



National Communications System

**45** Years of Service to the Nation  
1963–2008



Homeland  
Security





National Communications System

**45** Years of Service to the Nation  
1963–2008



Homeland  
Security



“For time and the world do not stand still. Change is the law of life. And those who look only to the past or the present are certain to miss the future.”

President John F. Kennedy

# Cold War, Hotline, and Dot.com

## The Evolution of the National Communications System

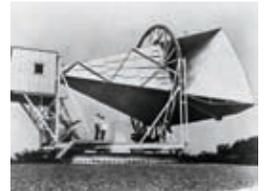
The early 1960s encompassed an array of social and political turning points within American history that, 45 years later, continues to resonate within our consciousness, culture, and current events. Forces such as the Civil Rights Movement and the Cold War created a climate of both possibility and uncertainty. As relations with the Soviet Union became locked in brinksmanship, the world's first communications satellite made its initial orbits in space.

The Nation was communicating in turbulent and technologically advancing new ways, highlighting the increasing need for communications security. In response, President John F. Kennedy created the National Communications System (NCS) to serve a critical function that has persisted through decades of ever-changing national security and emergency preparedness (NS/EP) challenges. Today, the NCS bears a 45-year history that has itself been one of evolution, challenge, and bold innovation.

The NCS has provided an enduring and forward-looking service to the Nation. Through the tensions of domestic and international communication in the 1960s, the proliferation of telecommunications in the 1970s, and the technology surge of the 1980s and 1990s, the NCS evolved with the security and technological environment. The years leading up to the 21st century could not have prepared the NCS for the torrent of new challenges revealed in the wake of the September 11, 2001, terrorist attacks. The first decades of the NCS laid a crucial foundation for the unprecedented security and preparedness innovations emerging today.

### Historic Milestone

The Horn reflector antenna at Bell Telephone Laboratories in Holmdel, New Jersey, was built in 1959 for pioneering work in communication satellites for the NASA ECHO I. It was used to detect radio waves that bounced off Project ECHO balloon satellites. The horn was later modified to work with the Telstar Communication Satellite frequencies as a receiver for broadcast signals from the satellite. (Photo by NASA)



## 1960s

In July of 1962, the world ushered in a new age of technology with the launch of AT&T's Telstar, the world's first commercial communications satellite. Telstar not only allowed the first telephone call transmitted through space, it also successfully transmitted live and taped television across the Atlantic Ocean.

President Kennedy marked the communications milestone with the world's first live transatlantic press conference. Just a month later, Massachusetts Institute of Technology Professor J.C.R. Licklider released the first recorded concepts of the Internet, when he produced a series of memos describing his vision for a globally interconnected set of computers that would allow users to quickly access data and programs from any location. He also became the first head of the Defense Advanced Research Projects Agency, which helped to spur the development of Information Technology (IT) through several decades. With the introduction of groundbreaking technologies, the landscape of communications was becoming more global and connected, but also more complex.

Strategic Air Command personnel interpreting reconnaissance photo during the Cuban Missile Crisis, 1962. (U.S. Air Force photo)



Months after delivering his landmark televised address using Telstar, President Kennedy utilized the new technology to deliver a televised address to the Nation on October 22, 1962, briefing the American public on what would become known as the Cuban Missile Crisis. The challenges arising out of this national emergency formed the impetus that created the NCS.

October 1962, Executive Committee of the National Security Council meeting. White House, Cabinet Room. (Photo by Cecil Stoughton, White House, October 29, 1962.)

The crisis began when a U.S. reconnaissance mission flying over Cuba discovered the presence of Soviet-owned missile launchers. In response, President Kennedy imposed a naval blockade on the island, threatening an air strike if the Soviet Union failed to remove its missiles from the Cuban bases.

