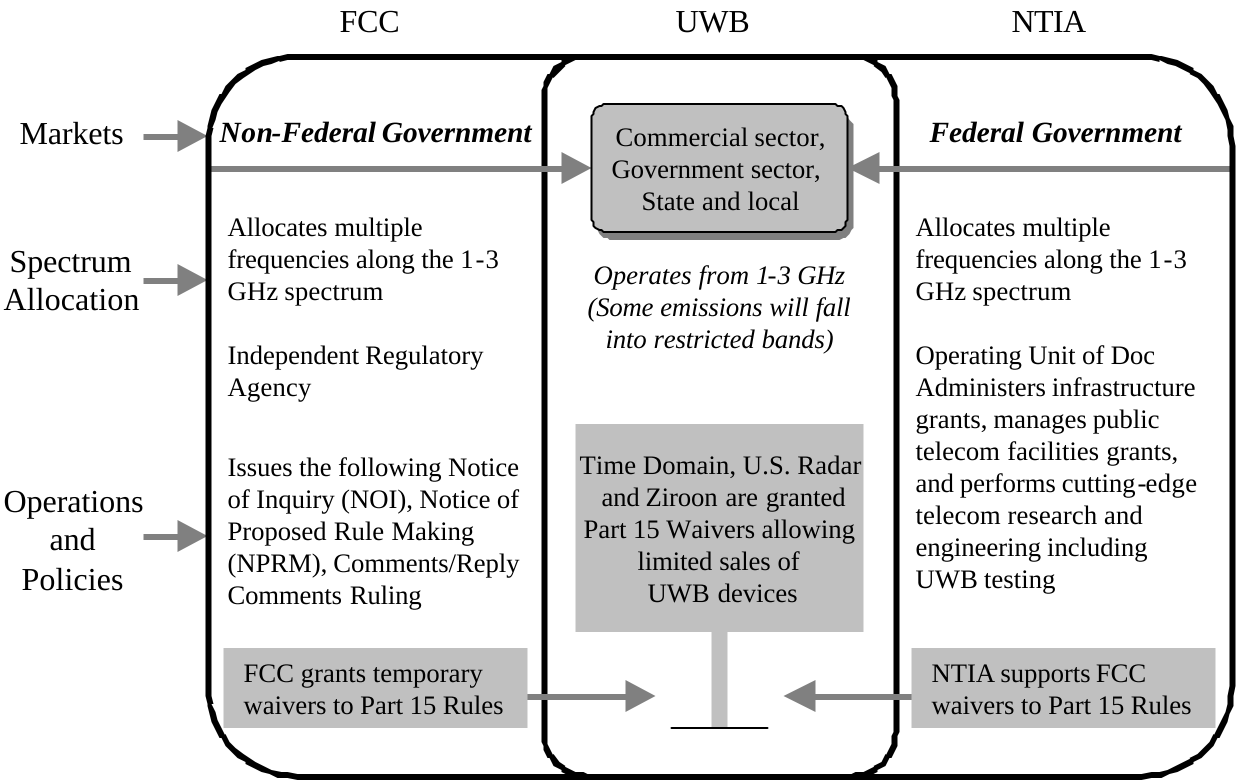
U.S. Radar, Inc., located in Matawan, New Jersey, is currently marketing SPRscan, a ground-penetrating radar (GPR) system that is used to detect buried objects, such as plastic gas pipes, or reveal structural flaws in roads, bridges, or airport runways.

Two other companies studying uses of UWB are Multispectral Solutions, Inc., and Fantasma Networks.

## FCC And NTIA Rules And Regulations

On September 1,1998, the Federal Communications Commission (FCC), which is responsible for allocating frequencies to non-Federal Government users, released a Notice of Inquiry (NOI). The purpose of the NOI was to investigate the possibility of permitting the operation of UWB technology on an unlicensed basis. The NOI requested comments on the standards and operating requirements that would need to be applied to UWB systems to prevent interference with other radio services.

