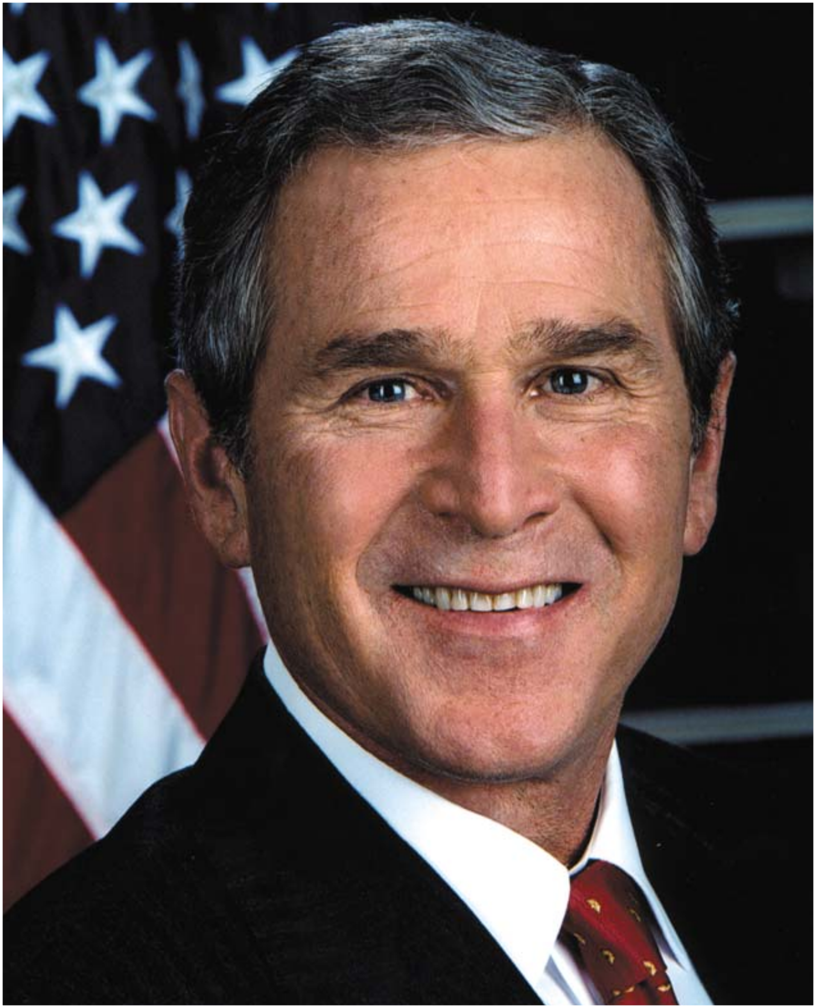
40th Anniversary

Forty Years of Service to the Nation: 1963-2003

National
Communications
System

We the People
insure domestic Tranquility, provide for the comm
and our Posterity, do ordain and establish this
Article 1



THE WHITE HOUSE

WASHINGTON

June 1, 2004

I send greetings to those commemorating the 40th anniversary of the National Communications System.

Our Nation must be prepared to respond to any urgent situation at a moment’s notice. For four decades, the NCS has coordinated our country’s emergency telecommunications system. Your efforts to maintain these critical services help protect our homeland and enhance our ability to react to and recover from threats and emergencies. By partnering with Federal, State, and local government, as well as industry and nonprofit organizations, you increase the safety of our citizens, our communities, and our Nation.

I commend NCS members for your hard work. Your commitment reflects the true character of America. Laura joins me in sending our best wishes for a memorable anniversary celebration.

At The Forefront of National Security and Emergency Preparedness Telecommunications

Forty years ago, the world stood still as the United States and the former Soviet Union readied for war during the Cuban Missile Crisis. As Americans watched the superpower showdown apprehensively, few knew that the crisis was dangerously prolonged by a technical and procedural breakdown in lines of communication between the two countries. This near-catastrophe exposed the need for secure and reliable communications between world leaders in times of emergency. To meet this need, President John F. Kennedy established the National Communications System (NCS) in 1963.

Begun as a small intergovernmental agency, the NCS today is an important global leader in national security and emergency preparedness (NS/EP) telecommunications. Through the highly effective intergovernmental and industry/Government forums it manages and the dedicated staff it employs, the NCS provides the Nation's leadership with sound policy recommendations and cutting edge technologies to advance U.S. security.

Since its inception, the NCS mission has grown and evolved. No longer focused solely on national security, but also on emergency preparedness activities, the NCS leverages the knowledge and experience of its 23 member agencies to quickly adapt to each new threat — cyber and physical — affecting the Nation's telecommunications networks. At first concerned with electromagnetic pulse and survivability issues, the NCS now contends with a variety of complex security topics including critical infrastructure protection, wireless security, and foreign ownership of the country's telecommunications infrastructure.

As the NCS entered the new millennium, it welcomed another chapter in its evolutionary process. The NCS transition into the Department of Homeland Security (DHS) is complete, and it now has the opportunity to share its knowledge and experience and forge new trusted relationships with the other new partners in the Information Analysis and Infrastructure Protection (IAIP) Directorate. As a part of the DHS, the NCS will continue its steady effort to protect our Nation's telecommunications capabilities and infrastructure.

THE NCS—A COLD WAR GENESIS

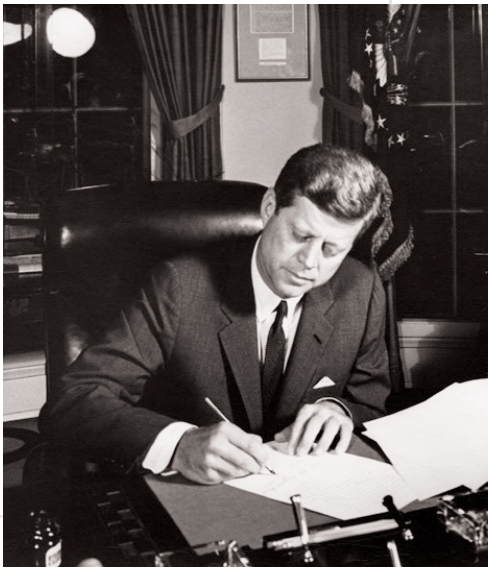
The clock was ticking. Soviet Premier Nikita Khrushchev made an offer to withdraw Soviet missiles from Cuba in exchange for an American pledge not to invade the island nation. The United States accepted the offer, but procedural and technical delays in the transmission and the Soviet receipt of this crucial message via telegraph nearly brought the country to war. For almost 12 hours, as it waited for the Soviet response to its acceptance of the offer to withdraw, the United States was poised to carry out an air strike and land invasion of Cuba. Although tensions eventually eased and the agreement achieved between the countries averted a possible global nuclear incident, the Cuban Missile Crisis went down as one of the most anxious moments in American history. From this tension was born the concept of the NCS as a unifying agency for the Federal Government for NS/EP communications under all circumstances-crisis, emergency, attack, recovery, and reconstitution.