In the midst of negotiations, communications malfunctioned and slowed at critical junctures, bringing the country dangerously close to a national and international security crisis. Even as a new communications satellite orbited the earth, for several tense days, an international communications crisis loomed over the Nation. Ultimately, in exchange for a United States pledge not to invade Cuba, Soviet Premier Nikita Khrushchev offered to withdraw the Soviet missiles. However, procedural and technical delays in transmitting and receiving this crucial message led to a 12-hour delay in its delivery. When the message finally reached the President's desk, the United States had been just hours away from initiating an air strike and land invasion.

The message of Khrushchev's assent provided the basis for an agreement that drew the crisis to a close on October 28, and though the resolution was peaceful, the lesson had been potent. The near-catastrophe exposed the need for secure and reliable communications between world leaders, particularly in times of emergency.

As the country neared an impasse with its potential for intensified involvement in the escalating war in Vietnam, the Cuban Missile Crisis led President Kennedy to order the National Security Council (NSC) to perform a review of national security communications. As a result of that review, on August 21, 1963, the President issued a memorandum establishing the NCS to connect, secure, unite, and progressively expand Federal interagency communications.

President Kennedy turned to Secretary of Defense Robert S. McNamara to lead the NCS as its first Executive Agent, assigning NCS responsibilities and defining its organization within the Department of Defense (DOD). The President charged the new agency with overseeing the communications functions of six Federal departments and agencies, including: the General Services Administration, DOD, the Department of State, the Federal Aviation Agency (now the Federal Aviation Administration), the National Aeronautics and Space Administration (NASA), and the Central Intelligence Agency. Each of these member agencies appointed a full-time liaison to the NCS to serve as a point of coordination.



Robert S. McNamara was appointed to lead the NCS as the first Executive Agent. He defined the organization within DOD. (Photo by Yoichi R. Okamoto, White House Press Office)

## The hot line was just one NCS initiative launched in the early 1960s, as the newly organized NCS leadership team carried out President Kennedy's mandates.

Within weeks of the Cuban Missile Crisis resolution, the NCS created a direct teletype link known as the Washington-to-Moscow hot line, to safeguard against the kind of transnational miscommunications that plagued the negotiations. Significantly, the hot line marked the first major NCS contribution to Federal communications, and is still a functioning resource, serving as an essential tool in negotiations to end the Arab/Israeli Wars of 1967 and 1973, and in communications during both the 1991 Persian Gulf War and the 2003 Operation Enduring Freedom campaign.

The hot line was just one NCS initiative launched in the early 1960s, as the newly organized NCS leadership team carried out President Kennedy's mandates.

The President initially tasked the Executive Agent with preparing a near-term plan outlining initial NCS objectives, followed by a series of long-range plans over the course of the next several years. The NCS submitted a near-term plan in October of 1963, offering a preliminary look at the communications assets of several Federal agencies, identifying 32 communications networks operated by five major operating agencies.

Just a month after the NCS submitted this first planning goal, the Nation suffered a stunning loss, and the NCS its leading advocate, when an assassin killed President Kennedy in Dallas, Texas, on November 22, 1963.

### Historic Milestone

The Cuban Missile Crisis ranks with the Berlin Blockade as one of the major confrontations of the Cold War, and is often regarded as the moment in which the Cold War came closest to escalating into a nuclear war.



Following President Kennedy's death, Lyndon B. Johnson stepped into the presidency at a heightened time of involvement in the Vietnam War, and international security moved to the political forefront once again. Despite having lost its main proponent so early in its planning stages, the NCS continued work on developing a long-term plan that would serve as a foundation to the integrated Federal communications system President Kennedy had envisioned. Like his predecessor, President Johnson strongly advocated this concept, declaring that "there will be a single, unified communication system for use by the Federal Government under any condition, normal or otherwise."

Meanwhile, NCS member agencies were studying the interconnectivity and survivability of the commercial telecommunications networks that had become integral to Government function. In an effort to sculpt a new level of information sharing and interconnectivity to protect the Nation's communications infrastructure, the NCS Manager began fostering collaboration between public and private national security telecommunications stakeholders.