The FCC and National Telecommunications and Information Administration (NTIA) develop rules for operations of unlicensed devices. The NTIA, an agency within the U.S. Department of Commerce (DOC), is responsible for managing spectrum allocated to Federal Government users. These rules


FCC
UWB
NTIA
Markets
Spectrum Allocation
Operations and Policies
Non-Federal Government
Allocates multiple frequencies along the 1-3 GHz spectrum
Independent Regulatory Agency
Issues the following Notice of Inquiry (NOI), Notice of Proposed Rule Making (NPRM), Comments/Reply Comments Ruling
FCC grants temporary waivers to Part 15 Rules
Commercial sector, Government sector, State and local
Operates from 1-3 GHz (Some emissions will fall into restricted bands)
Time Domain, U.S. Radar and Ziroon are granted Part 15 Waivers allowing limited sales of UWB devices
Federal Government
Allocates multiple frequencies along the 1-3 GHz spectrum
Operating Unit of Doc Administers infrastructure grants, manages public telecom facilities grants, and performs cutting-edge telecom research and engineering including UWB testing
NTIA supports FCC waivers to Part 15 Rules

This illustration shows how Ultra-wideband regulation correlates with the Federal Communications Commission and the National Telecommunications and Information Agency. (NCS illustration) are detailed in Part 15, Title 47 (47 CFR 15), of the Code of Federal Regulations, which sets forth guidelines and oper-ational policy for all unlicensed devices that transmit a frequency signal, and thus have the ability to interfere with communications within assigned and restricted bands.

Part 15 designates certain sensitive and safety-related frequency bands as restricted. Only spurious emissions not exceeding the general emission limits are permitted within these restricted bands. Such bands include safety spectrum and GPS spectrum, which both possess emergency response and critical communication implications. Ultra-wideband devices emit low levels of power, but because their bandwidths generally exceed 1 GHz and go up to 10 GHz, it is nearly impossible for these devices to avoid placing emissions within the restricted bands.

Based on the comments and replies submitted in response to the NOI, and on preliminary testing from independent sources, the FCC concluded that low-power UWB would be able to operate within the existing spectrum without causing significant interference. The FCC subsequently released a Notice of Proposed Rule Making (NPRM) on May 10, 2000, proposing regulations that would amend Part 15 rules to permit the unlicensed operation of UWB devices.

Most UWB devices will be marketed for the public; therefore, individual licensing would be unrealistic. The FCC prefers a system with maximum peak emission levels for unlicensed UWB operation, but also recog-nizes that higher output devices may require special licensing or jurisdiction under another FCC rule. The FCC has requested comments on the text of the NPRM to help develop policy guidelines for amending Part 15.

During the NPRM comment waiting period, temporary waivers have been granted to Time Domain Corporation, Zircon Corporation, and U.S. Radar, Inc. Granted June 29, 1999, these waivers give permission for these companies to manufacture and sell a limited number of UWB devices during a 4-year period. Time Domain's waiver allows it to produce no more than 2,500 units of its UWB system for detecting persons in a building environment. U.S. Radar's waiver permits it to produce 25 units of its GPR system, and Zircon is authorized to build its surface probing impulse radar, limiting sales to professional tradespeople.

Because the waiver requests include UWB intrusion into frequency bands allocated to the U.S. Government, the waivers were coordinated closely in conjunction with the NTIA. In a June 15, 1999, letter, the NTIA agreed with the FCC's decision to grant waivers to the three companies. The NTIA reiterated that all conditions of the waivers should be strictly followed to avoid harmful interference to authorized users. It recommended that all additional waivers be suspended or limited until further tests could be conducted regarding the safety of UWB devices.

## Current Testing

To address concerns over the interference issues, the NTIA's Office of Spectrum Management (OSM) in Washington, D.C., and Institute of Telecommunications Sciences in Boulder, Colorado, have been tasked to obtain test results that will assess the potential for certain classes of UWB systems to interfere with other radio services. The testing will consist of measurement procedures that will accurately measure UWB signal characteristics.

The tests will also evaluate the levels of UWB interference to authorized radio communications or sensing systems. The NTIA released their test results in mid-January and are available on at http://www.ntia.doc.gov/osmhome/reports/UwbGps/index.html.

Because the aviation community has expressed its concerns over UWB's possible interference with the GPS signal used to navigate aircraft and guide missiles, the NTIA will develop a measurement and analysis plan that will address GPS-specific issues. The Department of Transportation is funding tests conducted by Stanford University's GPS Laboratory to study effects of UWB signals on GPS systems within aircraft, specifically during landing and takeoff.

On September 7, 2000, the NTIA held the first of several public meetings to define operational scenarios to test for interference between UWB and GPS devices. Attendees that would help define these scenarios included GPS companies and industry organizations, UWB companies, military organizations, and government agencies. Once scenarios are selected and refined, the NTIA will apply its test data to them and provide the results to the FCC.

Tests conducted to date have shown some potential for interference, but further tests are needed to identify the level of interference and whether the UWB signal has a significant effect on other radio communication systems.

### Conclusions

Since its inception in the 1940s, contributors to UWB development have been searching for practical applications in which to use UWB technology.  With the conclusion of the FCC testing period, commercial deployment of UWB devices could take place as early as 2001.