MANAGEMENT OF THE NATION'S COMMUNICATIONS SYSTEM

Long before the Cuban Missile Crisis, the Nation's leaders understood that the country's telecommunications lines were vital to the security of the United States. In wartime, every President since Abraham Lincoln depended on communications received and transmitted via telegraph and telephone to coordinate troops, follow the progress of enemy and allied personnel, and communicate with foreign leaders. However, as the complexity of the communications system grew during the 20th century, the Eisenhower Administration saw the need for better organization and management of the Nation's communications resources, and in 1959, detailed a plan to build a unified communications system to serve the Government in times of peace and emergency.

Before he took office, President-elect Kennedy received a report emphasizing the need for the consolidation of national and international communications. Consideration of this report led to the issuance of Executive Order (E.O.) 10995, "*Assigning Telecommunications Management Functions*," on February 16, 1962. This order centralized the leadership for telecommunications policy within the Executive Office of the President with a mandate for establishing a well-planned national and international telecommunications program. It marked the beginning of the coordination efforts for the U.S. communications infrastructure.

After the Cuban Missile Crisis, President Kennedy quickly shifted communications priorities in accordance with E.O. 10995, directing the National Security Council (NSC) to investigate national security communications and



to identify and eliminate deficiencies in the Nation's communications networks. Several months later, the NSC confirmed the military, diplomatic, and civilian agencies' resource interdependence in times of crisis and recommended to the President the creation of a survivable national communications system to serve the needs of the President and other key national security personnel in crisis. Consequently, on August 21, 1963, President Kennedy officially established the NCS via Presidential Memorandum, "*Establishment of the National Communications System.*" The new communications system would link, improve, and gradually extend the communications facilities and components of Federal agencies.

EARLY YEARS OF THE NCS

President Kennedy's memorandum establishing the NCS delineated both the managerial framework for the NCS and the new system's first critical tasks. President Kennedy appointed Secretary of Defense Robert S. McNamara as the Executive Agent for the NCS and Secretary McNamara, in turn, appointed Army Lieutenant General Alfred E. Starbird, Director of the Defense Communications Agency (now the Defense Information Systems Agency) as the NCS Manager. To commence the unification process, the NCS received the communications assets of six agencies: the General Services Administration (GSA), the Department of Defense (DOD), the Department of State (DOS), the Federal Aviation Agency (FAA) (now the Federal Aviation Administration), the National Aeronautics and Space Administration (NASA), and the Central Intelligence Agency (CIA). Each of these Federal agencies appointed a full-time representative to the NCS.

In the early years, NCS leadership worked diligently to build the organizational framework and the unified communications system as outlined in the Presidential memorandum. Within weeks, the NCS developed a direct teletype link known as the Washington-to-Moscow Hot Line to prevent future misunderstandings between the two governments. Still in service today, the Hot Line has proven itself an essential communications tool during negotiations in the Arab/Israeli Wars of 1967 and 1973 and communications during the 1991 Gulf War and the 2003 Enduring Freedom campaign. The initial operation of the Hot Line marked the beginning of the NCS activities in provisioning communications for the Federal Government.

In addition to working on the Hot Line, the NCS developed near term and long-term concept plans to guide the development of the integrated system that would link the Government's long haul networks procedurally and technically. Between 1964 and 1972, the various plans identified and revised the NCS evolving objectives and requirements as necessary and listed the Federal agency's assets that should become a part of the NCS communications system. Where the communications assets did not meet the requirements, the NCS Managers identified and included the requirements in the plans for future action.

While NCS leadership crafted the plans that would lead the system operationally into the future, the NCS member agencies studied the interconnectivity and survivability of the commercial

telecommunications networks, upon which the Government relied, and fostered interagency and public/private cooperation between national security telecommunications stakeholders. Through the efforts of the member agencies, the NCS began sculpting a new level of information sharing and interconnectivity among the Government agencies responsible for protecting the Nation's communications infrastructure.

Upon completion of the mandated long range planning in 1972, the NCS determined that the coordination of the Federal Government's telecommunications capabilities would be better served through the creation of a survivable, interoperable communications system instead of a unified structure. Consequently, the NCS revised its operational structure to be a confederation of telecommunications networks, run by a consortium of Federal agencies that would achieve its goals through coordinated planning, interoperability, and system standardization in an evolutionary environment. NCS member agencies broadly approved the new approach following the restructuring and continued to delve into communications issues integral to the new mission including interoperability, operational management, survivability, standards, and priority restoration — all important issues to the NCS today.

By the close of the 1970's, the NCS accrued a wide body of knowledge on a variety of communications issues. Recognizing the importance of the telecommunications networks on the Nation's national security, the NCS developed a memorandum of understanding in concert with the Office of Science and Technology Policy and the NSC, regarding its responsibilities for national security telecommunications. In response, the NSC directed the NCS to draft a National Security Telecommunications Policy Implementation Concept Plan and manage its implementation. This initiative became the foundation for the NCS national security activities of the 1980's.

Building Partnerships and Technologies to Support NS/EP

In the late 1970's and early 1980's, several trends emerged that dramatically affected the security of the telecommunications industry, among them:

- Proliferation of Government-owned and Government-leased networks, complicating telecommunications functionality without a commensurate concern for interoperability;
- Heightened pace of technological change, offering new opportunities for system improvements;
- Divestiture and deregulation of the telecommunications industry, increasing dramatically the number of industry players; and
- Resurgent role of the Congress, the courts, and regulatory agencies, shaping a new economic and legal setting for telecommunications.

Given this new complex environment, the Government decided to ensure telecommunications for wartime and for domestic emergencies under a single framework of NS/EP telecommunications.

BUILDING PARTNERSHIPS

The 1980's brought several new challenges for the NCS. At that time, the arms race between the United States and the former Soviet Union was at its height, and the NCS had to be prepared for any eventuality. The divestiture of AT&T also posed a major difficulty to the NCS in coordinating the Nation's NS/EP telecommunications. The world's largest corporation had maintained a 70-year monopoly on the telephone industry, which the Government sought to break through its 1974 suit. By the late 1970's and early 1980's, small businesses and the Federal Communications Commission (FCC) were campaigning to give other service providers and equipment manufacturers an opportunity to compete. After eight years of legal wrangling, the Government announced the breakup of AT&T's Bell System in 1982.

The dramatic changes in the telecommunications marketplace and the intensity of the threat from the Soviet Union imposed fundamental change on the NCS with the April 3, 1984, E.O. 12472,

"*Assignment of National Security Telecommunications and Emergency Preparedness Functions*," establishing a broad new charter for the NCS. The E.O., which superseded the original charter of the 1963 Kennedy Memorandum, outlined an organizational structure and technical path for creation of an exclusive NS/EP telecommunications capability. As before, the NCS purpose was to serve the Federal Government under any and all circumstances — crisis or emergency, attack, recovery, and reconstitution. Now, however, the NCS was also to be the exclusive focal point for industry and Government to jointly plan NS/EP telecommunications to ensure the NS/EP needs would be addressed regardless of changes to the telecommunications industry. In the years that followed, the NCS became the model for industry/Government cooperation for national security.