New NCS initiatives planted seeds of industry/Government collaboration that would become one of the NCS' most enduring principles. The Washington Area Secure High Speed Facsimile System, which interconnected a number of radio stations within the region, and the Emergency Employment of Radio Systems project, which evaluated the usefulness of Government and non-Government radio systems as an emergency back-up to the NCS, were some of the first NCS efforts toward that collaborative principle.

### 1970s

Richard M. Nixon won a landslide victory to his second term in office in 1972, pledging to guide the Nation's international conflicts toward peace. The same year, IT engineers were developing the first email protocols, and the Nation marveled the near-catastrophic Apollo 13 mission, crippled by explosion two days after its launch, returned safely to Earth. The NCS had also been exploring new territories, forging ahead with a mission to complete the final long-range plans for an integrated Federal communications system.

Apollo 13 was the third manned lunar-landing mission, part of Project Apollo under NASA in the United States. Two days after the launch, the Apollo spacecraft was crippled by an explosion, caused by a fault in an oxygen tank. However, the crew safely returned to earth in the command module. The mission was thus called a "Successful Failure."  
(Photo by NASA)



In 1970, President Nixon unveiled plans to retire both the Office of the Director of Telecommunications Management and the position of Special Assistant to the President for Telecommunications. Executive Order (E.O.) 11556, *Assigning Telecommunications Functions*, replaced these offices with the Office of Telecommunications Policy (OTP), with Clay T. Whitehead appointed OTP director.

Shortly after the NCS had forwarded its sixth and final long-range plan to the White House in 1971, the newly appointed NCS Manager, Air Force Lt Gen Gordon T. Gould, Jr., reexamined the NCS' long-range goals, and concluded that the original concept of a single universal communications system was unrealistic and unwarranted. Secretary of Defense Melvin R. Laird, the NCS Executive



President Richard Nixon and his wife, Pat in Nashua, New Hampshire. Nixon won a landslide victory to his second term in office in 1972.

Agent, agreed, and in April of 1972, he notified Mr. Whitehead that the NCS would drop the universal single system approach. The NCS determined that the Federal Government's telecommunications capabilities would be better served through the creation of a survivable, interoperable communications system, rather than the unified communications structure initially envisioned. Consequently, the NCS redesigned its operational structure into a partnership of telecommunications networks, run by a consortium of Federal departments and agencies that would pursue NCS goals through coordinated planning, interoperability, and system standardization in an evolutionary environment.



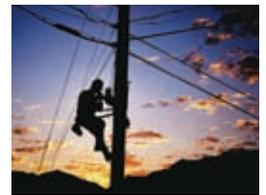
In March of 1978, President Jimmy Carter issued E.O. 12046, transferring NCS policy activity from the OTP to the NSC, which assumed responsibility for the development of plans, programs, and standards for the use of telecommunications resources in times of emergency.

With a new structure and a refreshed mission, NCS member agencies delved into researching increasingly relevant communications issues—interoperability, operational management, survivability, standards, and priority restoration. The OTP and the NCS Executive Agent ordered a review and decongestion of the restoration priority (RP) program, concerned that the increasing number of circuits, at 22,500 in 1970, would eventually congest the RP network. The NCS Manager led the pursuit of a realistic circuit priority restoration program that would ensure the availability of critical circuits in national emergencies, leading to the establishment of the NCS Circuit Restoration Priority Program and the Data Base Maintenance System in the latter half of the decade. The RP program made notable decongestion progress by lowering the percentage of Federal RP circuits from 42 percent in 1969 to 10 percent in 1980.

In the telecommunications arena, the Nation was entering a season of change with new and important trends—an increase in Government-owned and Government-leased networks, a rapidly accelerating technology landscape, and a resurgent Congressional and legal role in the telecommunications environment.