UWB technology could spur the development of innovative devices that would efficiently use the frequency spectrum. With government and non-government entities vying for space on the currently congested spectrum, this technology could change the way that frequency has been viewed traditionally.

Future potential technologies could include not only low-power wireless networks linking phones, computers, and televisions without the need for hardwiring, but also cell phones that could help determine a user's location for a 911 emergency operator. This technology could radically change how national security and emergency preparedness personnel operate in search and rescue efforts and other crisis events.❖

# NSTAC Holds Fourth R&D Exchange at University of Tulsa

**By Kiesha Miller, Customer Service Division, OMNCS**

The President's National Security Telecommunications Advisory Committee (NSTAC) held its fourth Research and Development (R&D) Exchange at the University of Tulsa in Tulsa, Oklahoma, on September 28 and 29, 2000.

Focusing on long-term security R&D issues related to the convergence of public networks and Internet technologies, the exchange was co-sponsored by the White House Office of Science and Technology Policy (OSTP) in conjunction with the Telecommunications and Information Security Workshop.  This workshop was co-sponsored by the National Institute of Standards and Technology (NIST), the National Information Assurance Partnership (NIAP), and the National Telecommunications and Information Administration (NTIA).

The theme of the 2000 R&D Exchange was "Transparent Security in a Converged and Distributed Network Environment: A Dream or a Nightmare?"  The exchange provided a dynamic dialogue among Government, industry, and academia on network security, critical infrastructure protection, and network convergence.  Nearly 100 people participated in the 2-day event, divided into four facilitated panel discussions.

Dr. Peter Fonash, Chief of Technology and Programs for the National Communications System, moderated the workshop's Session I.  Dr. Fonash also provided an overview of convergence issues and discussed NCS technology programs.

The session, "Differing Perspectives on Security in Converged Networks," began with a keynote address, via satellite, from Congressman Curt Weldon of Pennsylvania.  Congressman Weldon serves as the Chairman of the Military R&D Subcommittee, House Armed Services Committee, and is the Senior Member of the House Science Committee.

In his broadcast, Congressman Weldon emphasized the importance of protecting our Nation's telecommunications and information systems from an array of new threats.  He discussed the importance of maintaining information dominance during war and expressed the growing threat posed by cyber terrorism.

In concluding his remarks, Congressman Weldon outlined three recommendations to the group.  First, he asked attendees to develop technical tools and capabilities to collect, aggregate, and mine threat information.

He then asked the corporate conference attendees to invest in R&D programs to ensure that the U.S. military retains access to emerging information technologies on the battlefield. Finally, he expressed the need to help train the next generation of computer security professionals and followed his address by participating in an interactive question and answer period.

Session I continued with presentations from five panelists identified as representing the views of telecommunications users, vendors, and network providers. Dr. Paul Prucnal of Princeton University presented a briefing on emerging optical technologies and their potential impact on the Next Generation Internet. He highlighted the high demand of bandwidth, and noted the reason most often cited for shortfalls was the limited capacity of fiber optic cable to transmit high-speed data. Pracnal also explained that there was a great deal of unused bandwidth on fiber optic cables and that the bottleneck was really the inability of routers to manage data flow.

Hank Kluepfel (right), from Science Applications International Corporation, an active participant in NSTAC activities, hands an NSTAC information brochure to a conference attendee at the Fourth NSTAC R&D Exchange. The 2-day session was held at the University of Tulsa. (Photo by Kiesha Miller, National Communications System)

A second panelist—Robert Wright of BellSouth—explained a network provider's perspective on managing risks and described the tension in corporations of balancing the need for security versus the benefits of utility and accessibility.

Edward Balkovich of Verizon Communications, who highlighted the security issues related to integrated voice and data networks and voice over internet-protocol technology, followed Wright. Balkovich also emphasized the importance of focusing on the SS7 to IP security interconnections, where attacks are most likely to occur.

Following Balkovich was Dan Woolley of Global Integrity, who provided an overview of the increased incidence of electronic intrusions and discussed the costs associated with security incidents and recovery operations. Woolley said cyber protection is essential to a business surviving and explained that surveyed organizations estimate losses of $265 million in 1999 as a result of unauthorized employee access or abuse. Woolley cited several reported incident types that include IP theft, sabotage, fraud, viruses, and penetration. In the case of IP theft, Woolley said companies surveyed lost over $65 million in the past year.