The NCS quickly devised a new way to fulfill its mission for consolidated management of the Federal Government's NS/EP telecommunications networks while building relationships with an array of new service providers who were developing increasingly complex systems. To do this, the NCS created three highly effective partnerships:

- The National Security Telecommunications Advisory Committee (NSTAC);
- The National Coordinating Center for Telecommunications (NCC); and
- The Committee of Principals (COP) and its subordinate body, the Council of Representatives (COR).

These partnerships remain in place today and were carried over to the DHS environment as a result of their continuing success.

National Security Telecommunications Advisory Committee: Industry Advice to the President

The Reagan Administration promptly responded to the AT&T divestiture and loss of a single point of contact in the industry for coordination of NS/EP activities with E.O. 12382, "*President's National Security Telecommunications Advisory Committee*." The 1982 E.O. created the NSTAC with the charge to provide the President with critical industry-based analysis and advice on policy and technical issues for NS/EP communications. Comprised of 30 chief executives from the telecommunications, hardware, software, aerospace, and related industries appointed by the President, the NSTAC has advised four Presidents and six administrations. It's studies span topics from early network survivability and electromagnetic pulse to critical infrastructure protection, information sharing, network security, convergence, and wireless security. NSTAC recommendations have led to enhancements to the Nation's NS/EP communications capabilities through both the development of operational tools and industry/Government planning, coordination, and implementation of policy. Today, the White House recognizes NSTAC as one of the premier models for fostering cooperation and trust both among industry participants and between industry and Government.

National Coordinating Center for Telecommunications: Industry and Government Operational Alliance

The result of a 1983 NSTAC recommendation to President Reagan to create a coordinating center to handle emergency telecommunication requests, the NCC began operations on January 3, 1984. The NCC is an industry/Government body comprising four Government agencies and departments and 32 industry participants in which industry and Government representatives work together in day-to-day operations to coordinate NS/EP telecommunications responses during cyber and physical crises and to produce emergency response plans and procedures for real-world events.

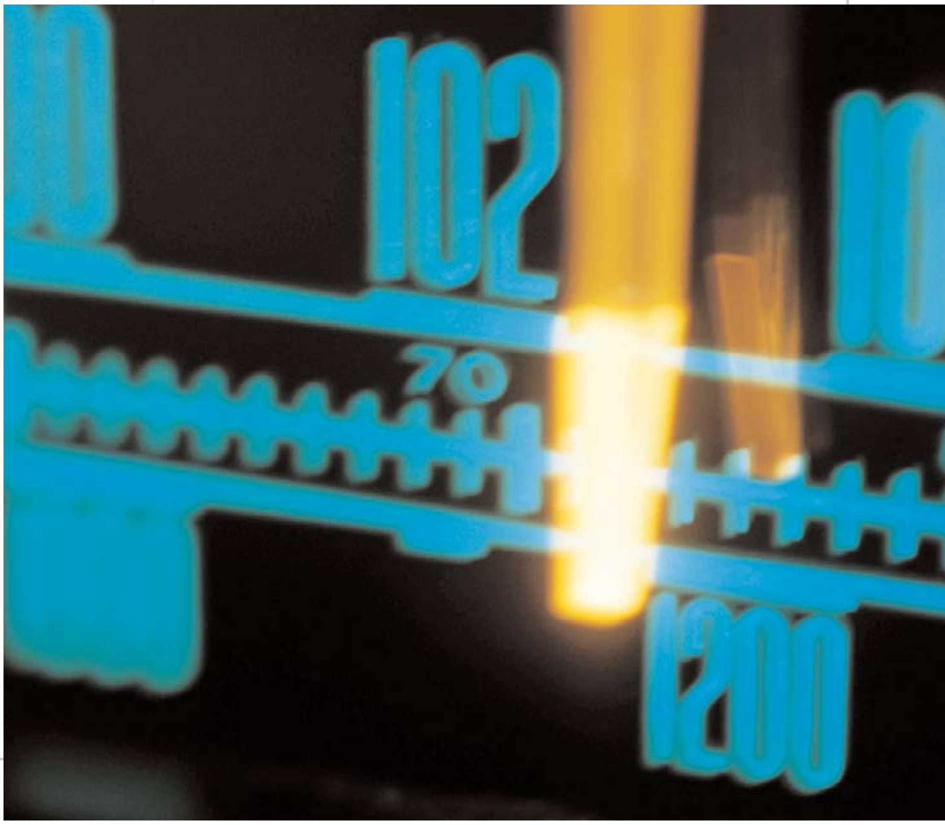
The NCC has proven the value and effectiveness of the partnership between the private and public sectors through its rapid response to crises posed by Hurricanes Hugo, Fran, and Marilyn; Operations Desert Storm, Desert Shield, and Enduring Freedom; the Oklahoma City Bombing; the Love Letter Worm, and the Sobig.f virus; floods and earthquakes across the country; and the September 11, 2001, terrorist attacks. NCC representatives also work to build awareness of NS/EP concerns globally through participation in the US/Canada Civil Emergency Planning Telecommunications Advisory Group, the North Atlantic Treaty Organization's Civil Communications Planning Committee, and the International Telecommunication Union.

Committee of Principals and Council of Representatives: Multi-Agency Cooperation in Government

Although originally organized in the early 1970's to help shape the NCS agenda, it was not until 1984 that the Government officially instituted the NCS Committee of Principals and the Council of Representatives. In response to E.O. 12472, the COP and COR emerged from hiatus to serve as the forums for intergovernmental interaction on issues relating to NS/EP telecommunications, encompassing topics such as standards, communications satellites, information systems, and digital communications. The NCS Manager chairs the COP, and each member agency appoints a Principal member to sit on the COP and a delegate Representative to sit on the COR. Through the COP and COR programs, NCS leadership consistently receives vital information from its member agencies on the full spectrum of Federal Government NS/EP telecommunications assets and responsibilities. In turn, the NCS member agencies receive crucial information and guidance on the means to leverage the NS/EP programs and initiatives developed by the NCS.

BUILDING TECHNOLOGIES

To carry out its mission, the NCS developed programs and technologies to ensure telecommunications capabilities for the Federal Government at all times. The Network Design and Analysis Capability (NDAC), the National Level NS/EP Telecommunications Program (NLP), the Telecommunications Service Priority (TSP) Program, and the Shared Resources-High Frequency Radio Program (SHARES-HF) are initiatives that built the NCS broad cadre of current tools and technologies and transformed the Federal Government's ability to prepare for and respond to crises.



Network Design and Analysis Capability

The NCS constantly prepares for threats to the Nation's telecommunications infrastructure. Given the telecommunications industry's growing reliance on computer networks and cyberspace communications, the NCS studies and monitors the health of these networks, looking for vulnerabilities and testing new designs. Developed in 1986, the NDAC performs infrastructure analyses of the commercial telecommunications network that supports critical Government functions. The main objective of the NDAC is to determine how the loss of a critical telecommunications asset could adversely impact Government functions.