In 1974, the Government filed a lawsuit against AT&T that sought to dismantle its 70-year monopoly on the telephone industry. The prospects of a changed marketplace motivated small businesses and the Federal Communications Commission (FCC) to campaign for open competition among service providers and equipment manufacturers. The telecommunications environment was becoming increasingly complex, and the prospect of losing a single industry point-of-contact was creating looming challenges for the NCS in developing industry-wide emergency communications standards.

The changing environment spurred the concept of a single NS/EP framework for wartime and crisis telecommunications, and policy trends began to change. In March of 1978, President Jimmy Carter issued E.O. 12046, transferring NCS policy activity from the OTP to the NSC, which assumed responsibility for the development of plans, programs, and standards for the use of telecommunications resources in times of emergency. The order tasked the OTP with implementing these functions under the policy guidance of the NSC, and gave other functions to



#### Historic Milestone

In 1974, the Government filed a lawsuit against AT&T that sought to dismantle its 70-year monopoly on the telephone industry.



a new office within the Commerce Department—the Assistant Secretary of Communications and Information (which would become the National Telecommunications and Information Administration).

This realignment of responsibility, combined with policy concerns about the deregulation of the telecommunications industry and security tensions over an increase in Soviet-owned nuclear missiles, underscored a need for a clear policy statement with regard to national security communications. In 1979, President Carter signed the National Security Telecommunications Policy (NSTP) Presidential Directive, calling for communications facilities “to gather intelligence, conduct diplomacy, command and control our military forces, provide continuity of essential functions of Government, and to reconstitute the political, economic, and social structure of the Nation.” The Directive assigned the NCS to draft and mobilize an NSTP Implementation Concept Plan, and explicitly encouraged the NCS to place “substantial reliance” upon the private sector for advice and assistance. The plan spawned a wealth of NCS activities and contributions into the next decade.

### 1980s

The new presidency of Ronald Reagan marked the Nation’s transition into the 1980s, characterized by a rapidly emerging middle class, a blend of conservative politics, and a bold position of power in the changing Cold War environment. The NCS also faced new challenges domestically and internationally. For one, the NCS had a compelling mandate to prepare the Nation for potential critical situations in the face of a heightening arms race between the United States and the former Soviet Union. On the home front, after eight years of legal battling, in 1982 the Government announced the breakup of AT&T’s Bell System. The divestiture created dramatic changes in the telecommunications marketplace and complicated the challenges associated with creating effective NS/EP telecommunications policies. During this time, the FCC adopted an order to provide a uniform system of priorities for the restoration of vital commercial private line services during emergency situations. Up until the divestiture, the Federal Government relied almost completely on AT&T for the provision of survivable and restorable communications networks. The divestiture meant the loss of a single industry point-of-contact for NS/EP coordination.

In response to this new need for expanded collaboration with multiple industry contacts, President Reagan issued E.O. 12382, which created the President’s National Security Telecommunications Advisory Committee (NSTAC). President Reagan charged the NSTAC with providing the President with critical industry-based analysis and advice on policy and technical issues for the critical challenges the Nation faced in the NS/EP communications environment.

**Historic Milestone**  
On September 13, 1982, President Reagan created the President’s National Security Telecommunications Advisory Committee (NSTAC). The NSTAC was charged with providing the President with critical industry-based analysis and advice on policy and technical issues for the critical challenges the Nation faced in the NS/EP communications environment.



On April 3, 1984, President Reagan revised the NCS Charter with E.O. 12472, *Assignment of National Security Telecommunications and Emergency Preparedness Functions*. The order outlined a broad new scope for the NCS, defining an organizational structure and technical path for the creation of a concentrated NS/EP telecommunications function.

While E.O. 12472 did not deviate from the NCS' original mission to serve the Federal Government under any and all emergency circumstances, it would now also act as a nexus for industry and Government collaboration in NS/EP telecommunications planning, through any and all changes in the telecommunications environment. Industry owned the very communications structures on which governmental NS/EP communications depended, and this collaboration was vital to ensuring success in the NCS mission. The NCS soon became the model for cooperation between industry and Government on issues of national security, facilitating unprecedented collaborations between the public and private sectors.