Concluding Session I, Dr. Jack Edwards, NSTAC's Industry Executive Subcommittee (IES) member from Nortel Networks, emphasized the importance of security in the control space. Dr. Edwards also described the importance of devoting R&D to developing better test and evaluation methodologies.

Session II, "Technology Transfer Issues," included discussions of security issues involving technology transition and implementation. Dr. Gif Monger of Science Applications International Corporation (SAIC) described the netEraser program partially funded by In-Q-Tel. The netEraser program was established to provide secure network services in the ".com" domain. NetEraser creates a secure gateway for electronic commerce.

## Scenes from NSTAC's Fourth R&D Exchange

Members representing the NSTAC hold an informal discussion. From left to right are Dr. Jack Edwards of Nortel Networks, Bob Wright of BellSouth, Hank Kluepfel of Science Applications International Corporation (SAIC), Ed Balkovich of Verizon Communications, and Dr. Paul Prucnal of Princeton University.

As former NSTAC Industry Executive Subcommittee member Robert Burns (right) listens, Ed Balkovich of Verizon Communications speaks to a conference attendee during a break.

Dr. Terrence Kelly (left), Senior National Security Officer assigned to the International Affairs Division of the White House Office of Science and Technology Policy, and Dr. John Hale of the University of Tulsa answer questions during a break . (Photos by Kiesha Miller, NCS)

WorldCom's Paul Krumviede then outlined several areas where Government and industry have collaborated regarding the Internet and challenges concerning the effective transfer of technologies.

The final two sessions were facilitated discussions of the main ideas taken from the previous day's R&D Exchange and NIST/NIAP tracks. Included in these panel discussions were presentations from SAIC's Hank Kluepfel, Dr. Edwards, Dr. Terrence Kelly from the White House Office of Science and Technology Policy, and Dr. John Hale from the University of Tulsa. Panelists encouraged participants to identify key issues and challenges associated with security in converged networks.

Several attendees suggested the President gain more support for CyberCorps, training of law enforcement and lawyers for prosecution of computer crimes, standards for broadband switch security, partnerships of Government and industry, and R&D funding.

Following Session I, SBC Communications hosted a reception and tour for Exchange participants at the Gilcrease Museum in Tulsa. Five NSTAC companies—Computer Sciences Corporation (CSC), SAIC, the National Telecommunications Alliance (NTA), Nortel Networks, and Northrop Grumman—sponsored a farewell luncheon concluding the exchange.

In effort to increase NSTAC visibility, the National Communications System and the NSTAC exhibited an NSTAC display to promote various NSTAC reports, CDs, and anniversary brochures.

Since 1990, NSTAC has devoted considerable attention to network security and information assurance issues. NSTAC continues to examine network security standards, and analyze intrusion detection technology research and development. The Presidential advisory committee has previously sponsored three R&D Exchanges to facilitate and promote a dialogue among industry, Government, and academia.

The last R&D Exchange—held in October 1998—discussed the need for security metrics and large-scale test beds; the "brain drain" of information technology and security professionals leaving Government and academia; and the need to adopt a long-range view (approximately 5-10 years) of security technology R&D.

Participants at the fourth R&D Exchange encouraged NSTAC to hold another R&D Exchange in 2001. Suggested topics include: (1) the human dimension of network security and the challenges major education, training, and awareness organizations face in protecting their key systems, and (2) identification of emerging technologies—such as self-healing systems—that promise to assist organizations in compensating for shortfalls in personnel or skills.

R&D exchange proceedings, including any conclusions and recommendations resulting from the Tulsa Exchange, are currently being developed by the NSTAC's R&D Task Force.

For additional information on the NSTAC R&D Exchange, please visit the TISW 2000 Workshop website at www.cis.utulsa.edu/tisw2000, the NSTAC homepage at www.ncs.gov/nstac/nstac.html or contact Kiesha Miller at (703) 607-6134.❖

# TSP Program Provides Priority Telecommunications for NS/EP Missions

**By Betty Hoskin, Operations Division, OMNCS**

On March 28, 2000, twin tornadoes struck downtown Fort Worth, Texas, smashing windows in several skyscrapers, flattening buildings, overturning vehicles, and scattering debris along downtown streets. A few hundred feet away from the direct path of one of the tornadoes, the windows on nearly every floor of the building that housed the Bureau of Alcohol, Tobacco, and Firearms (ATF) were blown out. With power and telephone lines out to thousands of customers—including the ATF—the Bureau's Office of Science and Technology (OST) had a

## CSC's Honeycutt Thanked for Service to NSTAC, Nation

Lieutenant General Harry D. Raduege, Manager of the National Communications System, presents Computer Sciences Corporation (CSC) Chairman, President, and Chief Executive Officer Van B. Honeycutt with a letter signed by former President Bill Clinton. The President thanked Mr. Honeycutt for his two years of service as Chairman of the President's National Security Telecom-munications Advisory Committee. Lt Gen Raduege made the presentation to Mr. Honeycutt on March 22 at CSC's Executive Business Center in Falls Church, Virginia. (Photo by Karen Clark, CSC)

crisis on its hands.