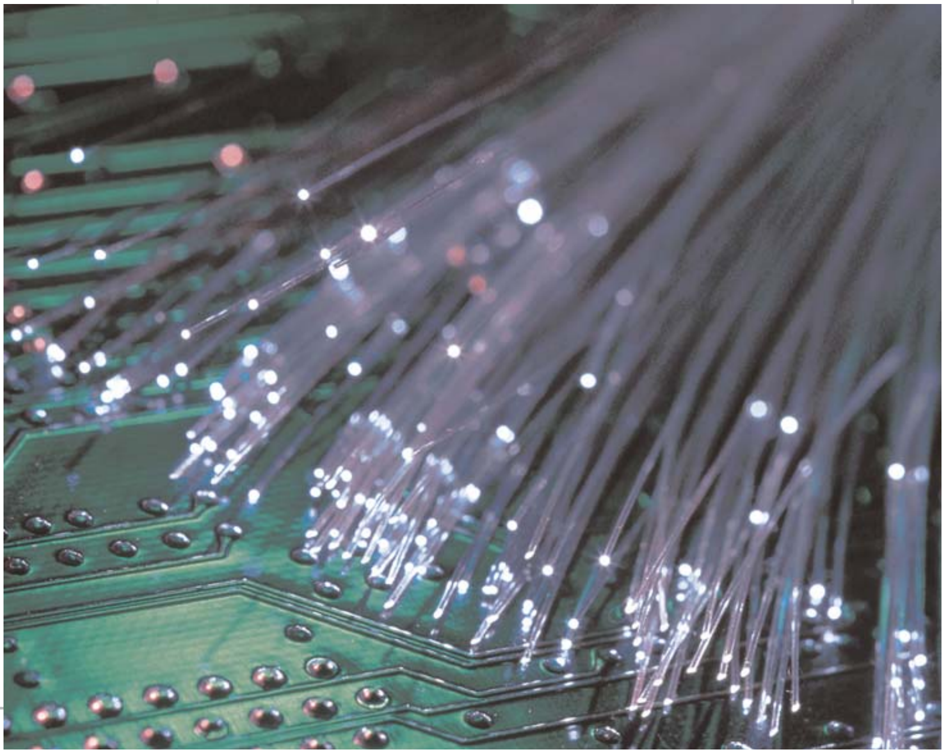
Using a suite of modeling tools, the NDAC studies the performance of the public switched network (PSN), including telephony and the Internet, during regional outages and national emergencies. By analyzing the telecommunications infrastructure during times of stress, the NDAC is able to measure potential service degradation caused by network transmission and switching losses. The NCS uses this data to ensure vital NS/EP telecommunications lines are reliable and protected.

National Level NS/EP Telecommunications Program

In 1986, the NCS developed the NLP as a single initiative — encompassing the development and implementation of several programs — to devise a comprehensive telecommunications nuclear response and recovery plan. Through the NLP, the NCS projected the evolution of technological capabilities to improve the routing, survivability, connectivity, and interoperability of the PSN, particularly in the event of nuclear attack. The NLP housed three crucial programs: the Commercial Network Survivability (CNS), the Commercial Satellite Communications Interconnectivity (CSI), and the Nationwide Emergency Telecommunications Service (NETS). The CNS and CSI programs focused on reconstituting the commercial carrier networks by maximizing their survivability and interoperability. Both programs were updated to incorporate new switching, satellite, and software technologies, but the programs were eventually ended as the Cold War de-escalated. NETS concentrated on establishing nationwide communications under nuclear war conditions. It evolved to meet the growing threats to the security of the telecommunications infrastructure with development of a technical approach — the Government Emergency Telecommunications Service (GETS) — that is today one of the NCS primary tools to secure communications during crises.

Telecommunications Service Priority Program

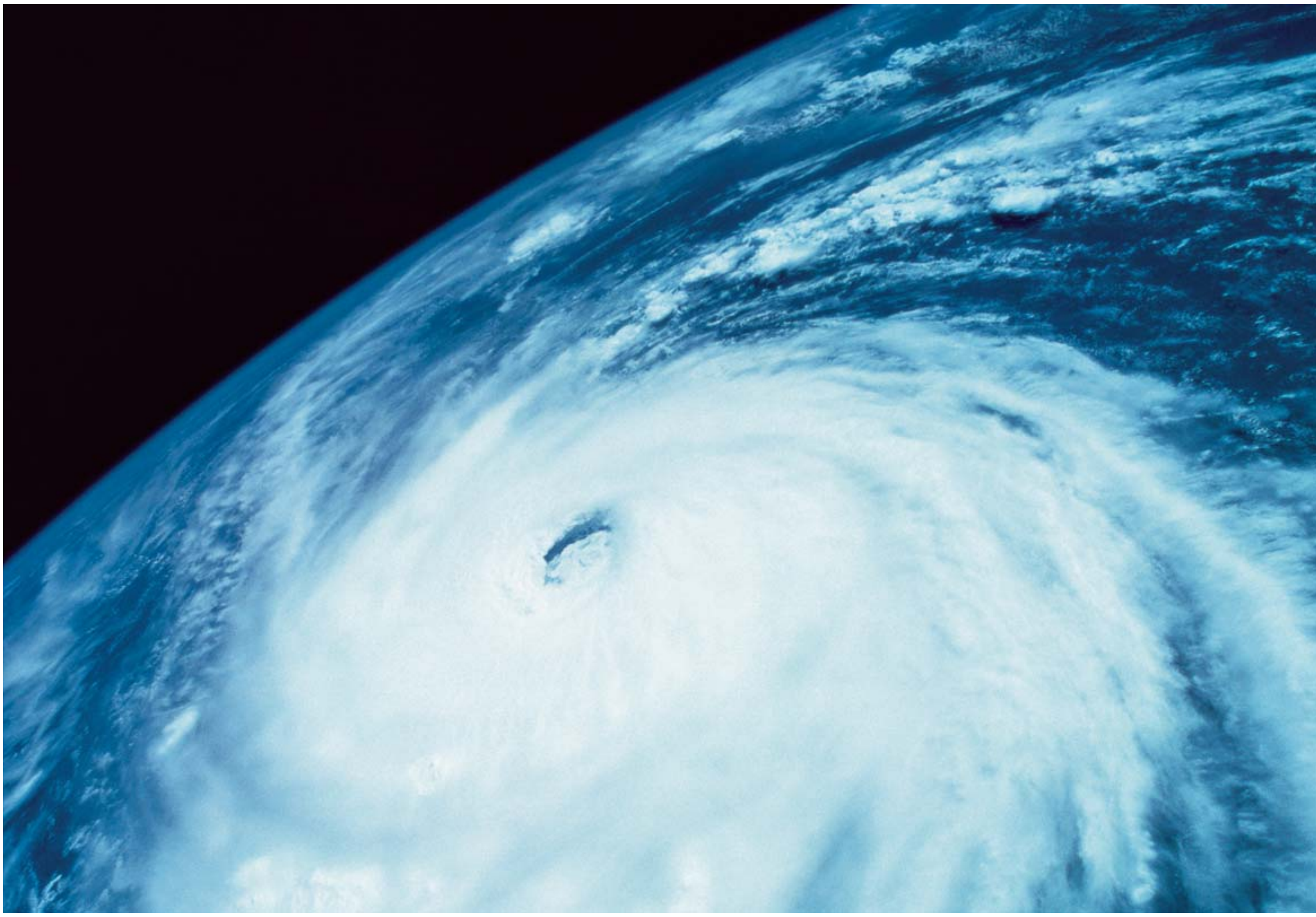
The TSP Program is the result of one of the first recommendations of the NSTAC — the need for a system to assign priority provisioning and restoration of critical NS/EP telecommunications services in the hours immediately following a disaster. The Office of the Manager, NCS (OMNCS) and the NSTAC worked with the FCC on establishing the regulatory guidelines for the creation of the TSP System, which culminated in the issuance of an FCC Report and Order on November 17, 1988. The Office of Priority Telecommunications (OPT), established by the OMNCS, would support the TSP Program by coordinating requests for priority provisioning and restoration from NS/EP telecommunications users with the telecommunications carriers serving those



