National Security and Emergency Preparedness

Telecom News

2003, NSTAC Special Edition

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

Table of Contents

Dr. Vance D. Coffman (left), Chairman and Chief Executive Officer of Lockheed Martin and Chair of the President's National Security Telecommunications Advisory Committee (NSTAC), opens the NSTAC XXVI Executive Session held in Washington, D.C. on April 30, 2003. Alongside Dr. Coffman is Mr. Robert Liscouski, the Department of Homeland Security's Assistant Secretary for Infrastructure Protection. (Photo by Ms. Donna Burton, Defense Information Systems Agency)

NSTAC at 20: Providing National Security Telecommunications Policy Expertise for Two Decades

In celebrating its 20th anniversary, the President's National Security Telecommunications Advisory Committee (NSTAC) marks a milestone achievement in the history of industry and Government collaboration. Established in 1982 by Executive Order 12382, President's National Security Telecommunications Advisory Committee, the NSTAC continues to be at the forefront of emerging national security and emergency preparedness (NS/EP) communications issues.

Composed of up to 30 industry leaders, NSTAC members are presidentially appointed chief executives from the telecommunications, aerospace, hardware, software, and other relevant

NSTAC at 20, page 3

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

Corporate Leaders from Lockheed Martin and BellSouth Appointed Chair and Vice Chair of NSTAC

On August 9, 2002, President George W. Bush announced the appointment of Dr. Vance Coffman, Chairman and Chief Executive Officer (CEO) of Lockheed Martin Corporation, as Chair of the President's National Security Telecommunications Advisory Committee (NSTAC). Dr. Coffman replaced the outgoing NSTAC Chair, Raytheon's CEO Mr. Daniel Burnham. The President also designated Mr. F. Duane Ackerman, Chairman and CEO of BellSouth, as NSTAC's Vice Chair.

Dr. Vance Coffman
Chairman & CEO,
Lockheed Martin Corp.

Dr. Coffman was elected to his current position at Lockheed Martin in April 1998 after having served as CEO and Vice Chairman since August 1997. He has also served in a number of other corporate leadership positions at Lockheed Martin, including President, Chief Operating Officer (COO), Executive Vice President, and President and COO of the company's Space & Strategic Missiles Sector. Before the merger of Lockheed and Martin Marietta Corporation in 1995, Dr. Coffman served as Lockheed's Executive Vice President, Vice President, and President of the Space Systems Division. While President of the Space Systems Division, he was responsible for oversight of the Hubble Space Telescope, the MILSTAR satellite communications program, the Follow-On Early Warning System (now called Space Based Infrared System), and for work on Iridium.

Dr. Coffman was elected to the Board of Directors of 3M in February 2002, the United Negro College Fund in October 2001, and Bristol-Myers Squibb in January 1998. He is a member of the National Academy of Engineering and the Security Affairs Support Association. In 1989, he received Iowa State University's Professional Progress in Engineering Award, and in 1999 he earned a Distinguished Achievement Citation from Iowa State.

Born in Kinross, Iowa, on April 3, 1944, he earned a bachelor's degree in aerospace engineering from Iowa State University and a master's and doctorate degree in aeronautics and astronautics from Stanford University.

Dr. Coffman holds an Honorary Doctorate of Aerospace Engineering from Embry-Riddle University and an Honorary Doctorate of Law from Pepperdine University's George L. Graziadio School of Business and Management. He was elected a Fellow in both the American Institute of Aeronautics and Astronautics and in the American Astronautical Society.

Mr. F. Duane Ackerman
Chairman & CEO,
BellSouth Corp.

Mr. Ackerman began his communications career in 1964 and has served in numerous capacities with BellSouth. In November 1992, he was named President and CEO of BellSouth Telecommunications, BellSouth's local telephone service unit and largest subsidiary.

On January 1, 1995, Mr. Ackerman was promoted to Vice Chairman and COO of the parent company, BellSouth Corporation, and was promoted to the position of President and CEO on January 1, 1997. A year later to the day, he was appointed Chairman and CEO.

In addition to serving on the Board of Directors of BellSouth Corporation, Mr. Ackerman is also a member of the Board of Directors of Wachovia Corporation and the Allstate Corporation.

His civic commitments include immediate past Chair of the Georgia Research Alliance and membership on the Board of the Woodruff Arts Center. Mr. Ackerman is the Chairman of the National Council on Competitiveness, a trustee of Rollins College, and a former member of the Board of Governors for the Society of Sloan Fellows of the Massachusetts Institute of Technology (MIT).

Early in 2000, Mr. Ackerman accepted the National Association for the Advancement of Colored People's (NAACP) prestigious Corporate Image Award on behalf of BellSouth. The award, presented during the 31st Annual NAACP Image Awards Gala in Pasadena, California, is given each year to a corporation whose business practices and public service depict an exemplary positive image to millions of people worldwide.

Mr. Ackerman, a native of Plant City, Florida, holds a bachelor's degree in physics, a master's degree from Rollins College in Winter Park, Florida, and a master's degree in business from MIT.

NSTAC at 20, continued from page 1

industries. The committee works in partnership with the Federal Government through the National Communications System (NCS), an interagency consortium of 23 Federal departments and agencies that serves as the focal point for industry/Government NS/EP communications planning and response. Since its inception, the NSTAC has advised four Presidents and six Administrations and has proven itself adept at responding to new challenges related to changes in technology and national priorities. As the NCS continues its transition to the Department of Homeland Security (DHS), the NSTAC, in keeping with its long, supportive history, will continue to provide essential guidance through its new Executive Agent – the Secretary of Homeland Security.

AT&T's Mr. Frank Ianna (left) and Boeing's Mr. James Albaugh – two of eight new members appointed on April 24, 2003, to the President's National Security Telecommunications Advisory Committee (NSTAC) – take part in discussions during the NSTAC Executive Session, held April 30, 2003, in Washington, D.C. Mr. Ianna is President of AT&T Network Services, while Mr. Albaugh is President and Chief Executive Officer of Boeing Space and Communications. (Photo by Ms. Donna Burton, Defense Information Systems Agency.)

NSTAC: The Past and Present

Several factors during the early 1980s provided the impetus for the NSTAC's establishment. First, comprehensive command, control, and communications capabilities became ever more important in executing military and disaster-response operations, and the Government became increasingly reliant upon privately owned commercial communications systems to conduct its business. In addition, the telecommunications industry rapidly evolved and changed as competition and new services were introduced into the marketplace, and the Government needed a forum through which to remain abreast of new advances and to assess the impact of those new technologies on NS/EP activities. Finally, with the divestiture of AT&T, the Government lost its single point of contact within the telecommunications industry to coordinate NS/EP efforts. Consequently, the establishment of the NSTAC provided the necessary formal mechanism to continue

NSTAC at 20, page 4

NSTAC at 20, continued from page 3

to effectively facilitate industry/Government cooperation in the post-divestiture environment.

During its early years, the NSTAC focused its efforts on concerns over the Government's growing reliance on commercial telecommunications services.

As the telecommunications network continued to evolve, however, NS/EP communications planning and response also became increasingly complex and critically dependent on information infrastructures, demanding an innovative means of protecting the Nation's public and private communications assets. In response, the NSTAC amended its focus to include planning and response issues.

In the years since its inception, NSTAC activities have led to the development of both technical reports with recommendations to the President and operational programs that provide essential telecommunications capabilities to the Nation's Government personnel and first responders during times of crisis. For instance, the National Coordinating Center (NCC) for Telecommunications, an industry/Government coordination center for day-to-day operational support to NS/EP telecommunications activities, was created as a result of a series of recommendations that the NSTAC made to the President in 1984. Today, the NCC plays a vital role in the initiation, coordination, restoration, and reconstitution of NS/EP communications services and/or facilities.

More recently, the NSTAC played a key role in the designation of the NCC as the Telecommunications Information Sharing and Analysis Center (Telecom – ISAC) when it concluded in its Operation Support Group report of June 1999 that the NCC already performed the primary functions of the ISAC for the telecommunications sector and that industry and Government should establish it as such. In January 2000 the National Security Council concurred with the NSTAC and designated the NCC as the Telecom – ISAC. This Center, which collects and analyzes data on threats and vulnerabilities to better protect the national communications infrastructure, was also the first ISAC to include both industry and Government participation. In addition, the Priority Service and Internet Technology and Standards Program was established in 1999 as a result of a recommendation from the Network Group's Internet Report: An Examination of the NS/EP Implications of Internet Technologies issued in June 1999.

Ms. Susan Spradley (left), President of Wireline Networks for Nortel Networks, listens to discussion on national security telecommunications issues with Mr. Herbert W. Anderson, President of Northrop Grumman Information Technology, during the 26th meeting of the President's National Security Telecommunications Advisory Committee. The meeting was held April 30, 2003, in Washington, D.C. (Photo by Ms. Donna Burton, Defense Information Systems Agency.)

To gain a wide range of perspectives for its recommendations, NSTAC and its various task forces work with numerous industry and Federal bodies, including the Federal Communications Commission's Network Reliability and Interoperability Council (NRIC), the National Telecommunications and Information Administration (NTIA), the National Infrastructure Assurance Council (NIAC), the White House Office of Science and Technology Policy (OSTP), and the National Institute of Standards and Technology (NIST). NSTAC task forces have worked with these organizations to examine such issues as the network security implications of Internet technologies, "last mile" bandwidth availability, intrusion detection, information sharing, network convergence, and research and development activities.

In 1982, when President Ronald Reagan established the NSTAC, he sought advice on the implementation of the country's national security policy from the perspective of the telecommunications industry. Twenty years later, the NSTAC continues to provide valuable advice to the President in five critical mission areas: critical infrastructure protection, information assurance, network convergence, information sharing, and outreach.

Critical Infrastructure Protection

The well being of the Nation and its ability to sustain national security missions depends on secure and reliable infrastructures. The manipulation of the telecommunications, energy, transportation, and banking and finance infrastructures, would be detrimental to the welfare of the United States. During the mid-1990s, the President acknowledged such interdependencies and encouraged the private sector to actively participate in the protection of critical infrastructures from both physical and cyber attacks.

Following the September 11, 2001, terrorist attacks, the NSTAC played a leading role in helping the Government understand potential vulnerabilities and in developing policy recommendations to mitigate associated risks. Building on previous infrastructure specific assessments, the NSTAC analyzed physical security threats and possible remedies to critical telecommunications infrastructure sites, focusing, in particular, on trusted access issues, concentration of critical telecommunications assets in telecom hotels, and the resiliency of Internet peering points.