Because the OST oversees the ATF's application of science and technology to collect, clarify, and communicate the information needed to reduce violent crime, collect revenue, and protect the public, OST was responsible for overseeing the restoration of the ATF's communication lines. Given the ATF's unique position within the law enforcement community in enforcing Federal laws relating to alcohol, tobacco, firearms, explosives, and arson, it was important that OST restore the ATF's communications capabilities as quickly as possible.

Fortunately, OST was able to rely on the Telecommunications Service Priority (TSP) Program for priority restoration of the ATF's telecommunications circuits. While the ATF was establishing an emergency command center a few blocks away, the ATF's telecommunications carrier began priority restoration efforts. The circuits were reinstalled the next morning.

The preceding scenario is common for the TSP Program. Entities with national security and emergency preparedness (NS/EP) missions requiring expedited restoration of existing telecommunications services or provisioning of new services to meet mission-critical requirements use TSP. The Federal Communications Commission defines NS/EP missions as those used to maintain a state of readiness or respond to any event (local, national, or international) that could harm the population, damage property, or threaten the NS/EP posture of the U.S.

When natural disasters such as tornadoes, floods and earthquakes, and technical disasters occur, requests for restoration often inundate telecommunications service vendors. The TSP Program provides telecommunications vendors with a regulatory, administrative, and operational framework for priority provisioning and restoration of qualified NS/EP services.

The TSP Program originiated at the time of the AT&T divestiture in 1984—an action that brought the formation of the Regional Bell Operating Companies (RBOCs). Officials with the Federal Communications Commission (FCC) realized that the U.S. needed a system among the various carriers to identify and prioritize critical NS/EP telecommunications services. Soon thereafter, the FCC issued the TSP Report and Order establishing the TSP Program. The program grants common carrier telecommunications vendors the legal protection necessary to provide priority treatment to telecommunications services designated with TSP assig-nments over non-TSP services.

The Office of the Manager, National Communications System (OMNCS) administers the TSP Program. Within the OMNCS, the Office of Priority Telecommunications (OPT) manages the day-to-day operations of the TSP Program and is the point of contact for TSP matters.

The first step in the TSP process is identifying services that support NS/EP missions, including national security, public health and safety, and public welfare, as indicated in FCC's TSP Report and Order (FCC 88-341). The TSP Program is available for use by organizations whose missions meet those criteria. Non-Federal TSP users must have a Federal agency sponsor for their TSP requests. The OPT can help the non-Federal user determine which Federal organization would be an appropriate sponsor, based on a shared mission.

With more than 36,900 NS/EP services currently protected with TSP assignments, the TSP Program has been very successful. These assignments ensure that the telecommunications services that are crucial to performing NS/EP missions will receive priority restoration from vendors before non-TSP services. Currently, State and local organizations constitute the largest growth area for TSP restoration assignments, indicating the important role that TSP can play in regard to Federal, State, and local government, and industry critical infrastructure protection efforts.

Chatry Perry, Section Leader of the OMNCS Training/Planning/Operational Support Section, believes the program is vital to national security. "By using TSP, an organization can take proactive measures to prepare for the unexpected," said Perry. "Our daily use of telecommunications services creates a presumption that they will always be available. By providing a prioritized response to a loss of service, TSP can enhance the effectiveness of an organization's operational activities."

The OPT has also successfully applied information technology solutions to support its mission and enhance the administration and operation of the TSP Program. The OPT uses the Priority Telecommunications System (PTS) client and server platform to process administrative information while providing users, vendors, and Federal sponsors with a flexible way to remotely access TSP information and on-line services.

In addition, the OPT uses the Internet for TSP outreach and information sharing. A continuously updated TSP Web Site is available at http://tsp.ncs.gov. This Web site includes expansive information about the TSP Program, descriptive TSP graphics, and a link to electronic versions of TSP Program forms. The TSP electronic forms (e-form), such as the TSP Request for Service Users and the Service Confirmation for Service Vendors forms, are accessible via a secure server.