users. The close working relationship between the NSTAC and the OMNCS aided TSP program implementation, as both the provisioning and restoration of circuits rely heavily on the public switched telephone network of the NSTAC member companies. While originally intended for communications restoration in the event of a nuclear disaster, TSP has proven extremely effective in all types of emergencies, including during the NCS response and recovery efforts following the September 11, 2001, attacks in New York and Washington.

Shared Resources High-Frequency Radio Program

Approved by the Executive Office of the President under the mandate of E.O. 12472, the SHARES-HF Radio Program is a single, interagency emergency message handling system. It combines the high frequency (HF) radio resources of industry, Federal, and State organizations should an event occur that destroys normal communication lines or makes them unavailable for NS/EP usage. The SHARES network today consists of over 1,100 HF radio stations, representing 91 industry, Federal, and State resource contributors. SHARES stations are located in every state and at 20 sites overseas. Nearly 200 emergency personnel participate in SHARES, and the network has more than 150 HF frequencies earmarked for its usage.



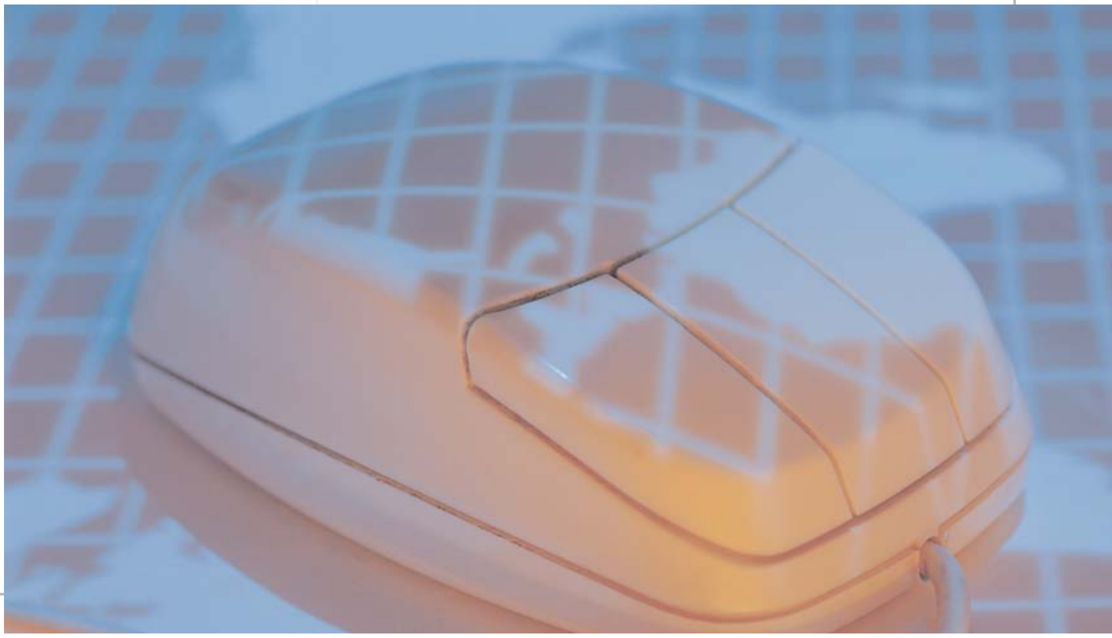
An Evolving Threat—Critical Infrastructure Protection

The 1990's marked another series of challenges for the NCS, defined by changing worldwide political climates and emerging technological advances in the telecommunications network. When President Reagan signed E.O. 12472, nuclear war posed the primary threat to the Nation's national security. However, with the collapse of the Soviet Union and the fall of the Berlin Wall in 1989, the Cold War danger subsided. In its stead appeared a new type of threat to the Nation's telecommunications system, bred by the increasing dependence on the Internet, computers, and other networked information systems. Although far less damaging in appearance than nuclear war, "cyber warfare" possesses the ability to quickly and ruthlessly cripple the Nation's many critical infrastructures, including its telecommunications networks, with the click of a mouse from anywhere in the world. Simultaneously, the Nation's vital communications are vulnerable to physical attacks that could cause sustained outages and widespread disruption.

The NCS recognized the need to modify its approach to NS/EP telecommunications and promptly acted to adapt its more mature technologies and programs and introduce new innovative programs to directly meet the new cyber risk. At the same time, the NCS broadened its mandate and began to support recovery from natural and man-made disasters and from significant domestic and international events.

NCS and the National Information Infrastructure

By the early 1990's, the Internet — in conjunction with public, private, and proprietary networks, and other emerging information technologies — was known as the National Information Infrastructure (NII). The NII concept originated in the late 1980's when information systems were still largely operationally independent. By the early 1990's, the NII had grown significantly, and the Government's dependence on the interconnection of information systems had become an important part of the



communications network. In 1993, the Federal Government released the "*National Information Infrastructure: An Agenda for Action,*" a framework for addressing the policy and technology associated with the NII. The burgeoning growth of the NII and the Internet had major implications for the NCS, and to effectively address them and protect the Nation's critical infrastructures, the NCS undertook two new initiatives in the early 1990's:

Network Security Information Exchanges

The Network Security Information Exchanges (NSIE) provide a working forum to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. Separate, but closely coordinated, the Government and NSTAC formed NSIEs in 1991 as a result of an NSTAC recommendation to improve industry/Government coordination on network security issues. Among the NSIEs' objectives are learning more about intrusions into and vulnerabilities affecting the PSN, developing recommendations for reducing network security vulnerabilities, assessing network risks affecting network assurance, acquiring threat and threat mitigation information, and providing expertise to the NSTAC for recommendations on network security to the President.