The NSTAC also fostered cooperation and information sharing initiatives across all critical infrastructures, including the electrical power, transportation, and financial services industries.

Information Assurance

The Nation relies on the information and communications infrastructure to function successfully, and the NSTAC is actively involved in efforts to address cyber-related vulnerabilities, network security issues, and wireless technology vulnerabilities that threaten this infrastructure. The launch of several distributed denial of service attacks and the propagation of malicious worms in the last few years have demonstrated how easy it is for nefarious actors to exploit cyber vulnerabilities. In addition, the growing reliance on mobile e-services and applications has rendered security of wireless protocols and systems an issue of concern, especially when related to NS/EP communications transiting wireless networks and technologies.

Network Convergence

The late 1990s saw a fundamental shift in the overall architecture of the telecommunications network as many telecommunications carriers chose to leverage components of both the circuit-switched and packet-based network infrastructures resulting in a period of network convergence before the full transition to the next generation network. Over the past several years, the NSTAC has focused much attention on the NS/EP consequences of the converged environment, especially as it relates to such NS/EP communications programs as the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP) system. Acting on the advice of the NSTAC, the NCS increased its participation in standards bodies and the Executive Office of the President formed an interagency Convergence Working Group to address issues associated with network convergence.

Information Sharing

While the NSTAC has long recognized the value of information sharing—since it recommended the establishment of the NCC in 1983—other public and private sectors only more recently recognized its true value. In the late 1990s, the NSTAC set out to better understand existing and proposed channels with which the telecommunications industry shares information. The NSTAC observed that information sharing depends on receiving a benefit when voluntarily shared, is based on trusted relationships, and may be affected by legal barriers. Through its Network Security Information Exchange (NSIE) and its task forces, the NSTAC continues to examine information sharing, especially as it relates to critical infrastructure protection and legislative and regulatory activities.

Outreach

Through outreach efforts such as symposia, published reports, and interaction with public and private sector leaders, the NSTAC fosters the exchange of information between NS/EP stakeholders. The NSTAC provides technical analyses and develops risk assessments with other commercial industries to heighten the awareness of cross-sector information assurance and infrastructure protection issues. The NSTAC also actively encourages the exchange of ideas among representatives from industry, Government, and academia through research and development (R&D) exchanges. Since 1991, the NSTAC has sponsored five R&D exchanges.

NSTAC: The Future

During the past 20 years, the NSTAC has been an integral member in one of the Nation's most successful public-private partnerships. As the NCS transitions to the DHS and the Government continues to explore new ways to protect its home front and critical infrastructures—physical and virtual—the NSTAC will continue to play an important role in furthering NS/EP priorities.

The NSTAC continually re-evaluates its relevance to the changes in technology and in the geopolitical landscape—adapting its priorities appropriately. During the next few years, it will study and provide recommendations to the President and the Administration on issues related to network and cyber security, critical infrastructure protection, infrastructure interdependencies, physical security, satellite security, and information sharing.

The NSTAC members and the entities they represent are committed to the partnership in support of national security and emergency preparedness on behalf of the United States and look forward to serving the President for another 20 years.

National Security Telecommunications Advisory Committee Plays a Significant Role in Emergency Services and Homeland Security

Historically, one of the President's National Security Telecommunications Advisory Committee's (NSTAC) flagship missions has been to advise the President of the United States on the feasibility of implementing specific measures to improve the telecommunications aspects of the United States' national security posture. National security and emergency preparedness (NS/EP) communications enable Government to make an immediate and coordinated response during emergency situations, whether caused by a natural disaster or an intentional act.

As a result of its 20 years of dedicated service to the Executive Office of the President, the NSTAC was well positioned to respond to the changing threats against and the shifting needs of the Nation by helping the Government understand infrastructure vulnerabilities and by developing possible remedies to mitigate risks. One of the critical lessons learned from the response to the terrorist attacks was the ramification of losing key telecommunications assets on the ability of NS/EP users to communicate and the economy's ability to operate.

In part due to the NSTAC's recommendations to the President over several years, NS/EP users at the Federal, State, and local levels now have several mechanisms that help emergency responders communicate.

Supporting NS/EP Users Through Priority Services

One of the first issues that the NSTAC addressed after its creation in 1984 was the need for a system to assign priority provisioning and restoration of critical NS/EP telecommunications services in the hours immediately following a disaster. For more than five years, beginning in 1985, the NSTAC's Telecommunications Service Priority (TSP) Task Force worked with the Office of the Manager, National Communications System (OMNCS) to resolve the legal, regulatory, and operational issues involved in providing priority provisioning and restoration services.

Dr. J. Robert Beyster (left), Chairman and Chief Executive Officer (CEO) of Science Applications International Corporation (SAIC); Mr. Donald J. Obert (center), Group Executive, Network Computing for Bank of America; and Mr. Daniel P. Burnham, Chairman and CEO of Raytheon Company, discuss agenda items prior to the President's National Security Telecommunications Advisory Committee meeting, held April 30, 2003, in Washington, D.C. (Photo by Ms. Donna Burton, Defense Information Systems Agency.)

As a result of these efforts, the Federal Communications Commission (FCC) created the TSP system through a Report and Order issued on November 17, 1988. Under that Report and Order, the FCC tasked the OMNCS to establish the Office of Priority Telecommunications (OPT) to support these requirements. The OPT is responsible for coordinating requests for priority provisioning and restoration from NS/EP telecommunications users with the telecommunications carriers serving those users. According to Ms. Deborah Bea, a telecommunications specialist with the OPT, more than 52,000 circuits are protected today under TSP, most of which service State and local agencies.

The close working relationship between the NSTAC and the OMNCS enhanced the implementation of the TSP program, as both the provisioning and restoration of circuits rely heavily on the public switched telephone network operated by NSTAC member companies. The importance and efficiency of TSP was clearly demonstrated during the hours and days following the terrorist attacks on September 11, 2001, when the NCS processed nearly 600 TSP provisioning requests to support the response effort. According to Ms. Bea, between September 11, 2001, and July 1, 2002, 7,600 TSP provisioning and restoration requests were made – nearly 4,200 more than in the same period the previous year.

The NSTAC also played an important role in the development of the Government Emergency Telecommunications Service (GETS) program, which provides priority queuing of calls across the public switched telephone network for NS/EP users. Specifically, the NSTAC's Enhanced Call Completion (ECC) Task Force provided assistance to the Government in obtaining approvals for the High Probability of Call Completion standard in 1993.

Supporting Changing NS/EP Requirements with Wireless Priority Service

The need for a priority service that works on cellular networks was first identified after Federal emergency communications coordinators, along with other Federal, State, and local responders, encountered frequent blocking of cellular calls when responding to Hurricanes Andrew and Iniki in 1992. The NSTAC studied the concept of priority treatment on the cellular network in its ECC Task Force and the NSTAC NS/EP Panel, which documented lessons learned from responses to the hurricanes.

In July 1994, NSTAC's Wireless Services Task Force established the Cellular Priority Access Services (CPAS) Subgroup to investigate the technical, administrative, and regulatory issues associated with the deployment of a nationwide priority access capability for NS/EP cellular users. The CPAS recommended to the President in 1995 that a wireless priority service (WPS) be made available to NS/EP users. That year, the OMNCS began to develop such capabilities, and in 1998, the FCC adopted the First Report and Order (R&O) for Priority Access Service (PAS). [In July 2000, the FCC adopted the Second R&O for PAS, establishing the regulatory, administrative, and operational framework that enabled commercial mobile radio service providers to offer WPS.]

After renewed interest by President Bush and the first responder community following September 11, 2001, WPS was activated in Washington D.C. and New York City in May 2002. Additional markets came online in late 2002 and in 2003. The NSTAC continues to be involved in WPS program development by providing advice on potential barriers to ubiquitous nationwide rollout and other policy-related issues. (See the story on Wireless Task Force activities for more details.)

NSTAC's Homeland Security Role

For the entire NS/EP community and the members of the NSTAC, the events directly following the September 11, 2001, attacks reaffirmed the importance of their missions and the criticality of communications. In the months following the attacks, the NSTAC compiled a list of lessons learned and discussed the NSTAC's future role in homeland security with Government officials. The recommendations from the lessons learned included: (1) the need for standard access control procedures at disaster sites; (2) the need to deploy priority services for NS/EP users over wireless networks; (3) support for emergency telecommunications services standards; and (4) protection of critical infrastructure information, that industry voluntarily shares with Government, from disclosure under the Freedom of Information Act.

In response to the attacks and increased possible threats to the Nation's networks, the Bush Administration quickly worked to develop national strategies for homeland security, protection of critical infrastructures and key assets, and cyber security. Many important themes in these strategies are relevant to the NSTAC's mission and are reflected in issues under consideration for study by the NSTAC:

- the National Strategy for Homeland Security proposed the Department of Homeland Security, calling for the protection of physical and virtual assets to be managed through an Information Analysis and Infrastructure Protection Directorate. The plan also recognized the need for a strong partnership with the private sector in order to succeed in this area;
- the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets acknowledged that consolidated key infrastructure assets could be targets for terrorists in the future. Specifically, it said "Because the government and critical infrastructure industries rely heavily on the public telecommunications infrastructure for vital communications services, the [telecommunications] sector's protection initiatives are particularly important";

NSTAC Role in Emergency Services, page 10

Wireless Task Force Provides Recommendations on the Ubiquitous Rollout of Wireless Priority Service and Wireless Security Vulnerabilities

During the President's National Security Telecommunications Advisory Committee's (NSTAC) XXVI cycle, the Wireless Task Force (WTF) studied two wireless issues integral to national security and emergency preparedness (NS/EP) activities – the ubiquitous deployment of wireless priority service (WPS) and the secure operation of wireless technology in support of NS/EP stakeholders.

Deploying Wireless Priority Service

As part of the response to the September 11, 2001, terrorist attacks, the National Communications System (NCS), in concert with the White House, requested that the Nation's commercial mobile radio services providers work with the OMNCS and its service integrators to implement WPS on an expedited basis.

The importance of WPS was again emphasized during the March 2002 meeting of NSTAC, when Senator Robert Bennett of Utah requested that NSTAC revisit the WPS issue and further examine obstacles to its ubiquitous rollout. Consequently, in May 2002, the NSTAC's Industry Executive Subcommittee (IES) established the WTF to assess the circumstances surrounding the WPS rollout.

As part of its study, the WTF closely monitored WPS deployment. Task force members noted that the ubiquitous deployment of the program had not been achieved for a variety of operational, technical, financial, and regulatory reasons. However, they agreed that ubiquitous, nationwide deployment of WPS would be achieved if the Government included all wireless technologies in the solution set, used satellite back-up capabilities, and encouraged the participation of large and small wireless carriers.