After completing a registration form and receiving authorization from the OPT, e-form users can submit TSP forms to the OPT online. The OPT then processes the information and posts return information, such as TSP assignments, on a secure server for access by authorized e-forms users. These technologies and applications will ensure that the TSP Program continues to serve the critical needs of NS/EP users into the 21st century.

For more information about the TSP Program, please contact:

Office of the Manager, NCS
Attn: Office of Priority
Telecommunications
701 South Court House Road
Arlington, Virginia 22204-2198
Phone: 703/607-4932
Fax: 703/607-4937
E-mail: tsp@ncs.gov❖

*The author is an NS/EP telecommunications specialist and the day-to-day operational manager of the OPT.*

# NIST Seeks Final Comments on Advanced Encryption Standard

On February 28, 2001, the National Institute of Standards and Technology (NIST) formally published details of its new Advanced Encryption Standard (AES) in the Federal Register, opening a public comment period on the new technique for securing the confidentiality of sensitive, unclassified electronic data.

The AES specifies the Rijndael encryption algorithm, which was selected by NIST in October 2000 at the end of a multiyear, worldwide competition.

NIST's Information Technology Laboratory is asking cryptographers and other interested parties to comment on the draft Federal Information Processing Standard (FIPS). Following the 90-day comment period that ends May 29, 2001, NIST will make any necessary revisions to the draft standard, which then will be submitted to Commerce Secretary Donald Evans for his review and approval.

If all steps of the process go as planned, NIST will publish the final standard in the fall of 2001. The AES will be a public algorithm designed to protect sensitive Government information well into the 21st century. It will replace the aging Data Encryption Standard, which NIST adopted in 1977.

Comments may be sent electronically to AEScomments@nist.gov or mailed to the Chief, Computer Security Division, Information Technology Laboratory, Attn: Comments on Draft FIPS for the AES, NIST, 100 Bureau Drive, Stop 8930, Gaithersburg, Maryland 20899-8930.

For more information on the AES and to download the February 28, 2001, Federal Register notice, go to http://www.nist.gov/aes.❖
(Courtesy of NIST)

# FBI, NIPC Introduce National InfraGard Program

The Federal Bureau of Investigation (FBI) and the National Infrastructure Protection Center (NIPC), located at FBI Headquarters, introduced on January 5, 2001, the National InfraGard Program to the public.

The National InfraGard Program began as a pilot project in 1996, when the Cleveland FBI Field Office asked local computer professionals to assist the FBI in determining how to better protect critical information systems in the public and private sectors. From this new partnership, the first InfraGard Chapter was formed to address both cyber and physical threats.

The NIPC, in conjunction with representatives from the private industry, the academic community, and the public sector, further developed the "InfraGard" initiative to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats.

The initiative, encouraging the exchange of information by Government and private sector members, continued to expand through the formation of additional InfraGard chapters, within the jurisdiction of each FBI Field Office. As of January 5, 2001, all 56 field offices of the FBI have opened an InfraGard chapter, with a total of 518 company members across the nation.

The National InfraGard Program provides four basic services to its members: an intrusion alert network using encrypted e-mail, a secure Web site for communication about suspicious activity or intrusions, local chapter activities, and a help desk for questions.

The critical component of InfraGard is the ability of industry to provide information on intrusions to the local FBI Field Office using secure communications in both a "sanitized" and detailed format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation, while the NIPC at FBI Headquarters can analyze that information to determine if the intrusion is a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. In addition, the secure Web site contains a variety of analytic and warning products that can be made available to the InfraGard community.

> ***The InfraGard Program allows law enforcement and industry to work together and share information that could prevent potential intrustions into our national infrastructure.***

"The InfraGard Program allows law enforcement and industry to work together and share information regularly, including information that could prevent potential intrusions into our national infrastructure," said former Attorney General Janet Reno. "Building bridges between law enforcement and the public and private sector(s) is one of the most important ways we can protect ourselves from these threats."

FBI Director Louis J. Freeh also applauds the success of the National InfraGard Program: “Computer crime is one of the most dynamic problems the FBI faces today. I am proud of the progress we have made in dealing with this problem by establishing the InfraGard initiative and opening the lines of communication between the public and private sectors and the law enforcement community. I am confident that we will continue to work together to further develop the capabilities to meet the computer crime problem, in all its facets, head on. Our economy and public safety depend on it.”

For additional information about the National InfraGard Program or infrastructure protection, please contact your local FBI Field Office. For additional information about the National Infrastructure Protection Center, please inquire via e-mail at nipc@fbi.gov. ❖ (Courtesy of the NIPC.)