At that time, arrays of new service providers were developing increasingly complex systems. To integrate evolving industry technology into NS/EP communications, the NCS mobilized three highly effective, and still-operating, partnerships—the NSTAC, the National Coordinating Center (NCC), and the Committee of Principals. Over 20 years later, the success of these partnerships would make them priority elements in the NCS transition into the Department of Homeland Security (DHS), upon its creation following the terrorist attacks of September 11, 2001.

The 1980s were also pivotal for the growth of digital technology becoming widely available on a consumer level. Bill Gates developed the Microsoft Corporation from an obscure concept to become a driver of an entirely new industry. As a result, computers took great leaps in speed, reliability, portability, and affordability, and became widely accessible for personal use. The applications for computers and digital technology use skyrocketed to levels unimaginable only a few years prior. These watershed evolutions in the technological landscape precipitated an escalation in both the threats to national security, as well as the tools Government could utilize to counter those threats.

For the NCS, keeping pace with technological progress has always been a national security necessity both in identifying threats and utilizing digital tools. In 1986, the year in which IBM unveiled the first laptop computer, the NCS developed the Network Design and Analysis Capability to analyze the impact of potential telecommunications losses through a suite of digital modeling tools. The same year, the White House approved the first National Level NS/EP Telecommunications Program (NLP) to devise a comprehensive telecommunications nuclear response and recovery plan. The program was a milestone for the NCS mission to develop an NS/EP telecommunications capability. The NCS projected within this initial NLP program the evolution of technological capabilities to improve the routing, survivability, connectivity, and interoperability of the Public Switched Network (PSN) and the Internet, particularly in the event of nuclear attack.



In 1986, the White House approved the first National Level NS/EP Telecommunications Program (NLP) to devise a comprehensive telecommunications nuclear response and recovery plan.



#### Historic Milestone

In 1986, IBM unveiled the first laptop computer—the IBM 5140. Although the 5140 weighed 12 lbs, it was a technological breakthrough at the time and offered the ability to run without using a power outlet.

By the end of the decade, the dissolution of the Cold War gave way to entirely new international security issues, as the role of the NCS in NS/EP became more cyber-savvy.

### 1990s

For the NCS, evolving worldwide political climates and emerging technological advances in the telecommunications network defined the 1990s. The end of the Cold War and the collapse of the Soviet Union gave way to the progression of globalization, while the Nation enjoyed an economic resurgence from the 1980s recession. While the establishment of the Internet society and the unveiling of the World Wide Web in 1992 meant that Internet technology was evolving into a powerful means of communication, business, and information sharing, it would also create potential for malevolent use and a new brand of security threat.



The World Wide Web was unveiled in the early 1990s, providing a powerful means of communication, business, and information sharing, at the same time, also creating new security threats.

In the wake of the post-Cold War Era, a new type of threat to the Nation’s telecommunications system emerged out of the world’s increasing dependence on the Internet, computers, and other networked information systems. It was perpetrated by individuals and non-state actors, rather than enemy nation states.

When President Reagan signed E.O. 12472, revising the NCS’ role in national security, the United States considered nuclear war with the Soviet Union as the Nation’s primary threat. In the wake of the post-Cold War Era, a new type of threat to the Nation’s telecommunications system emerged out of the world’s increasing dependence on the Internet, computers, and other networked information systems. It was perpetrated by individuals and non-state actors, rather than enemy nation states.

To the average American, when the concept of “cyber warfare” began to emerge, it didn’t carry the visceral translation of other national security threats, such as nuclear war. Cyber visionaries, however, foresaw cyber warfare’s 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. Attackers could be terrorist organizations or independent hackers from domestic or international territories, operating based on non-conventional motivations. Under the virtually anonymous, under-secured nature of the Internet of that time, the identities of potential cyber attackers could go virtually undetected and unprosecuted. The NCS recognized the need to modernize its approach to NS/EP telecommunications in the face of this new threat, and launched innovative programs to respond directly to the new cyber risk.