Critical Infrastructure Warning Information Network

To strengthen the Nation's growing cyber network, the NSC asked the NCS in 1991 to develop a system to facilitate immediate alert and notifications for threats to the network to industry and Government partners. In response, the NCS created the Critical infrastructure Warning Information Network (CWIN), a classified and unclassified communications network among key Federal Government facilities and industry sites that produces the immediate alert and notification components the NSC requested. Renamed in August 2003, as the Critical infrastructure Warning Information Network, the CWIN provides a non-PSN-switched, non-Internet, private voice and data network that gives Government assured reliability under emergency conditions. At its full operational capacity, the CWIN facilitates the dissemination of time-sensitive warnings on imminent threats or ongoing attacks against the Nation's critical infrastructures and supports the transmission of both classified and unclassified information.

NCS AND CRITICAL INFRASTRUCTURE PROTECTION

In the mid 1990's, the Clinton Administration issued a series of Executive Orders and Presidential Directives to examine the vulnerability of critical infrastructures to terrorism, develop a comprehensive strategy to leverage Federal resources to assure the continuity and viability of the Nation's critical infrastructures, and engage the private sector in these efforts.

These documents did not directly outline the NCS role in critical infrastructure protection (CIP), but the new national emphasis on CIP showcased how NCS NS/EP efforts were directly relevant to emerging CIP concerns. As a result of the Federal emphasis on CIP, the NCS established a CIP division in the late 1990's to address critical infrastructure threats and vulnerabilities with a unique industry/Government mission of ensuring the availability of critical NS/EP telecommunications services in the event of emergencies, including conventional and terrorist attacks, natural and man-made disasters, and other crises. For example, the NCS and the NSTAC worked bilaterally with the

electric power industry to investigate electric power and telecommunications restoration procedures. Examining the interdependencies of the telecommunications infrastructure with other critical infrastructures continued throughout the late 1990's.

The CIP Division also focused on looming threats to the telecommunications infrastructure such as the Year 2000 rollover and the possibility that global computer networks would cease to function because of the calendar change from 1999 to 2000.
In preparation, the NCC set up a Y2K database to track the status of participating members around the world. The database provided real-time support and monitoring of many critical telecommunications networks. The rollover passed with little incident; however, the database and processes developed during the preparation for Y2K would prove invaluable for future efforts.

Since the private sector owns a majority of the telecommunications infrastructure, leveraging its partnerships with industry is an important part of the NCS CIP strategy. In 2000, the NSC designated the NCC as the Telecommunications Information Sharing and Analysis Center (ISAC) in response to the 1998 Presidential Decision Directive (PDD)-63, *Protecting America's Critical Infrastructures*. The NCC Telecom ISAC facilitates voluntary collaboration and information sharing between critical telecommunications industry/Government players. It is used to gather information on vulnerabilities, threats, intrusions and anomalies from multiple sources and perform analysis with the goal of averting or mitigating impact upon the telecommunications infrastructure.

NCS EXPANDED EMERGENCY RESPONSE MISSION

While the NCS mission during the 1980's included emergency response, they did not begin these activities until the late 1980's-early 1990's. Today, the NCS mission addresses a wide spectrum of disruptive and destructive threats, including nuclear incidents, terrorist activities, civil disorder, information warfare, and natural disasters. The NCS had to modify its operations in light of the changes to the threat and changes in technology.

In the 1990's, the NCS worked closely with the Federal Emergency Management Agency (FEMA) — also now part of the DHS — to identify all communications requirements for a disaster area and to implement solutions to improve communications capabilities. Among these solutions was the Emergency Response Link (ERLink) — a Web site linking Federal Response Plan participants and providing them with response reports and other documents. With the assistance of the NCC, NCS Regional Managers, and Individual Mobilization Augmentees (IMAs), the NCS also facilitated response activities, including the maintenance and restoration of communications lines and systems during a wide range of natural disasters, such as Hurricanes Bonnie, Georges, and Floyd; wildfires in Arizona and Florida and surrounding areas; ice storms in the Northeastern United States; and flooding across the Atlantic Basin.

To respond to its expanded mission of ensuring NS/EP personnel have the ability to communicate during any type of crisis, while keeping mindful of costs, the NCS enhanced and updated relevant programs, including the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and the Alerting and Coordinating Network (ACN).

Government Emergency Telecommunications Service Program

Created during the early 1990's, GETS is a method of prioritizing wireline telephone calls in emergency situations, allowing vital members of the Government and telecommunications industry to maintain contact with their respective agencies and to coordinate the best recovery scenario possible. The NCS designed GETS to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in NS/EP missions. GETS replaced the NETS program by shifting from hardware solutions to software-based solutions, offering greater flexibility and cost efficiency. GETS operated over three types of networks to prioritize NS/EP telecommunications:

- The major long-distance networks provided by Interexchange Carriers (IXCs) — AT&T, MCI, and Sprint;

- The local networks provided by Local Exchange Carriers (LECs) such as the Bell Operating Companies and Independent Telephone Companies (ITCs), cellular carriers, and personal communications services (PCS); and

- Government-leased networks, including the Federal Telecommunications System (FTS) and the Defense Information System Network (DISN).

Wireless Priority Service

As wireless communications became increasingly used for NS/EP operations, the NSTAC recommended the development of a priority access program for wireless networks, similar to the service GETS provides for wireline users. After the FCC issued the first Report and Order on priority access service in 1996, the NCS began development of WPS. NS/EP users invoking WPS are placed at the top of the queue for the next available channel, improving their ability to complete wireless calls during times of emergency. The service is available only to key NS/EP leadership and is not intended for use by all emergency service personnel.

After renewed interest by President George W. Bush and the first responder community following September 11, 2001, WPS became an operational reality. The NCS first activated a wireless priority service in Salt Lake City to support the Winter Olympic Games in February 2002, then activated a WPS pilot program in Washington D.C. and New York City in May 2002. Initial operating capability began in December of 2002, with additional nationwide markets coming online throughout 2003.

The NCS remains involved in the design and implementation of the WPS full operating capability (FOC), and hopes to eventually have a variety of global systems for mobile communications (GSM) and code division multiple access (CDMA) carriers providing the service. NCS officials expect the WPS FOC to be an end-to-end service, fully integrated with the GETS program. The NCS is also working to ensure that the WPS user base, including State and local governments and NS/EP entities, becomes more aware of the service and its benefits.

Alerting and Coordination Network

With the potential vulnerability of the PSN, the NCS further ensures NS/EP telecommunications through the ACN. The ACN is a private network that provides its users with a non-public network based switching capability for direct connectivity to State and local Government agencies, telecommunications service providers, and equipment manufacturers. The ACN provides a stable emergency voice communications network connecting telecommunications service providers' Emergency Operations Centers (EOC) and Network Operations Centers (NOC) to support NS/EP telecommunications network restoration coordination, transmission of telecommunications priorities and requirements, and incident reporting when the PSN is inoperable, stressed, or congested.

With each passing year, the NCS mission widens in scope. The Information Age and the Internet have heightened the threats to our Nation's information security and made it harder to counteract those threats. NCS knowledge of and experience in national security telecommunications uniquely enables it to devise programs to meet these new challenges. Preparedness is still the key to overcoming new hurdles, and the NCS is growing even now to meet these challenges head-on.