## Ruhl Receives NSTAC Certificate

G. William Ruhl (right), Chief Executive Officer of D&E Telephone Company, Senior Vice President of D&E Communications, Inc., and Chairman of the United States Telecom Association (USTA), accepts a White House proclamation certificate designating him as member of the President’s National Security Telecommunications Advisory Committee (NSTAC). Lieutenant General Harry D. Radeuge, Manager of the National Communications System (NCS) and Director, Defense Information Systems Agency, made the presentation on January 18. (Photo by Donna Burton, Defense Information Systems Agency.)

## High-Tech Industry Announces New Information Sharing and Analysis Center for Information Security

**By Tinabeth Burton, Information Technology Association of America**

Nineteen of the nation’s leading high tech companies announced on January 16, 2001, the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems.

In response to the recent increases in the number and nature of cyber attacks on networked information systems, the IT industry has banded together to fund this new organization to facilitate the sharing of threat and vulnerability information.

The IT-ISAC is a not-for-profit corporation that will allow the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices, and other protective measures. The organization is a voluntary, industry-led initiative with the goal of responding to broad-based security threats and reducing the impact of major incidents.

Membership in the IT-ISAC is open to all U.S.-based information technology companies. It will offer a 24-by-7 network, notifying members of threats and vulnerabilities. The 19 Founding Member companies of the IT-ISAC, all represented at the announcement, are:

- ■AT&T
- ■Cisco Systems
- ■Computer Associates
- ■Computer Sciences Corporation (CSC)
- ■EDS
- ■Entrust Technologies
- ■Hewlett-Packard Company
- ■IBM
- ■Intel Corporation
- ■KPMG Consulting
- ■Microsoft Corporation
- ■Nortel Networks
- ■Oracle Corp.
- ■RSA Security
- ■Securify Inc.
- ■Symantec Corporation
- ■Titan Systems Corp.
- ■Veridian, and
- ■VeriSign, Inc.

Six of the 19 companies involved in the IT-ISAC (AT&T, Cisco Systems, CSC, EDS, Microsoft, Nortel Networks) are member companies of the President's National Security Telecommunications Advisory Committee (NSTAC). Of those six, five are active participants in the telecommunications ISAC operated by the National Communications System's National Coordinating Center for Telecommunications (NCC).

Significant IT industry input to the President's Commission on Critical Infrastructure Protection led to the adoption of a number of industry recommendations in the Commission's final report, including the creation of public-private partnerships and information sharing mechanisms addressing threats and vulnerabilities of IT networks. These industry views were included in Presidential Decision Directive 63, which advanced a public-private sector plan for critical infrastructure protection. The IT industry has worked closely with the Department of Commerce and other Federal agencies in laying the groundwork to implement information sharing mechanisms.

In February 2000, many IT industry leaders participated in a White House summit on network security and committed to create an IT industry mechanism to share information on cyber attacks, vulnerabilities and security practices. The January 16 announcement was the next step in what has been, and will continue to be, an ongoing cross-industry and Government partnership that is vital to improved network security and reliability and our common national interests.

The IT-ISAC Founding Members were joined at

## Microsoft's Mundie Becomes NSTAC Principal

Lieutenant General Harry D. Raduege, Manager of the National Communications System, and Director, Defense Information Systems Agency, administers an oath of Federal Service to Craig J. Mundie as he officially becomes a member of the President's National Security Telecommunications Advisory Committee. Mundie is the Senior Vice President of Advanced Strategies for Microsoft Corporation. (Photo by John Kandrac, DISA) the announcement by former Commerce Secretary (and Transportation Secretary) Norman  Mineta; Information Technology Association of America President Harris N. Miller; Richard Clarke, the National Coordinator for Security, Infrastructure Protection, and Counterterrorism; and Greg Rohde, the Assistant Secretary of Commerce for Communications and Information.

The creation of the center prompted numerous statements from the founding companies.  Statements are posted at www.itaa.org.❖

# Michael Powell Named FCC Chair

**By Steve Barrett, Customer Service Division, OMNCS**

President George W. Bush named the Federal Communications Commission's Michael K. Powell chair the FCC, following the resignation of William Kennard as FCC Chair.

"I am deeply honored and privileged to have received President Bush's designation to be Chairman of the Federal Communications Commission," said Powell in a written statement released by the FCC January 22.  "I look forward to working with the new administration, Congress, my fellow Commissioners and the very talented FCC staff on the important and challenging communications issues facing our Nation."

Powell has been a commissioner at the FCC since 1997, when the U.S. Senate confirmed his nomination by then-President Bill Clinton.  His current term with the FCC ends June 30, 2002.