By the early 1990s, many users called the Internet—in conjunction with public, private, and proprietary networks, and other emerging information technologies—the National Information Infrastructure (NII), a concept that originated in the late 1980s when information systems were still largely operationally independent. In 1991, the NSC asked the NCS to develop a Critical Warning Information Network to facilitate immediate threat alerts and secure information belonging to the network, industry, and Government partners. Renamed the Critical Infrastructure Warning Information Network (CWIN) in 2003, the CWIN provides the Government with a reliable voice and data network in times of emergency. At its full operational



**Historic Milestone**

In 1993, with Bill Clinton in the first year of his presidency, the Federal Government released the *National Information Infrastructure: An Agenda for Action*, a framework for addressing the policy and technology associated with the NII.

capacity, the CWIN provides time-sensitive warnings on imminent threats or ongoing attacks against the Nation’s critical infrastructures, and supports the transmission of classified and unclassified information.

In 1993, with Bill Clinton in the first year of his presidency, 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 NCS responded to the burgeoning growth of the NII and the Internet with new initiatives, including Network Security Information Exchanges, which provided working forums to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. The industry landscape also faced policy changes. In 1996, Congress passed the *Telecommunications Act of 1996*, the first major overhaul of telecommunications law since the *Communications Act of 1934*, in an effort to lower carrier prices and increase quality of service.

The mid-1990s also marked the first terror attacks on U.S. soil. On February 26, 1993, a car bomb was detonated below Tower One of the World Trade Center in New York City, injuring over 1,000 people and killing six. And on April 19, 1995, a domestic terrorist bombing at a U.S. Government complex in downtown Oklahoma City killed 168 people and injured hundreds more.

Both attacks shook the Nation, deadly precursors to the devastating attacks that would occur on September 11, 2001. The U.S. military presence overseas and efforts to disarm Iraq in the wake of the first Persian Gulf War also began to escalate. The escalation was one of several early indications of militant Islamic hostility toward the United States, and a precursor to the War on Terror. On the policy front, the Clinton Administration issued a series of E.O.s and Presidential Directives to engage the private sector in efforts to examine the vulnerability of critical infrastructures to terrorism and develop a strategy to secure the continuity and viability of the Nation’s critical infrastructures. President Clinton issued Presidential Directive 63, *Critical Infrastructure Protection*, in 1998 in response to findings from the President’s Commission on Critical Infrastructure Protection (CIP). The Directive called for a public-private CIP partnership, established a national organizational structure to guide that partnership, and directed the development of Government and cross-sector CIP plans.

The NCS’ role in emerging critical infrastructure concerns had begun to take shape by the close of the decade, when the NCS began to focus on grave infrastructure threats and vulnerabilities. Directive 63 spurred a unique collaborative mission between industry and Government to ensure the availability of critical NS/EP telecommunications services in emergency situations. Early in the next decade, the NCS would create an Integrated Product Team (IPT) that would clearly define the NCS role in CIP plans. With the majority of the telecommunications infrastructure in the hands of the private sector, leveraging Government partnerships with industry would become an important part of that strategy, and a formal CIP Division was designated in 2001.

On April 19, 1995, a domestic terrorist bombing at a U.S. Government complex in downtown Oklahoma City killed 168 people and injured hundreds more. (DOD photo by SSgt Preston Chasteen)



In addition to spurring many of the NCS' CIP initiatives, the 1990s were also a time of pivotal partnership between the NCS and the Federal Emergency Management Agency (FEMA). The NCS collaborated with FEMA to identify key communications requirements for disaster areas and to implement improvement solutions. These activities included the maintenance and restoration of communications lines and systems during natural disasters like 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.

While Y2K fears did not come to fruition as 1999 came to an end, the U.S. Government intercepted a terror plot to attack Los Angeles National Airport, as the terrorist threats that had for years seemed contained overseas seemed to have clearly seeped onto American soil.