A New Chapter - Transition Into Department of Homeland Security

RESPONSE TO SEPTEMBER 11, 2001, AND RECOVERY EFFORTS

On September 11, 2001, the United States suffered the worst terrorist attack ever perpetrated on America's soil. Two planes struck the World Trade Center in New York City, one struck the Pentagon in Washington, D.C., and a fourth hijacked plane crashed into a field in western Pennsylvania. On that fateful day, the NCS and its NCC, in partnership with private companies, quickly assembled an unprecedented level of resources at the National, State, and local levels to support the response and recovery efforts.

Damage to the communications infrastructure in the affected areas was severe. The attacks crippled several critical switches, cut important cable lines, flooded cable vaults, and disrupted electricity to the area. Officials estimated that the attacks damaged 200,000 voice lines, 100,000 business lines, 3.6 million data circuits, and 10 cellular towers, causing severe communications congestion for emergency personnel and citizens alike. Despite the possible damage to their own network infrastructures, NSTAC member companies immediately contacted the NCS to learn how their companies could help the NCS in its response to the terrorist attack.

NCS coordination efforts began immediately. NSTAC member companies offered assistance in restoration efforts, despite the fact that some of their infrastructure had been among the most severely damaged. The NCC began 24/7 operations to facilitate NS/EP communications among Federal, State, and local responders; to restore damaged communications lines in Arlington, Virginia, and New York City; and to provision new lines for use for recovery and investigation activities. The NCC operated at four sites: the NCC, the Federal Emergency Management Agency (FEMA), the headquarters of the DOD's Global Network Operations Support Center, and one remote continuity of operations location. The NCS further deployed Individual Mobilization Augmentees to three FEMA regional operations centers.

In the two weeks after the attacks, the NCS issued more than 500 TSP requests to 46 different organizations, including the Federal Bureau of

Investigation (FBI), the Port Authority of New York, and the Federal Reserve Board, ensuring the necessary telecommunications services were in place to swiftly reinstate business functionality. Even after Wall Street capabilities were restored, the NCS issued TSPs to expedite the provisioning of other telecommunications services in support of Operation Enduring Freedom. Between September 11, 2001, and July 1, 2002, more than 7,000 TSP provisioning and restoration requests were made, nearly 4,200 more than during the same period in 2000.

GETS also proved its capabilities after the 9/11 attacks. More than 1,000 new GETS emergency personal identification numbers, adding to the 45,000 cards already in circulation, were issued in the two weeks after the attacks to several agencies, such as the NSC; the FBI; the National Military Command Center; the Joint Chiefs of Staff; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Director, National Security Agency and his immediate staff. Of the thousands of GETS calls national leaders and emergency responders attempted in that period, the service completed more than 95 percent of the calls on the first attempt, despite heavy network congestion.

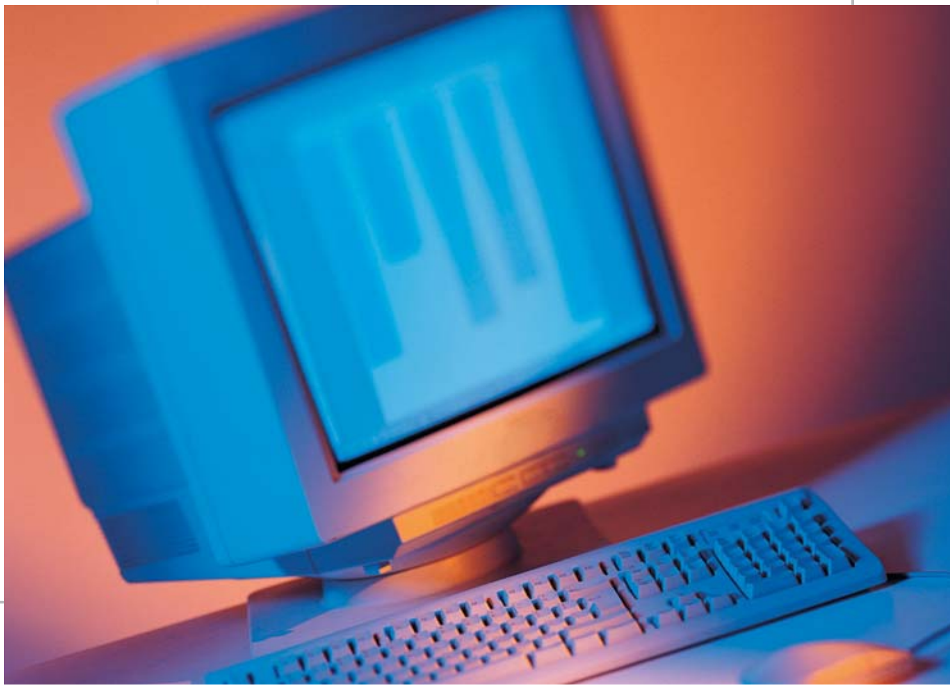
In addition to its provisioning responsibilities, the NCC also coordinated the gathering and sharing of information. It hosted daily conference calls among resident and non-resident members of the NCC to coordinate efforts, identify problems, and share information on progress. The NCC coordinated access for telecommunications service providers into the Manhattan "Red Zone" to restore NS/EP communications and conduct other activities, such as refueling emergency generators, to ensure continued operation and viability of facilities. It also brought the Wireless Emergency Response Team into the "Red Zone" to triangulate transmission on emissions from cell phones and pagers to aid in the search for victims.

POST SEPTEMBER 11, 2001, NCS ACTIVITIES

The events of September 11, 2001, reinforced the immense value of the TSP and GETS programs and instigated a renewed interest from the first responder community in the WPS and CWIN programs developed by the NCS in the 1990's. In addition, it also became very clear to NCS representatives that additional programs would be needed to continue to facilitate NS/EP communications in the new homeland security environment. Two new systems — the Global Early Warning Information System (GEWIS) and the Emergency Notification System (ENS) — are being developed as a result.

Global Early Warning Information System

GEWIS is a prototype health assessment tool to provide information for early detection of significant Internet/inter-network performance events and anomalies. It then corroborates the information and builds conclusions within a superset process involving skilled human analysts, decision-makers, and public and private sector constituents responsible for critical infrastructure protection and mitigation. GEWIS uses multiple commercial data sources and applied knowledge management techniques to provide a fused situation assessment and to detect anomalies based on a deviation from the normal.



Emergency Notification System

The ENS, a national system to provide emergency notification or alerts to the general public currently under development by the NCS, is designed to facilitate interoperability across existing systems and to provide for data collection across infrastructures. The ENS will use multiple communication technologies, including telephone, short message service, pager, and e-mail, for notification, and automatically notify intended recipients on a repeated basis until delivery is confirmed or until a predetermined number of attempts have been made. ENS is currently operating as a pilot program.

In the months following the attacks, the NCS, through the NSTAC, undertook a number of policy related activities with regard to homeland security as it waited to see how the Federal Government would organizationally respond to the new threat environment. Directly following the attacks, the NSTAC compiled a list of lessons learned and discussed the NSTAC's future role in homeland security with Government officials. Moreover, following the release of the draft *National Strategy for Homeland Security* in September 2002, the NSTAC submitted suggested revisions to the draft to the President's Critical Infrastructure Protection Board from the perspective of its member companies.