Prior to assuming the FCC chair, Powell served as the FCC's Defense Commissioner and was responsible for overseeing all national security and emergency preparedness functions for the Commission.  He also served as the FCC representative to the President's Council on Year 2000 Conversion, which was established by President Clinton on February 4, 1998, to address the Year 2000 computer issues.

Powell previously served as the Chief of Staff of the Antitrust Division in the Department of Justice.  In that capacity, he advised the Assistant Attorney General on substantive antitrust matters, including policy development, criminal and civil investigations, and mergers.  Prior to joining the Antitrust Division, he was an associate in the Washington, D.C. office of the law firm of O'Melveny and Myers LLP, where he focused on litigation and regulatory matters involving telecommunications, antitrust, and employment law.

Powell graduated from the Georgetown University Law Center in 1993 following which he served as a judicial clerk to the Honorable Harry T. Edwards, Chief Judge of the United States Court of Appeals for the District of Columbia Circuit.

Before attending law school, from 1988 to 1990, he served as a policy advisor to the Secretary of Defense on matters involving the United States-Japan security relationship.

Michael K. Powell, an FCC Commissioner since 1997, was selected by President George W. Bush to become Chairman of the FCC.  (FCC Photo)

His experience also includes military service as an armor officer in the United States Army.  He spent the majority of his active service with the 3rd Squadron, 2nd Armored Cavalry Regiment in Amberg, Germany, serving as a cavalry platoon leader and troop executive officer.  While on duty, Powell was seriously injured in a training accident and, after spending a year in the hospital, was retired from service.

Powell graduated in 1985 from the College of William and Mary, located in Williamsburg, Virginia, with a degree in Government.❖

## FCC Adopts Interoperability Standard To Ensure Effective Public Safety Communications Between Different Agencies

The Federal Communications Commission (FCC) adopted a Fourth Report and Order (Fourth R&O) and Fifth Notice of Proposed Rulemaking (Fifth Notice) on January 11, 2001, establishing a framework and issuing guidance that will allow public safety officials throughout the country to communicate with each other on designated interoperability channels in the 700 MHz band.

This interoperability is essential when different public safety agencies respond to emergencies using otherwise-incompatible equipment. The Commission has long noted that the inability of different public safety agencies to efficiently communicate with one another was a concern for the public safety community.

Establishing rules for the interoperability channels on the 700 MHz band will help prevent a physical disaster from becoming a communications disaster.

In the Fourth R&O, the Commission adopted Project 25 Phase I as the voice standard for communications on the 700 MHz band interoperability channels, which are channels specifically set aside to allow different public safety entities to communicate with one another. The Public Safety National Coordination Committee (NCC), a group chartered under the Federal Advisory Committee Act to advise the Commission on various issues related to the 700 MHz public safety band, recommended the adoption of the Project 25 Phase I standard.

This standard will ensure that all radios with voice capability on the 700 MHz band will have the ability to communicate with each other on designated interoperability channels. The Commission also adopted the data standard incorporated in the Project 25 suite of standards for data communications on the 700 MHz band interoperability channels. These channels will allow public safety entities, such as police and fire departments, to send status messages or short e-mails to one another.

By adopting the Project 25 Phase I standard, the Commission promotes the development of public safety equipment in the 700 MHz band and facilitates the effective use of that band by public safety entities.

In a related matter, in the Fifth Notice, the Commission seeks comment on the issue of migration to an efficiency standard of one voice path per 6.25 kHz on the General Use channels. Because the Commission believes that eventual adoption of such an efficiency standard would be in the public interest, it seeks further comment on the proper migration path to a 6.25 kHz efficiency standard.

To encourage early use of the 700 MHz spectrum, the Commission concluded in the Fourth R&O that (1) the earliest date the Commission would require 6.25 kHz technology would be December 31, 2005, (2) any 12.5 kHz-based systems constructed and placed in operation prior to December 31, 2005 will be able to continue to purchase and deploy 12.5 kHz equipment for system expansion or maintenance, and (3) any 12.5 kHz systems constructed and placed in operation prior to December 31, 2005 will not be required to cease operations and convert to 6.25 kHz technology prior to December 31, 2015, at the earliest.

The Commission also took other actions to facilitate interoperability in the 700 MHz band. Given the primary role the states have in responding to disaster situations, the Commission concluded that states should develop and administer plans for using the interoperability channels. In the event a state is unable to develop and administer an interoperability plan, the state may delegate this function to the 700 MHz band Regional Planning Committee (RPC).❖

(Courtesy of the FCC)