In continuing their research, the task force members cited inadequate Government funding, a lack of liability protection for carriers, and technological limitations as additional impediments to ubiquitous rollout of WPS. Lastly, task force members determined the need for an effective WPS outreach campaign to State and local governments, smaller wireless carriers, private sector critical infrastructure protection providers, and the general public.

In its report to the President, Wireless Priority Service, the NSTAC recommended that the President encourage the development and deployment of WPS solutions for all wireless technologies to maximize WPS coverage, increase ubiquity, and give NS/EP users the flexibility to handle a variety of emergencies and disasters. The NSTAC also recommended that the President reaffirm the Federal Communications Commission's (FCC) Second Report and Order on Priority Access Service to extend liability protection to wireless priority solution providers that would be equivalent to the liability protection found in wireline priority communications programs.

In addition, the NSTAC recommended that the President encourage and support adequate funding for the development and deployment of a multi-technology and multi-carrier WPS program, including a satellite backup capability. Finally, the NSTAC recommended that the President direct the appropriate departments and agencies to conduct outreach and educational campaigns regarding WPS and its role in homeland security, specifically targeting: State and local governments, small carriers, private sector critical infrastructure providers, and the general public.

Securing Wireless Technologies

During that same NSTAC XXV Meeting Business Session, the NSTAC Principals addressed the topic of security vulnerabilities in wireless communications devices and networks. Because wireless technologies transmit voice, data, and video in support of NS/EP operations, the Principals agreed that the NS/EP community needed to identify its wireless security requirements and better understand any potential wireless vulnerabilities.

The Principals noted that wireless security challenges existed at many levels, including product design, wireless standards, wireless/Internet convergence, and implementation of existing security features. As a result, the NSTAC, through its IES, tasked the WTF to determine how NS/EP stakeholders could operate in a secure wireless environment and asked the WTF to provide conclusions and recommendations regarding wireless security.

To adequately discuss such subjects and formulate actionable recommendations designed to help offset wireless threats and vulnerabilities, the WTF agreed to: (1) define the terms "wireless" and "wireless security"; (2) identify NS/EP wireless users' unique

WTF, page 11

Discussion with President Bush Highlights 26th NSTAC Meeting

President George W. Bush and Secretary of Homeland Security Tom Ridge meet with members of the President's National Security Telecommunications Advisory Committee (NSTAC) in the White House's Roosevelt Room on April 30, 2003. (White House photo)

A meeting with the President on key telecommunications issues highlighted the 26th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) held April 30, 2003, in Washington, D.C.

The NSTAC activities began in the White House's Roosevelt Room. There, the NSTAC Principals, led by the NSTAC Chair, Lockheed Martin Chairman and Chief Executive Officer Dr. Vance Coffman, held discussions with President George W. Bush on telecommunications challenges facing the Nation. These challenges not only relate to national security and emergency preparedness (NS/EP), but also to the challenges facing the Administration as it strives to overcome terrorist threats—both domestically and globally.

Following the meeting with President Bush, the Principals moved from the White House to the Department of the Treasury's Cash Room for the group's executive session. In his opening remarks, Dr. Coffman welcomed several NSTAC Principals recently appointed by President Bush. Those principals are: Mr. Frank Ianna, AT&T; Mr. Richard Notebaert, Qwest Communications; Ms. Patricia Russo, Lucent Technologies; Mr. Stratton Sclavos, VeriSign; Ms. Susan Spradley, Nortel Networks; Mr. James Albaugh, Boeing; and Mr. John Stanton, T-Mobile USA and Western Wireless, representing the Cellular Telecommunications Industry Association, which is also a new NSTAC member organization.

An eighth new member, Dr. Hector de J. Ruiz of Advanced Micro Devices (AMD), was unable to attend.

During the meeting, the NSTAC Principals reviewed the efforts of the last year and then identified several issues, with Federal Government telecommunications and critical infrastructure leaders, for consideration as NSTAC starts a new work cycle. These issues include information sharing, national policies and/or regulatory issues affecting telecommunications, critical facilities vulnerabilities, trusted access to communications facilities, and the commercial satellite industry and security. Through the discussions, the Principals began to shape and formulate their agenda and work plan. In describing the NSTAC meeting, Dr. Coffman stated that, "it is an honor—and a pleasure—to serve as the Chair of NSTAC during this critical time of peace and security."

Those providing the Government perspective to NSTAC on critical issues included Mr. Robert Liscouski, the Department of Homeland Security's Assistant Secretary for Infrastructure Protection; Admiral Steve Abbot, Acting Homeland Security Advisor;
Dr. John Marburger, the President's Science and Technology Advisor;
Mr. Paul Kurtz, Special Assistant to the President Critical Infrastructure Protection; Mr. Howard Schmidt, formerly the President's Cyberspace Security Advisor; and Lieutenant General Harry D. Raduege, Jr., Director of the Defense Information Systems Agency and former Manager of the National Communications System.

The meeting concluded with a reception hosted by Lockheed Martin, BellSouth, and the Department of Homeland Security at the Metropolitan Club. The social featured remarks by the Honorable Tom Ridge, Secretary of Homeland Security.

NSTAC Role in Emergency Services,
continued from page 7

- the National Strategy to Secure Cyberspace provided an initial framework for organizing and prioritizing cybersecurity efforts. Its first priority was to develop a national cyberspace security response system, requiring a strong partnership between industry and Government to perform analyses, issue warnings, and coordinate response efforts to cyber attacks.

The NSTAC members, having studied network security and critical infrastructure protection for over a decade, are well prepared to advise the President in these areas. Since 1990, the NSTAC has provided the President with recommendations on information security, including the security of the public switched network, wireless security, network vulnerabilities, and issues related to the convergence of the public network and the Internet. In 1991, the NSTAC formed the Network Security Information Exchange (NSIE) to work in partnership with the Government's NSIE on addressing the vulnerabilities of the Nation's communications systems to electronic intrusion. The NSTAC has also contributed comments to the National Plan for Information Systems Protection and the National Strategy to Secure Cyberspace.

Critical infrastructure protection and infrastructure dependencies have also been primary topics for study by the NSTAC. In direct response to the lessons learned from September 11, 2001, response efforts, the NSTAC's Vulnerabilities Task Force (VTF) studied the risks associated with consolidated telecommunications assets in telecom hotels and trusted access issues in 2002 and 2003. (See story on VTF activities for more details).

Further, the NSTAC has also performed information assurance risk assessments during the past 6 years for the electric power and transportation sectors. Most recently, the NSTAC's Industry Executive Subcommittee (IES) established the Financial Services Task Force to define areas of critical concern to the financial services sector; determine whether or how the telecom industry meets or addresses these concerns; and identify issue commonalities with other sectors.

As Rockwell Collins President and Chief Executive Officer Clayton Jones (right) listens, Mr. Craig Mundie, Senior Vice President and Chief Technical Officer for Advanced Strategies and Policies with Microsoft Corporation, responds to a discussion point during the 26th meeting of the President's National Security Telecommunications Advisory Committee, held April 30, 2003, in Washington, D.C. (Photo by Ms. Donna Burton, Defense Information Systems Agency.)

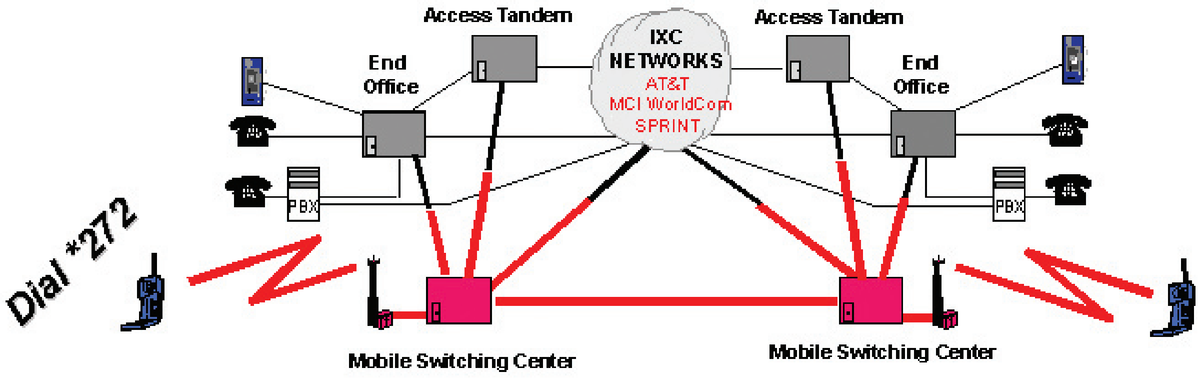
Future Roles for the NSTAC

The shift in the political agenda in Washington D.C. to homeland security is dramatically increasing awareness of NS/EP, network security, and critical infrastructure issues; however, the role of the NSTAC will remain virtually unchanged as it has been addressing these issues for more than 20 years. While the NSTAC will now report to the President through the Department of Homeland Security—due to recent changes to Executive Order 12382—it will continue to advise the President on the critical issues facing national security and telecommunications.

Over the coming years, the NSTAC will continue to ensure that it accommodates the NS/EP users' communications needs. This includes ensuring the physical security of key assets, security over the public switched network and wireless networks, and making sure appropriate standards bodies are aware of NS/EP requirements. The increased dependence of the NS/EP user on wireless devices will also drive the NSTAC agenda with possible investigations on the improvement of wireless security and priority provisioning of wireless networks during emergencies and the usage of commercial satellite services during NS/EP missions.

The NSTAC is best positioned to provide expert advise to the President, as well as Federal, State and local governments, and industry, and will continue to be, an essential asset to this Nation.

WTF, continued from page 8



Wireless Priority Service FOC Solution (As Planned)

requirements; (3) compile a list of wireless vulnerabilities and threats; and (4) where known, identify mitigation approaches to address wireless vulnerabilities and threats.

Through the input and assistance of subject matter experts from NSTAC member companies, other information technology companies, industry associations, and the Federal Government, the WTF concluded that wireless security challenges existed at many levels, including product design, wireless standards, and wireless/Internet convergence.

Based on its analysis of issues related to wireless security, the NSTAC compiled its Wireless Security report, offering a series of recommendations to the President. The NSTAC recommended that the President direct Federal departments and agencies to construct mitigation and alleviation policies regarding wireless vulnerabilities and further consider the applicability of the recent National Institute of Standards and Technology (NIST) and Department of Defense wireless security policies. Noting that the banning of wireless devices was counterproductive and ignored the efficiency that such devices brought to users, the NSTAC also recommended that the President direct Government chief information officers to immediately emphasize enterprise management controls with respect to wireless devices and ensure that appropriate security controls were implemented.