The NCS also enhanced and updated its own relevant emergency response programs, developing the Government Emergency Telecommunications Service (GETS) as a method of prioritizing wireline telephone calls in emergency situations. GETS became available to authorized users in 1995. The NCS also created the Alerting and Coordinating Network (ACN) as a private network providing users with a means to directly connect to State and local Government agencies, telecommunications service providers, and equipment manufacturers. The National Telecommunications Alliance (NTA) operated the system as a public network for coordination among the Regional Bell Operating Companies, long distance carriers, and equipment manufacturers, until the NTA dissolved in January 2001. Because the ACN provides emergency back-up communications capabilities that could help coordinate response to and recovery from a widespread network outage, the Office of Science and Technology Policy (OSTP) directed the NCS to acquire the assets and provide operational support to ensure the continued viability of the network.

Today, operational responsibility for the ACN is under the operations of the NCC for Telecommunications, serving as a vital coordination resource in the event of severe congestion or catastrophic damage to the PSN. The Office of the Manager, NCS, provides overall support for the program.

As the Nation approached the 21st Century, the Year 2000 (Y2K) date-change came and went without the feared computer disaster from software unequipped to handle the century change. Around the world, however, new security threats and emergency crises were developing. While Y2K fears did not come to fruition as 1999 came to an end, the U.S. Government intercepted a terror plot to attack Los Angeles National Airport, as the terrorist threats that had for years appeared contained overseas seemed to have clearly seeped onto American soil.

In Iraq, enforcement of disarmament terms from the first Gulf War on Saddam Hussein began to escalate into an ongoing war. As the NCS headed into a new century, its criticality to national security would be fiercely tested, strengthened, and emboldened in the face of the most deadly attack on American soil in modern history, and one of the most acute periods of national solidarity.



**Historic Milestone**  
In 1995, the NCS released GETS as a method of prioritizing wireline telephone calls in emergency situations.



“America will never run...and we will always be grateful that liberty has found such brave defenders.”

President George W. Bush

# Modern Mayday: A New Era of Emergency Communications

## September 11, 2001

The morning of September 11, 2001, began as a clear, sunny day on the East Coast, when without warning, the Nation was attacked. Nineteen al-Qaeda terrorists led four suicide missions within two hours, hijacking two commercial airliners used to topple the World Trade Center buildings in New York City. A third plane struck the Pentagon in Washington, D.C., and a fourth plane crashed into a western Pennsylvania field, never reaching its target. The attacks wreaked the largest single-day loss of life in American history, killing nearly 3,000 civilians. Four days later, President Bush declared that the Nation was at war against terror.

The unprecedented devastation had an indelible and enduring impact upon the Nation. But in the midst of mourning, the attacks spurred the American people into an unprecedented mode of unified response. Resource, recovery, and rebuilding efforts came from almost every facet of the American landscape, from the average citizen to agencies like the NCS.

Less than two years earlier, in January 2000, the White House had designated the NCC as an Information Sharing Analysis Center to facilitate telecommunications infrastructure information exchange between Government and industry. The NCS utilized the NCC to gather industry stakeholders and begin immediate communications infrastructure recovery and response efforts at Ground Zero in New York City following the attacks.

It was no small task. The World Trade Center attacks crippled several critical switches, cut major cable lines, flooded cable vaults, and disrupted electricity to the area. With the collapse of the towers, damages included an estimated 200,000 voice lines, 100,000 business lines, 3.6 million data circuits, and 10 cellular towers. The devastation

Fires still burned amidst the rubble and debris of the World Trade Center in New York City in the area know as Ground Zero two days after the September 11, 2001, terrorists attacks. (DOD photo by PH2 Jim Watson, USN)



congested communications for emergency personnel and civilians. NSTAC member companies—representing most of the major communications and information technology industry—looked to the NCS for ways to assist crisis response efforts, even before the damage to their own infrastructures had been fully assessed—and many were among the most badly damaged.