Critical infrastructure protection, network vulnerability, and infrastructure dependencies were also primary topics of study by the NSTAC in the early 2000's. In direct response to the lessons learned from September 11, 2001, response efforts, the NSTAC studied risks associated with consolidated telecommunications assets in telecom hotels, trusted access to critical facilities, vulnerabilities in pervasive software and protocols used over the telecommunications networks. More recent studies also include the security of NS/EP communications over satellite networks and further work on trusted access to facilities through improved background check processes.

NCS AND THE DEPARTMENT OF HOMELAND SECURITY

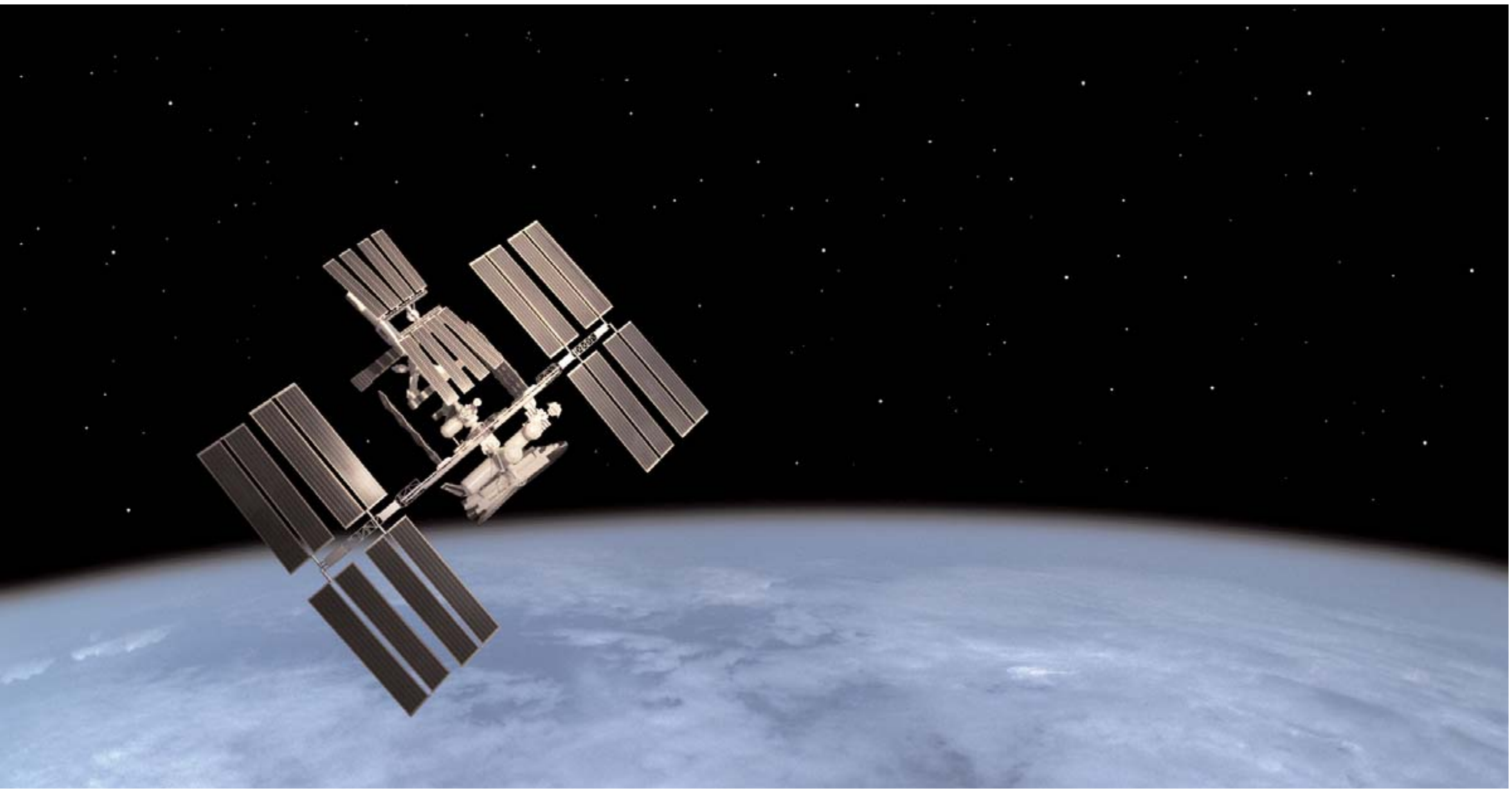
The events of September 11, 2001, brought the need for homeland security to the forefront. With the signing of the *Homeland Security Act of 2002*, President Bush created the DHS to bring agencies together to greatly improve homeland security in the shortest possible time. The NCS was selected to join the DHS because of its experience in infrastructure protection and assurance, its watch center capabilities, its suite of national programs for priority telecommunications services to the NS/EP community, and its strong relationships with industry through the NCC, NSIE, and the NSTAC. The transition was official on March 1, 2003. In the ceremony to mark the occasion, Major General Bruce Lawlor, USA, the former Chief of Staff for DHS, noted, "We sought out the NCS as a model for how we might take what you have done and implement it across all 14 sectors of critical infrastructure that exist across the country."

The ceremony symbolized a changing of the guard from DOD to DHS as the NCS Executive Agent. The NCS now faces the task of integrating its capabilities into the IAIP Directorate. As a component of the IAIP, the NCS will help fulfill the Directorate's mission to identify and assess threats to the homeland, map those threats against vulnerabilities, issue warnings, and provide the communications framework from which to organize protective measures to secure the homeland. The NCS mission will remain in the realm of protecting and assuring lines of communications in times of emergency and in coordinating NS/EP communications efforts. The partnerships the NCS has built over its illustrious 40-year history will now be called upon for homeland defense efforts coordinated on an even greater scale than before. It is a new age, and the NCS is adapting and advancing its capabilities to the new environment.

Conclusion—New Opportunities

For four decades the NCS has worked to secure and protect our Nation's critical telecommunications infrastructure. From the first Presidential hotline to the Kremlin to today's undersea fiber optics and orbital communications satellites, the NCS works to ensure that interoperable and survivable lines of communication are available to our leaders and first responders at all times.

With its transition into the DHS, the NCS now has new allies in the fight to prevent attacks on the country's vital critical infrastructures. As a pioneer in public/private and intergovernmental relationships and new security technologies, the NCS has much it can share in the Government's concerted effort to protect the homeland. While the threat of nuclear war, which first propelled the creation of the NCS, has diminished, the United States now confronts a range of malicious threats to our homeland, making efforts to secure the telecommunications network more important than ever before. The NCS embraces its new opportunities and stands ready to assist the Secretary of Homeland Security and the President for many years to come.



IAIP/NCS
Mail Stop #8510
Department of Homeland Security
Washington, DC 20528

www.ncs.gov