In its report, the NSTAC asked for Federal departments and agencies to work in concert with industry to develop security principles and to resolve security-related deficiencies in wireless devices when employed by NS/EP users. The report also asked for those same agencies using wireless communications to address wireless security threats and vulnerabilities by considering the end-to-end security of their respective communications and information system capabilities and purchasing and implementing fully tested and compliant secure wireless products and services.

The NSTAC recommendation also directed appropriate staff to advocate funding initiatives for replacing nonsecure analog with secure digital NS/EP equipment and systems and directed Federal departments and agencies using microwave communications facilities to address unprotected link security vulnerabilities. In addition, the recommendation also advised State and local governments and other critical infrastructure providers of the vulnerability of unprotected microwave communications as part of the homeland security initiative.

Finally, the NSTAC recommended that the President establish policies regarding limits on the public availability and dissemination of Federal critical infrastructure information (such as the Federal Aviation Administration databases listing tower locations).

NSTAC reports are available on the NCS web site at http://www.ncs.gov/nstac/nstac

Legislative and Regulatory Task Force Addresses Complex Policy Issues During NSTAC XXVI Cycle

Through the work of its Legislative and Regulatory Task Force (LRTF), the President's National Security Telecommunications Advisory Committee (NSTAC) supplied the President with top-level industry advice for supporting the continued rollout of the National Communications System's (NCS) Priority Access Service (PAS) and deterring cyber crime during the past year.

Ensuring Priority Access Service

The impetus for the NSTAC's assessments and recommendations on priority access service dates back to the March 2002 NSTAC XXV Meeting Business Session. There, NSTAC members determined that it would be valuable to study wireless PAS during the NSTAC XXVI cycle and subsequently tasked its Wireless Task Force (WTF) to research and analyze various technical and policy issues related to the ubiquitous rollout of PAS [now known as wireless priority service (WPS)]. The WTF then asked the LRTF to examine the legal and regulatory aspects of the Federal Communications Commission's (FCC) Second Report and Order for priority access service.

To broaden their knowledge of the issue, LRTF members received several briefings from the telecommunications industry and Government on a range of topics, including liability protections and technical limitations in the Report and Order, PAS funding by Congress, wireless interoperability, and how best to clarify the PAS Report and Order.

After giving careful consideration to the merits of reopening the PAS rulemaking, the LRTF concluded that revisiting the rules would be a lengthy process – one that could have the unintended consequence of slowing wireless priority service deployment. Therefore, the NSTAC decided to submit a letter to the President advising him on ways to spur Government action on PAS-related policy issues.

In its letter, the NSTAC advised the President to boost PAS deployment by first urging the FCC to accelerate its ongoing efforts to improve the communications interoperability of Federal, State, and local public safety agencies, and then restoring full Federal funding of the WPS program. The letter also clarified the task force's interpretation of the Report and Order's liability protections. It stated that the Report and Order language was to be interpreted to mean that wireless carriers, suppliers, manufacturers, and their agents providing priority access service shall have immunity from the legal liability from the proscription on preferential treatment in Section 202 of the Communications Act of 1934, "as is provided to wireline carriers offering Government Emergency Telecommunications Service (GETS) today."

Deterring Cyber Crime

On the cyber crime front, NSTAC XXV Business Session discussion touched on whether current laws governing intentional and malicious damage to public and private infrastructures through the Internet needed to be strengthened. From those discussions, the NSTAC Industry Executive Subcommittee (IES) tasked the LRTF to identify the existing legal penalties for committing intentional and malicious attacks on the Internet and to determine whether they should be strengthened and/or if additional penalties were needed.

In its letter, the NSTAC advised the President to boost PAS deployment by first urging the FCC to accelerate its ongoing efforts to improve the communications interoperability of Federal, State, and local public safety agencies, and then restoring full Federal funding of the WPS program.

During its deliberations, the LRTF recognized that many of the current cyber crime penalties had been either recently implemented or modified, making it difficult to assess their effectiveness over time. The

Rockwell Collins President and Chief Executive Officer, Mr. Clayton Jones (right) converses with Mr. Ken Kato, the Rockwell Collins Air Force Accounts Director, prior to the 26th meeting of the President's NSTAC. Mr. Kato serves on NSTAC's IES and advises Mr. Jones on NSTAC issues. (Photo by Ms. Donna Burton, Defense Information Systems Agency.)

U.S. Congress, for example, had just enacted two laws that modified the Computer Fraud and Abuse Act: the USA PATRIOT Act enacted into law on October 26, 2001, and the Homeland Security Act enacted into law on November 25, 2002. These new laws increased existing cyber crime penalties, made it easier to prosecute cyber crimes, and called for a review, and an amendment, if necessary, of sentencing guidelines for cyber crimes.

The LRTF membership, after reviewing such cyber crime penalties, concluded that existing Federal penalties were adequate for prosecuting cyber attacks. In its report, Penalties for Internet Attacks and Cyber Crime, the NSTAC stated that the, "recently modified Federal penalties were adequate for prosecuting Internet attacks because the penalties that now exist are very strong."

The report also proposed a series of recommendations for taking a "more well-rounded and proactive approach" to preventing and responding to cyber crimes, including suggestions for improving cyber crime efforts at the State level and on the international front. "State penalties for cyber crimes should be consistent with Federal penalties and must be strong enough to make the threat of State prosecution deter cyber crime throughout the Nation," the report stated. "In addition, States should have the necessary resources to train their personnel on how to address network vulnerabilities and respond effectively to cyber attacks."

Noting that the "vast majority" of Internet attacks in the United States have an international component, the NSTAC report emphasized the importance of forging positive diplomatic relations with other countries, "as the nature of the relationship often determines the level of cooperation for prosecuting" foreign hackers. As a first step to strengthening cyber crime prevention overseas, the NSTAC recommended that the President encourage Congress to ratify the Council of Europe (COE) Convention on Cybercrime, in conjunction with passing implementing legislation that would provide for the reimbursement of reasonable costs incurred by communications service providers responding to data preservation requests.

The NSTAC report also recommended that the President encourage other nations to adopt the COE Convention and to seek better cooperation among nations for locating and identifying cyber-criminals, gathering evidence to bring them to justice, and implementing procedures to more rapidly and effectively prevent and mitigate cyber attacks.

In its report, Penalties for Internet Attacks and Cyber Crime, the NSTAC stated that the, "recently modified Federal penalties were adequate for prosecuting Internet attacks because the penalties that now exist are very strong."

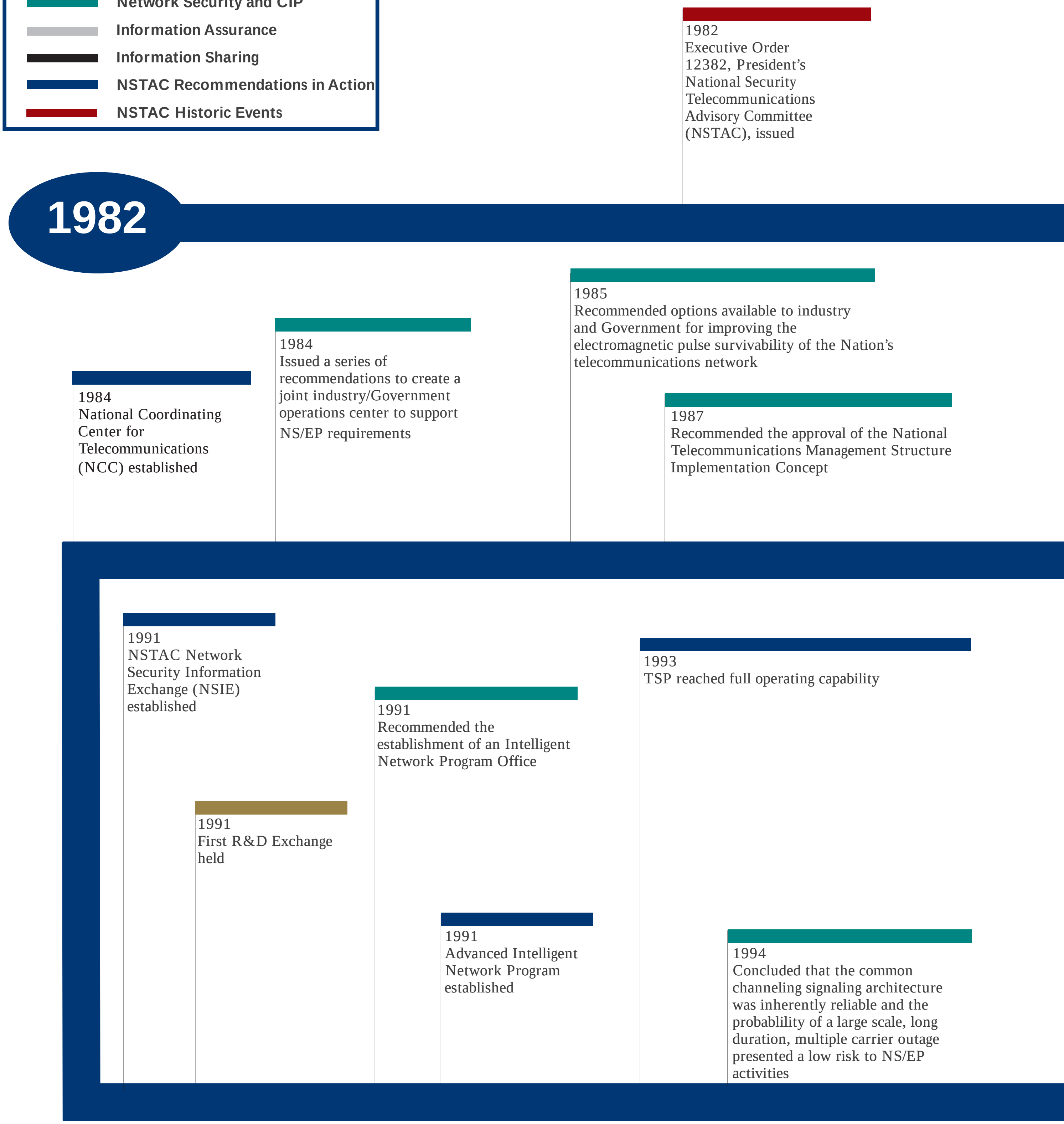
Continuing on the international front, the NSTAC report advocated working with U.S. international counterparts and through multilateral bodies, such as the G-8, COE, European Union, Organization of American States, and the Asia-Pacific Economic Cooperation to urge other nations to enact substantive and procedural laws implementing the provisions of the COE Convention. Further, the report suggested that other nations should be

LRTF, page 20

20 Years of Advising the President in Partnership:

KEYS

🟫	Outreach
🟩	Network Security and CIP
⬜	Information Assurance
⬛	Information Sharing
🟦	NSTAC Recommendations in Action
🟥	NSTAC Historic Events



🟥 1982
Executive Order 12382, President's National Security Telecommunications Advisory Committee (NSTAC), issued

🟦 1984
National Coordinating Center for Telecommunications (NCC) established

🟩 1984
Issued a series of recommendations to create a joint industry/Government operations center to support NS/EP requirements

🟩 1985
Recommended options available to industry and Government for improving the electromagnetic pulse survivability of the Nation's telecommunications network

🟩 1987
Recommended the approval of the National Telecommunications Management Structure Implementation Concept

🟦 1991
NSTAC Network Security Information Exchange (NSIE) established

🟫 1991
First R&D Exchange held

🟩 1991
Recommended the establishment of an Intelligent Network Program Office

🟦 1991
Advanced Intelligent Network Program established

🟦 1993
TSP reached full operating capability

🟩 1994
Concluded that the common channeling signaling architecture was inherently reliable and the probablility of a large scale, long duration, multiple carrier outage presented a low risk to NS/EP activities

* This timeline highlights many of the significant accomplishments of the NSTAC over the past 20 years; however, it is not an exhaustive representation of NSTAC activities. For a full description of NSTAC work, please see the NSTAC XXV Issue Review: 20th Anniversary Edition document located on the NCS web site at www.ncs.gov.

Significant Accomplishments of the NSTAC*

1982
NSTAC Charter developed

1983
NSTAC Bylaws adopted

1983
Advised the Department of State on the vulnerability and risk inherent in overseas leased networks and offered remedial measures

1984
Issued recommendations on how to reduce NS/EP dependence on automated information processing

1984
Identified telecommunications service priority (TSP) as an urgent issue for priority provisioning and restoration of NS/EP services for Federal, State, and local governments and private users

1987
Recommended the initiation of a study to identify options for ensuring survivable electric power

1988
Assessed the applicability of network management technology to NS/EP telecommunications survivability

1988
National Telecommunications Management Structure Program Office established

1990
Recommended continued Federal Government support and administration of the TSP system

1991
Recommended establishing an industry/Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion

1995
Tabletop CCS Restoration Exercise held

1995
Provided recommendations for the telecommunications industry for the next version of the National Plan and addressed industry concerns about disclosure of critical infrastructure protection-related information

1995
Worked closely with the President's Commission on Critical Infrastructure and other Federal organizations concerned with examining physical and cyber threats to the national critical infrastructure

1996
Telecommunications Act of 1996 passed

1996
Second R&D Exchange held

1997
Provided recommendations on the extent that the electric power infrastructure and financial service industries' operations depend on information systems and the telecommunications infrastructure

1997
NSTAC endorsed the creation of an Information Systems Security Board that would promote information systems security principles and standards

20 Years of Advising the President in Partnership:

1997
Issued recommendations to promote the R&D of intrusion detection technologies

1998
Issued its Year 2000 Problem Status Report

1998
Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, issued

1999
Priority Services and Internet Technology and Standards Program established

2000
Issued a report that concluded that historical and Y2K experiences demonstrate information sharing to be a worthwhile effort

2000
Examined current network security strategies to determine whether alternative strategies would diminish risk to the Internet

2000
Fourth R&D Exchange held at the University of Tulsa in Tulsa, Oklahoma

2001
Issued recommendations on the Wireless Priority Service (WPS) and wireless security and vulnerability issues

2001
Continued to monitor and track legislative activities affecting NS/EP telecommunications including network convergence and the next generation network

2001
Executive Order 13228, Office of Homeland Security and the Homeland Security Council, issued

2001
Executive Order 13231, Critical Infrastructure Protection in the Information Age, issued

2001
The USA Patriot Act passed

2001
GETS reached full operating capability

2001
TSP and GETS capabilities used to restore vital switches in New York's financial district and to give priority routing to 7,000 critical calls in Manhattan and Washington, D.C. after 9/11

* This timeline highlights many of the significant accomplishments of the NSTAC over the past 20 years; however, it is not an exhaustive representation of NSTAC activities. For a full description of NSTAC work, please see the NSTAC XXV Issue Review: 20th Anniversary Edition document located on the NCS web site at www.ncs.gov.

*Significant Accomplishments of the NSTAC**

1998
Third R&D Exchange held at Purdue University in West Lafayette, Indiana

1999
Issued recommendations for continued support for the efforts of the Department of Transportation to promote information sharing within the transportation infrastructure

1999
Made recommendations on the potential implications of Internet Protocol (IP) network and public switched network (PSN) convergence on existing NS/EP services

1999
Recommended the establishment of a permanent program to address NS/EP isssues related to the Internet

1999
Issued a report, for Industry Executive Subcommittee use, that details information sharing initiatives and entities and the legal barriers that might affect the sharing of information between telecommunications companies and the entities examined

2000
NCC designated as the Telecommunications Information Sharing and Analysis Center

2001
Issued a report that addresses barriers to information sharing, work with the US Space Command to further develop means for information sharing, and NSTAC input to the Administration's National Plan for Information Systems Protection

2001
Provided input to the Administration's National Plan for Critical Infrastructure Assurance

2001
Provided recommendation on the security and reliability of converged information and communications networks

2001
Issued a letter discussing access to disaster sites, communications procedures during emergencies, and industry representation in the NCC

2002
Recommended means for protecting against distributed denial of service attacks and securing the converged network control space

2002
Issued recommendations on bandwidth services in the last mile and the use of TSP to expedite last mile provisioning request

2002
Submitted input to the draft National Strategy to Secure Cyberspace

2002
Wireless Priority Service rollout

2003
Issued several reports that examined the risks associated with the concentration of critical telecom assets in telecom hotels and Internet peering points, vulnerabilities involving equipment chain of control, and trusted access procedures to telcom facilities

2003
Issued reports that discuss vulnerabilities in pervasive software and protocols and means to protect the "edge" of the Internet

2003
Fifth R&D Exchange held at the Georgia Institute of Technology in Atlanta, Georgia

2003
Issued report on penalties for Internet attacks and cyber crime

20th

Internet Security/Architecture Task Force Studies Ways to Protect the Internet Infrastructure and Reduce Cyber Vulnerabilities

Through its Internet Security/Architecture Task Force (ISATF), the NSTAC supplied the President with high-level advice and forward-thinking solutions for bolstering Internet security and architecture, including recommendations for identifying and remediating vulnerabilities in pervasive software/protocols and addressing the "edge elements" of the Internet.

> **"Streamlining the Government-funded groups would create a number of benefits for industry and Government," including reduced redundant activities, reporting requirements, and costs, the report stated. The NSTAC recommended establishing a lead organization within the Department of Homeland Security to coordinate a process with industry for warnings, notification, coordination, and remediation of widespread problems during a national emergency.**

Vulnerabilities in Pervasive Software/Protocols

In drafting its first report, *First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software/Protocols*, ISATF members noted that at the 25th Meeting of the National Security Telecommunications Advisory Committee (NSTAC) in March 2002, Mr. Richard Clarke, then Special Advisor to the President for Cyberspace Security, discussed the serious nature of threats posed by vulnerabilities within the domain name servers and the border gateway protocol.

From that and other discussions, task force members decided to first identify the vulnerabilities. Once they identified those weaknesses, task force members examined opportunities to assure the availability of resources for the analysis and remediation of security vulnerabilities in the pervasive software/protocols used on the Internet's infrastructure.

Many of the task force's discussions focused on how industry and Government could effectively share the critical information needed to address vulnerabilities in pervasive software/protocols. "Industry and Government cannot guarantee perfect system or network security. Therefore, it is essential that they effectively and efficiently share information to remain ahead of the threat as much as possible," the ISATF report stated.

On the basis of the ISATF analysis, the NSTAC made a variety of recommendations to the President. These recommendations included consolidating the Government-funded watch center operations of Federal agencies dedicated to the detection and dissemination of information related to Internet vulnerabilities into one organization. "Streamlining the Government-funded groups would create a number of benefits for industry and Government," including reduced redundant activities, reporting requirements, and costs, the report stated.

Further, the NSTAC recommended establishing a lead organization within the Department of Homeland Security to coordinate a process with industry for warnings, notification, coordination, and remediation of widespread problems during a national emergency.

The report also advocated funding efforts to identify and mitigate vulnerabilities in the most critical protocols or software relied upon within key sectors of the Nation's infrastructure.

"Edge Elements" of the Internet

During the NSTAC XXV Meeting, Mr. Clarke also expressed significant concern about the ability to protect the "edges" of the Internet against attack or exploitation. In response to those concerns, the NSTAC's Industry Executive Subcommittee (IES) tasked the ISATF to provide guidance to the President on how to define the edge of the Internet.

Following several months of discussion and analysis on this subject by task force members, the ISATF determined that because the Internet is a system of interconnected networks – and not a single network – the concept of a single edge is "impractical" and could not be defined. "There are many different interpretations and definitions of the edge of the Internet," the report stated. "Instead of a single edge, there is an ever-changing series of concentric circles that make up the Internet, extending all the way to the end device or user. This dynamic network of networks results in a perspective of the domain, under one's management control, based on where that individual sits in the overall architecture at any point in time," it said.

The task force members noted that while an Internet Service Provider's (ISP) view of the edge may be the end-user customer at a home computer, a backbone ISP may view the edge as the point where another ISP interconnects with the backbone network.

The ISATF agreed that because there is no single definition of the edge, protective measures should focus on defending the Internet as a whole. "By encouraging network operators to regularly scan, monitor, and maintain not only the perimeter but the interior of the network, the Internet as a fabric becomes stronger."

...the ISATF determined that because the Internet is a system of interconnected networks – and not a single network – the concept of a single edge is "impractical" and could not be defined. "There are many different interpretations and definitions of the edge of the Internet," the report stated. "Instead of a single edge, there is an ever-changing series of concentric circles that make up the Internet, extending all the way to the end device or user."

Thus, in its second report, Edge Elements of the Internet, the NSTAC advocated the continuation of Government efforts to identify the critical national security/emergency preparedness (NS/EP) missions and related functions that rely on the Internet and encouraged the parties responsible for those missions to ensure that they are adequately protected through redundancy and alternate capabilities.

The ISATF agreed that because there is no single definition of the edge, protective measures should focus on defending the Internet as a whole. "By encouraging network operators to regularly scan, monitor, and maintain not only the perimeter but the interior of the network, the Internet as a fabric becomes stronger."

Further, the NSTAC recommended ensuring that all products and services that compose the Internet have built-in baseline security features and that those capabilities are appropriately configured and kept up to date. The report also supported the development of a standard set of "key warnings and indicators" by Government, Internet security experts, and standards bodies for service providers to use as a baseline to measure security threats. "Although certain service providers can meet and exceed those baselines as a matter of customer service, standardized key indicators and warnings will provide earlier notice of national security level network events to downstream customers, upstream providers, and relevant security groups or Government organizations that may then react accordingly," the report stated.

The NSTAC believes that its recommendations to the President will help not only to improve Internet security in the near term, but also help to serve as a foundation for future work on the issue.

LRTF, continued from page 13

encouraged to adopt data preservation provisions of the sort set forth in the COE Convention, rather than data retention laws, which required retention ex ante of data regarding all communications on a network, and to dedicate well-trained and well-equipped personnel to combat cyber crime.

The NSTAC report made additional suggestions for industry and Government to pursue within the United States, including the coordination of a nationwide education campaign to increase public awareness of the penalties and consequences for committing Internet attacks. "Telecommunications service providers and infrastructure operators should also be encouraged to enter into non-disclosure agreements (NDA) that set a fixed amount of time for mitigating network incidents and vulnerabilities," the report stated.

Finally, the report recommended that companies implement common best practices for computer security that included specific ramifications for abuses, rather than lenient consequences. "With encouragement from the Government, companies could enhance their security practices, which can better secure Internet systems across the Nation."

In conclusion, the NSTAC's report stated that, "sufficient legal authority" exists in the United States to penalize and prosecute cyber criminals. Further, in the report, the NSTAC recognized that having sufficient legal penalties, "cannot completely stop cyber crimes altogether and that a more proactive and comprehensive approach to curbing cyber crime is necessary to protect the United States' critical networks."

President Bush Names Eight Senior Communications Executives to the NSTAC

On April 24, 2003, President George W. Bush announced the appointment of eight senior communications executives to the President's National Security Telecommunications Advisory Committee (NSTAC).

Named to the NSTAC were:

- Mr. James F. Albaugh, President and Chief Executive Officer (CEO), Space and Communications division of the Boeing Company;
- Mr. Frank Ianna, President of AT&T Network Services;
- Mr. Richard C. Notebaert, Chairman and CEO of Qwest Communications International, Inc.;
- Dr. Hector de J. Ruiz, President and CEO of Advanced Micro Devices, Inc. (AMD);
- Ms. Patricia F. Russo, Chair and CEO of Lucent Technologies;
- Mr. Stratton Sclavos, President and CEO of VeriSign, Inc.;
- Ms. Susan Spradley, President of Wireline Networks for Nortel Networks; and
- Mr. John W. Stanton, Chairman and CEO of Western Wireless and Chairman of T-Mobile USA, who will serve as the NSTAC Principal for the Cellular Telecommunications and Internet Association (CTIA).

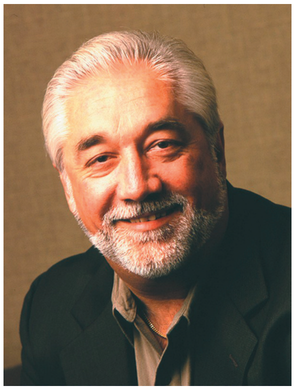
Mr. Albaugh, Boeing

Mr. Albaugh leads the Boeing Company's Space and Communications division – a nearly $10-billion, 43,000-person business unit that is the largest space-related enterprise in the world and the division charged with driving much of company's future growth. In his capacity as President and CEO, Mr. Albaugh provides strategic direction to nearly a quarter of Boeing's global workforce. Under his leadership, Boeing Space and Communications has grown to be the world leader in several key markets commercial and Government communication satellites, human space flight, and battle management – and a significant player in the launch services and classified programs markets.

Mr. Albaugh's career has spanned more than 26 years of service at Boeing in a variety of assignments. Before his current position, he was President of Boeing Space Transportation, a predecessor division that folded into Boeing Space and Communications, and President of Rocketdyne Propulsion & Power, now also a business unit within Space and Communications.

While at Rocketdyne, Mr. Albaugh oversaw a range of business interests that included the Space Shuttle Main Engine (SSME) program; the Space Station Electrical Power System; liquid rocket booster engines; laser and electro-optics applications; and propulsion systems for advanced launch vehicles. He also directed the Energy Technology Engineering Center, a U.S. Department of Energy project.

A Washington State native, Mr. Albaugh joined the company in 1975 as a project engineer in Hanford, Washington. He holds bachelor's degrees in mathematics and physics from Willamette University and a master's degree in civil engineering from Columbia University.



Mr. Ianna, AT&T

As President of AT&T Network Services, Mr. Ianna is responsible for the design, development, deployment, and operation of AT&T's local and long-distance communications networks. In addition, he leads the company's Business Customer Care operation, the Customer Relationship Management group, and service delivery of complex networking solutions to global businesses and Government agencies. He also has oversight responsibility for ensuring that AT&T Labs brings customer-focused innovations into the network.

Mr. Ianna is also AT&T's Chief Quality Officer. In this role, he is responsible for integrating quality with the management of the AT&T business, as well as providing direction, support, and assessment of the company-wide quality and customer-satisfaction programs.

Mr. Ianna has 30 years' experience in the communications industry. He earned his bachelor's degree in electrical engineering from Stevens Institute of Technology in New Jersey and his master's degree in electrical engineering from the Massachusetts Institute of Technology. He also completed the Program for Management Development at the Harvard School of Business.

Mr. Notebaert, Qwest Communications

Mr. Notebaert was elected Chairman and CEO of Qwest Communications International Inc. on June 17, 2002. Previously, Mr. Notebaert was President and CEO of Tellabs, a position he had held since August 2000. Before that, Mr. Notebaert was Chairman of the Board for the Ameritech Corporation.

His 30-year career with Ameritech included appointments as President of Ameritech Mobile Communications, President of Indiana Bell, and President of Ameritech Services. In 1993 he became President and Chief Operating Officer of Ameritech Corporation, and in January 1994 he was named the company's President and CEO. He was elected to the position of Chairman and CEO on April 20, 1994.

Mr. Notebaert received a bachelor's degree in 1969 and a master's degree in business administration in 1983, both from the University of Wisconsin. He has received a number of honors and awards, including the 1999 Distinguished Alumni Award from the University of Wisconsin-Milwaukee and three honorary degrees.

Mr. Notebaert has been very active in the communities where he has lived, most recently serving as Vice Chairman of the Civic Committee of the Commercial Club of Chicago, Co-Chairman of United Way's prestigious Alexis de Toqueville Society, and Board Member of the Executives' Club of Chicago.

Dr. Ruiz, AMD

Dr. Ruiz joined AMD in January 2000 as President and Chief Operating Officer and was named CEO in April 2002. Previously, Dr. Ruiz served as President of Motorola's Semiconductor Products Sector. In his 22-year career with Motorola, Dr. Ruiz held a variety of executive positions in the United States and overseas. He also worked at Texas Instruments in Dallas, Texas, in the company's research laboratories and manufacturing operations.

Born in Piedras Negras, Mexico, Dr. Ruiz earned his bachelor's and master's degrees in electrical engineering from

NSTAC Appointments, page 22

NSTAC Appointments, continued from page 21

the University of Texas, Austin. He earned his doctorate in electronics from Rice University in 1973.

Dr. Ruiz is personally committed to expanding the impact of education around the world. In 1999, he was appointed by the then Governor George W. Bush to the Texas Higher Education Coordinating Board. He currently serves on the Foundation Advisory Council for the College of Engineering at the University of Texas. Dr. Ruiz has been appointed to serve on the Board of Directors of the Society of Hispanic Professional Engineers (SHPE) and was inducted into the Hispanic Engineer National Achievement Awards Conference (HENAAC) Hall of Fame in 2000. In 2002, he received the International Engineering Consortium (IEC) Fellow Award and was honored by the Asociación de Ingenieros Universistarios Mecanicos Electricistas, A.C. (AIUME) for excellent achievement.

In addition, Dr. Ruiz is a member of the Governor's Task Force for Economic Growth, which advises the Texas Governor on ways to ensure long-term economic growth in Texas. He is also an active member of the Governor's Business Council, a group of business leaders that advises the Governor on issues affecting the business climate and economic development in Texas. Additionally, Dr. Ruiz serves on the Eastman Kodak Company Board of Directors.

Ms. Russo, Lucent Technologies

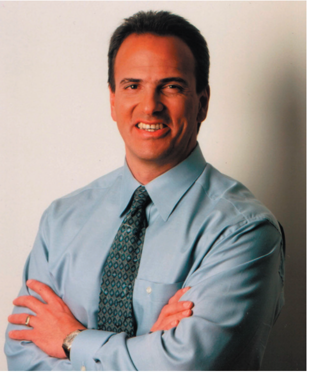
Ms. Russo was one of the founding executives who helped launch Lucent Technologies in 1996 and has spent 20 years of her career managing some of Lucent and AT&T's largest divisions and critical corporate functions. Before returning to Lucent in 2002,

Ms. Russo served as President and Chief Operating Officer of Eastman Kodak Company, overseeing the day-to-day operations of Kodak's operating divisions and serving as the CEO's strategic partner in pursuing new business opportunities. Before this appointment, Ms. Russo was Chair of Avaya Inc., one of the world's leading enterprise communications businesses.

From 1999 to 2000, Ms. Russo served as Executive Vice President and CEO of Lucent's Service Provider Networks Group and had responsibility for $24 billion in sales, distribution, installation, and development of products and systems for Lucent's service provider customers worldwide.

Ms. Russo also served as Executive Vice President, Corporate Operations at Lucent, from 1997 to 1999. In this role, she was responsible for the executive management and oversight of strategy and business development, including human resources development, public relations, investor relations, advertising, Government affairs, global procurement, and real estate services.

Ms. Russo serves on the boards of Avaya, Schering Plough Corporation, and Georgetown University. She received her bachelor's degree from Georgetown University and completed the Advanced Management Program at Harvard University in 1989. She also received an Honorary Doctorate in Entrepreneurial Studies from Columbia College in South Carolina. She was named to Fortune magazine's list of the 50 Most Powerful Women in American Business in 1998, 1999, and 2001.



Mr. Sclavos, VeriSign

As the President and CEO of VeriSign, Mr. Sclavos heads a company that is one of the leading providers of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals.

Since he joined VeriSign in July 1995, Mr. Sclavos has helped the company build a reputation as the Internet's most trusted utility. Under his leadership, the company has grown from four employees and less than $1 million dollars in annual revenues in 1995 to more than 3,000 employees and sales of over $1 billion dollars at the end of 2002. In January 1998, the company completed a successful Initial Public Offering, achieving operating profitability in 1999. Deloitte and Touche, in its year 2000 annual survey of America's fastest growing public companies, also recognized VeriSign as one of the Silicon Valley Fast 50.

Mr. Sclavos sits on the board of directors of several public and private companies including Juniper Networks, Keynote Systems, and Marimba Inc. He was recognized by the Silicon Valley Business Journal as the Entrepreneur of the Year in 1998 in the emerging companies category. In addition to being active in the local community, Mr. Sclavos and his wife formed the Sclavos Family Foundation in 1999 to support charitable efforts in education and medical research.

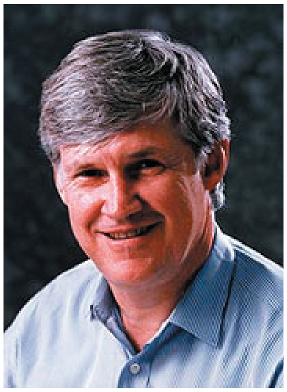
Before joining VeriSign, Mr. Sclavos held executive management positions with several Silicon Valley technology companies. From 1994 to 1995, he was Vice President of Worldwide Marketing and Sales for Taligent Inc., a joint venture of Apple, IBM, and Hewlett Packard. Mr. Sclavos served as Vice President of Worldwide Sales and Business Development for GO Corporation, a mobile computing company, from 1992-1993. Mr. Sclavos holds a bachelor's degree in electrical and computer engineering from the University of California, Davis.

Ms. Spradley, Nortel Networks

In her role as President of Wireline Networks, Ms. Spradley is responsible for driving cost-effective packet solutions for Nortel Networks' voice, data, and multimedia service offerings and maintaining Nortel Networks leadership position in circuit technology. Before her current position, she was President of Voice over Internet Protocol (VoIP) for Metro and Enterprise Networks, where she was responsible for delivering Nortel Networks' VoIP to the global market. This portfolio also included carrier and enterprise voice switching, voice portal solutions, and multimedia soft switches.

Since joining Nortel Networks in 1986, Ms. Spradley has held management positions with increasing responsibilities in sales, sales engineering, marketing, product line management, and customer service. Before her position at Nortel Networks, she established and led Siemens Corporation's product and marketing activities for entry into the personal communications system telephone business in the United States.

Ms. Spradley began her career at Data General as a systems engineer for a Fortune 500 business office. She holds a bachelor's degree in computer science from the University of Kansas and graduated from the Advanced Management Program at Harvard University Business School.



Mr. Stanton, CTIA

Although he is Chairman at both Western Wireless and T-Mobile USA, Mr. Stanton will represent the CTIA on NSTAC. CTIA is an international organization that represents all elements of wireless communications and serves its members via its relationships with the executive and legislative branches of the Federal Government dealing with taxation, fraud, technology, regulations, safety, and roaming. CTIA also distributes information to its members, policymakers, the investment community, customers, and the news media on the latest wireless policy and technical developments.

Mr. Stanton began his career in the telecommunications industry at Ernst and Whinney Telecommunications Group as a consultant with a primary focus on the cellular and long-distance business.

In 1988 Mr. Stanton and Ms. Theresa Gillespie formed Stanton Communications, which invested in businesses in various segments of the communications industry, including cellular, paging, telephone answering, alarm monitoring, voice mail, radio broadcasting, and private cable television. Internationally, Stanton Communications was involved in private television in the Soviet Union and cellular service in Hong Kong.

Mr. Stanton founded and became Chairman and CEO of Pacific Northwest Cellular in 1992, which was the Nation's eighth-largest independent cellular company. Mr. Stanton was elected Chairman of the Board of Directors for General Cellular Corporation in 1992, when Stanton Communications and Hellman and Friedman acquired a controlling interest in the company. In August 1994, he and his partners merged Pacific Northwest Cellular and General Cellular Corporation to form the Western Wireless Corporation.

He served as Chairman of Telocator, from 1986 to 1995 and is Chairman Emeritus of the CTIA. In addition, Mr. Stanton serves as a board member of Advanced Digital Information Corporation, Columbia Sportswear, and Pacific Science Center, and as a Trustee of Whitman College. A Seattle native, Mr. Stanton graduated from Whitman College with a bachelor's degree in political science. He received his master's degree in business administration from Harvard Business School.

Dr. Marburger, Director of the White House Office of Science and Technology Policy, Presents the Keynote Address at the NSTAC's 2003 R&D Exchange

From March 13 to 14, 2003, the President's National Security Telecommunications Advisory Committee (NSTAC) conducted its fifth Research and Development (R&D) Exchange titled, R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness (NS/EP).

The event, co-sponsored by the White House Office of Science and Technology Policy and the Georgia Tech Information Security Center at the Georgia Institute of Technology (Georgia Tech), was held at Georgia Tech in Atlanta, Georgia. The purpose of the R&D Exchange was to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding the trustworthiness of NS/EP telecommunications systems.

To kick-off the event and set the stage for further discussions over the two-day event, Dr. John H. Marburger, Director of the White House Office of Science and Technology Policy (OSTP), presented the keynote address during the opening plenary of the Exchange. Dr. Marburger began his address by noting the importance of increasing the trustworthiness of telecommunications and information systems that supported NS/EP activities and providing guidance to the Government on steps that should be taken to do so. He stated, "I am relying on this R&D Exchange to help me and my office give guidance to the Office of Management and Budget and other White House policy organizations on the need for specific funding or programs to enhance the trustworthiness of the Nation's NS/EP telecommunications."

Dr. Marburger continued his remarks by commenting on the dynamic environment in which the NSTAC continues to operate. In response to the evolving threat environment, the Administration has created the Department of Homeland Security (DHS), the largest Government reorganization in half a century. In addition, on February 28, 2003, President Bush signed an omnibus of Executive Orders (E.O.) related to the transfer of many Government functions and activities to the new Department. Dr. Marburger explained that two E.O.'s 12472 and 12382, and a new Homeland Security Directive, (HSD) 5, "ensure that NS/EP telecommunications services will be available in times of crisis for the President, other national leaders, and the emergency preparedness and response community."

Dr. John H. Marburger III, Director of the White House Office of Science and Technology Policy delivers the keynote address at the President's National Security Telecommunications Advisory Committee's Research and Development Exchange, held March 13 and 14, 2003, in Atlanta, Georgia. (Photo by Ms. Kiesha Miller)

Dr. Marburger stated that the Nation's R&D advantage must be used to support NS/EP telecommunications capabilities. To that end, he affirmed that the OSTP would continue to use the National Science and Technology Council (NSTC), and its subordinate subcommittees and working groups, as the key coordinating organization for R&D activities among Federal agencies and departments. Dr. Marburger emphasized that the NSTC would rely on NSTAC's NS/EP telecommunications and R&D expertise to support its activities.

Dr. Marburger concluded his remarks by reflecting on the current fiscal year 2004 budget proposals. He stated that, considering the uncertain economic recovery and growing Federal budget deficit, it was unlikely that an increase in discretionary spending would be sought. However, he said that a $123 billion budget request, a 7 percent increase over the 2003 request, was being requested to fund research activities related to homeland security and defense. Dr. Marburger asked participants to remain focused on the concept of trustworthiness in the context of NS/EP activities, and he emphasized that conclusions drawn from the Exchange discussion would have a real impact on the President's research and action agendas.

Ensuring Networks That Keep America Safe and Strong

The Vice Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC) said there is a growing disconnect between the pace of technology and our country's ability to manage it. Policies that control the telecommunications industry were written for an earlier age and discourage investment in research and development (R&D) when we need it the most.

As the featured luncheon speaker for the NSTAC's 2003 Research and Development Exchange in Atlanta, Georgia, Mr. F. Duane Ackerman, Chairman and Chief Executive Officer of BellSouth Corporation, said that the Nation's telecommunications backbone network providers must improve management of security and emerging technology issues. He also said the Government must realize that the Nation cannot have homeland security without economic security and that security and trust depends on a network of partners ready to combat today's communications challenges together.

"Private industry owns and operates nearly 90 percent of the Nation's critical infrastructure,," said Mr. Ackerman, adding that private industry has always depended on public science to fuel innovation. In the decade ahead, Mr. Ackerman said the Nation would spend billions of dollars to protect and upgrade U.S. networks and systems. "Now, more than ever, we need cutting edge R&D to make sure that we are spending those dollars wisely," he said.

One area of vital concern to Mr. Ackerman is physical security around "guns, gates, and guards." The BellSouth chairman said the Nation needs R&D in new areas like identity management and access control. "I think it is safe to say the policy of this country for the last decade or so has been to open networks, open buildings, open interfaces in our communications networks," he said. "There are people with access to some of the most sensitive infrastructure locations in the country and we don't know who they are."

To solve this issue, Mr. Ackerman said research needs to examine the possibility of creating a standard system of national security background checks and identity verifications to help ensure that only authorized personnel are getting access to critical facilities. "The availability of an interoperable standard for tamper proof, certificate based ID [identification] cards might help in this area," he said. "Technology, like biometrics, could be considered to ensure the identity of a card."

Although physical security is important, Mr. Ackerman said that cyber security is just as vital. According to Mr. Ackerman, the challenge is that network technology is outpacing industrys' and the Nation's ability to manage it. "We spent decades developing finely-tuned management practices in our existing networks…and we certainly need to keep mastering the fundamentals—documented policies, defined response procedures, disaster recovery and business continuity, redundant designs, 'failover' architectures, and ongoing audits."

Mr. Ackerman said the country needs a national strategy for continually hardening our existing network against attacks, while adapting new types of networks and protocols to ensure the same trust in new infrastructure as in the existing public switched network. By "new infrastructure," Mr. Ackerman refers to the trend toward convergence – where the Internet has merged with the public switched network in an effort to create the next generation network (NGN). He said the NGN which uses new protocols such as Multiprotocol Label Switching (MPLS) and Internet Protocol version 6 (IPv6) brings with it a host of new capabilities and new issues. "Emerging networks require new operating support systems and control systems to ensure their operability and security," he said.

Mr. F. Duane Ackerman, Chairman and Chief Executive Officer of BellSouth Corporation, addresses attendees at the President's National Security Telecommunications Advisory Committee's Research and Development Exchange luncheon on March 13, 2003, in Atlanta, Georgia. (Photo by Ms. Kiesha Miller)

Mr. Ackerman said the sheer complexity of today's communications infrastructure introduces security exposures, pointing out that there are over a billion access points to the Internet. A physical connection actually exists between the most determined terrorist organization on one of these access points and the most sensitive network system.

Ensuring Networks, page 26

Ensuring Networks, continued from page 25

"From a research perspective, the critical areas to consider are the network management interfaces and the security of the protocols that are involved in managing the connections and transporting information," said Mr. Ackerman. "The assurance that the software configurations deployed actually match the intended configurations and have not been intentionally or unintentionally altered."

It is critical that we reduce the number of vulnerabilities in the infrastructure through better software development. Many weaknesses have been introduced through coding errors during the development process. Security implications should be considered in the earliest stages and throughout the development process.

Admitting that not all attacks will be prevented, Mr. Ackerman said the R&D efforts must continue their roles to "detect and defend" the communications network. "We need mechanisms to automatically detect and quickly respond to attacks," he said, adding that standard techniques are based on monitoring traffic at network endpoints. Although research into further techniques here would help, Mr. Ackerman said the most important need is more research in network-wide pattern recognition and attack detection.

He also said service providers must have the ability to see overall traffic patterns across many ports in the network rather than seemingly random events from a single network end point. "We need detection in the face of secure tunnels and tunneling protocols—not just cryptology, but detection based on packet flow patterns," said Mr. Ackerman.

The NSTAC Vice Chair said that Government and industry could not control every access point in cyberspace. Redundancy of network capacity and connectivity, along with network management techniques, play a key role in the survivability of the network. Still, Mr. Ackerman said the country can also create a more trusted cyber-environment through separate identifiable network domains by using traffic priorities, quality of service (QoS) capabilities, and virtual private network (VPN) technologies. "This would ensure that the most critical traffic continues to flow when natural or malicious events unexpectedly force major reroutes of network traffic," he said.

Economic Security

A concern important to a successful R&D effort is the industry's ability to invest in the core data networks, according to Mr. Ackerman. He said service providers must be able to provide redundant network capacity to protect against physical and logical failures. This would allow carriers to increase network management and security and to deploy networks that support QoS and VPN capabilities to guarantee that attacks and incidents in one part of the network do not interfere with other parts of the network.

"In our increasingly data-centric network environment, R&D spending plays a critical role in improving the price, performance, management, and security of network equipment," said Mr. Ackerman. "And yet, at a time when we need to invest more, capital spending in the telecommunications industry has collapsed because of economic and regulatory uncertainty. Capital expenditure in telecom is expected to fall another 17 percent this year and remain flat through 2005."

In the 20th century, Mr. Ackerman said our Nation led the world in the deployment of advanced telecommunications infrastructure. Americans prospered from a steady flow of innovation, with better ways to get our work done, to learn, to create, to produce, to raise our standard of living. "I encourage all of us, including our partners in academia, to work on developing public policies that will help restore and protect the financial integrity of our national networks as we adapt to new threats and rapid technological change."

A Network of Partners

"Terrorists and cyberspace know no boundaries," said Mr. Ackerman, "[and] neither can our response to this changing world. We cannot operate in isolation. The concept of trustworthiness will evolve as new technology emerges and maintaining 'trusted' networks to stand up under all conditions and attacks will require an even stronger network of partners."

Mr. Ackerman said this is where NSTAC and its stakeholders must act. "At its heart, NSTAC is a learning and teaching organization, giving us access to the thinking of the best and the brightest to help us better serve the Nation and our customers." From a BellSouth perspective, he said participation in NSTAC is vital because, "…we are committed to keeping the phones ringing and the ones and zeroes flowing for the Nation… and our 44 million customers, including many critical infrastructure providers and first responders."

In concluding, Mr. Ackerman told attendees that they represent the central nervous system of the Nation's infrastructure. "We are its lifelines. We all represent key organizations and bring unique and diverse experiences to this task, " said Mr. Ackerman. "But when it comes to our role in NSTAC, there is only one agenda. Keeping America strong. Keeping America safe. Keeping America connected." And, as Secretary of Homeland Security Tom Ridge has said, "keeping America prepared and ready."

President's NSTAC Dedicated to Tackling R&D Issues that Affect NS/EP Services

Mr. Marshall Sanders of Level 3 Communications, Mr. Lowell Thomas, Director of National Security and Infrastructure Assurance for Verizon Communications and a member of the President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES), and Ms. Janet Jefferson, Chief of Industry Operations for the National Communications System, converse during the continental breakfast at the NSTAC's Research and Development Exchange, held March 13 and 14, 2003, in Atlanta, GA. (Photo by Ms. Kiesha Miller)

At the President's National Security Telecommunications Advisory Committee's (NSTAC) fifth Research and Development (R&D) Exchange, members of industry, Government, and academia gathered from all over the United States at the Georgia Institute of Technology to attend a two-day workshop dedicated to discussing pressing trustworthiness issues that could affect the telecommunications networks and information systems that directly or indirectly support national security and emergency preparedness (NS/EP) capabilities.

While the specific issue of trustworthiness discussed at the event was new to the NSTAC, the fifth R&D Exchange extended more than a decade worth of dedicated work on research and development issues related to NS/EP activities.

The R&D Exchange is a special event conducted periodically by the NSTAC. Historically, its broad purpose is to stimulate and facilitate a dialogue among industry, Government, and academia on emerging security technology R&D issues. To ensure inclusion of all stakeholders in the R&D community, the NSTAC partners with the Office of Science and Technology Policy (OSTP), the Defense Advanced Research Projects Administration (DARPA), the National Institute of Standards and Technology (NIST), and academic institutions in sponsoring R&D Exchanges.

The roots of the R&D Exchange date back to 1990 when the growing prevalence of hacker incidents led to the formation of the NSTAC's Network Security Task Force (NSTF). The task force's purpose was to assess the threats to and vulnerabilities of the public switched telephone network, and a key component of the task force's work included examining R&D issues related to security with a particular emphasis on improving commercially applicable tools.

In mid-1991, the NSTF identified six areas in which R&D on commercially applicable security tools was needed and asked the Government to share information about its R&D efforts in those areas. The subsequent briefings provided by representatives of the National Security Agency and NIST to the NSTAC constituted the NSTAC's first R&D Exchange and demonstrated that Government already had R&D efforts under way in all of those areas.

NSTAC R&D activities gained momentum again in March 1996 when the NSTAC's Industry Executive Subcommittee (IES) determined that it would again be useful to address network security R&D issues and charged the Network Security Group (NSG) with facilitating a seminar for industry and Government to discuss network security R&D activities and issues. The purpose of the seminar was threefold: (1) provide a common understanding of network security problems affecting NS/EP telecommunications; (2) identify R&D activities in progress to address those problems; and (3) identify additional network security R&D activities needed.

The NSG identified four areas of interest for further investigation – authentication, intrusion detection, integrity, and access control – and conducted the second R&D Exchange on September 18, 1996. Because the objective was to facilitate meaningful

History of R&D, page 28

History of R&D, continued from page 27

discussion among participants, participation at the Exchange was limited to 50 people representing 15 companies and 11 Government organizations, including one federally funded research and development center. The NSTAC limited industry representation to NSTAC member companies.

According to the NSG Network Security R&D Exchange proceedings, "the attendees were impressed with the willingness of both industry and Government representatives to share their R&D information so openly. Government participants took advantage of this opportunity to bring each other up to date on recent developments with their R&D activities, and the dialogue among participants initiated at the R&D Exchange can be expected to continue." Furthermore, in its recommendations to the IES, the task force recommended that, "network security R&D exchanges should be held regularly."

In 1997, in response to a number of stimuli, including the recommendations from the 1996 R&D Exchange, the Network Group's (formerly the NSG) Intrusion Detection Subgroup (IDSG) conducted a study of intrusion detection technology R&D and analyzed it in terms of meeting NS/EP requirements. The IDSG made four recommendations to the President, including the need to increase R&D funding for control systems of critical infrastructures and to encourage cooperative development programs to maximize the use of existing R&D resources in industry, Government, and academia. The task force's recommendations reinforced prior NSTAC recommendations to examine the need for and feasibility of collaborative R&D approaches for security technology and provided the basis for the concept of the third R&D Exchange, Enhancing Network Security Technology: R&D Collaboration.

The third R&D Exchange, held in October 1998, was sponsored in conjunction with the OSTP and Purdue University's Center for Education and Research in Information Assurance (IA) and Security to examine collaborative approaches to security technology R&D. The participants, which for the first time included members of the academic community, also discussed the need for training more information technology (IT) security professionals, creating large-scale test beds to test security products and solutions, and promoting the creation of IA Centers of Excellence in academia.

Mr. Brenton C. Greene, Deputy Manager, National Communications System, addresses a luncheon audience before introducting BellSouth's Mr. F. Duane Ackerman at the President's National Security Telecommunications Advisory Committee's Research and Development Exchange luncheon, held March 13 in Atlanta. (Photo by Ms. Kiesha Miller)

Deliberations at the R&D Exchange resulted in several findings and recommendations for future industry, Government, and academia work and three recommendations for future NSTAC consideration, including the need to, "conduct another R&D Exchange in the spring of 2000 to continue the dialogue on the long-term issues associated with infrastructure assurance and network security," such as new threats and convergence. The R&D Exchange conducted at Purdue University also provided the model for all future exchanges.

Sponsored in conjunction with OSTP, NIST, and the University of Tulsa, the NSTAC's fourth R&D Exchange was held at the University of Tulsa in Tulsa, Oklahoma, in September 2000. Participants examined issues of transparent security in a converged and distributed network environment and discussed the need to address the shortage of qualified information security professionals, expand the number of universities participating in the IA Centers of Excellence program, and promote best practices, standards, and protection profiles to enhance the security of the next generation network. Findings and recommendations from the Exchange included the establishment of NSTAC task forces to address standards and best practices for network security and the continuation of R&D Exchanges in following years.

Over the years, the NSTAC has strived to conduct R&D Exchanges that evolve conceptually to meet the continuous changes in technology and the political landscape and that include all stakeholders involved in protecting the Nation's NS/EP capabilities. Participation at NSTAC R&D Exchanges has grown from a small meeting of primarily Government representatives to a gathering of more than 200 industry, Government, and academia representatives in various places across the United States. As the NSTAC embarks upon its next 20 years of partnership with the Government, R&D Exchanges will continue to be a cornerstone of NSTAC outreach on issues vital to the success of the Nation's national security and emergency preparedness.