The NCC worked around the clock from four different sites—the NCC, FEMA, DOD’s Global Network Operations Support Center headquarters, and one remote continuity of operations location—to ensure NS/EP communications among Federal, State, and local responders and to restore damaged communications lines at the Pentagon and in New York.

The NCC worked around the clock from four different sites—the NCC, FEMA, DOD’s Global Network Operations Support Center headquarters, and one remote continuity of operations location—to ensure NS/EP communications among Federal, State, and local responders and to restore damaged communications lines at the Pentagon and in New York. The NCS fulfilled over 500 priority service requests from 46 different organizations within the first two weeks after the attacks, and over 7,000 requests over the course of the next year—almost double the number from the previous year.

The NCS also issued 1,000 new GETS cards to agencies including the NSC, the Federal Bureau of Investigation, the National Military Command Center and the Joint Chiefs of Staff, as the criticality of emergency communications was pushed to the forefront of NS/EP priorities. Despite heavy network congestion, 95 percent of the thousands of priority service calls attempted in that period were successfully completed on the first attempt, revealing the invaluable nature of GETS provisioning in times of crisis.

In the midst of its provisioning efforts, the NCS also hosted daily information sharing conference calls among NCC members, allowing the NCC to coordinate crucial Manhattan “Red Zone” access for telecommunications carriers, who restored NS/EP communications, refueled emergency generators, and assisted in the continuity of facility operations. The NCC also guided the sobering mission of leading the Wireless Emergency Response Team into the Red Zone to aid in the search for victims, pinpointing cell phone and pager signals from beneath the wreckage.

The New York Stock Exchange reopened just six days after the attacks. The valiant efforts of post-September 11 response teams were a testament to the Nation’s resiliency, helping to breathe continuity back into the American way of life. The attacks were also a crucible of devastating proportions, with fallout lessons that immediately became policy priorities.

## The NCS and Homeland Security

Emergency communications was just one element of national security that the Government scrutinized, reassessed, and reinforced in the wake of September 11, 2001. President Bush signed the *Homeland Security Act* in November of 2002 as a means of reinforcing all NS/EP elements, creating DHS to organize all of the necessary Federal agencies in pursuit of a more secure home front.



U.S. Air Force Master Sergeants in the Air National Guard, set up a commercial satellite antenna in Beaufort, South Carolina, April, 17, 2008. The commercial satellite antenna mobile ground station provides communications, imagery, and data to users from civil engineers and intelligence units. (U.S. Air Force photo by SMSgt Edward E.Snyder)

Homeland security organizers immediately identified the NCS as having existing relationships with telecommunications industry stakeholders, and experience in infrastructure protection and assurance. The NCS watch center capabilities and priority service programs were a lifeline during the September 11 recovery efforts, and as a result of this critical relationship to homeland security efforts, the NCS was among 22 agencies on March 1, 2003, formally transitioned into DHS, which replaced DOD as the NCS Executive Agent. Though the NCS' existing initiatives had received praise as Federal models, the new homeland security environment still needed a new generation of NS/EP programs to accommodate burgeoning technology trends and heightening security threats. In May of 2002, the Wireless Priority Service (WPS), which prioritizes key personnel at the front of a telephone queue during times of crisis and network congestion, became available in the Washington, D.C., and New York metropolitan areas, and expanded along the East Coast throughout 2003. That year, the NCS joined the FCC in launching a nationwide campaign to register the Nation's 9-1-1 call centers, or Public Safety Answering Points, in the Telecommunications Service Priority program to receive priority restoration in the event of a crisis.

In May of 2003, DHS also announced that State and local governments would receive nearly \$1 billion for anti-terrorism equipment training and exercises, and tens of millions of dollars would be invested in urban search and rescue teams, interoperable communications equipment, and community emergency response teams.

The growing threat of cyber attacks was also at the forefront of DHS preparations. In June of 2003, DHS announced the creation of the National Cyber Security Division (NCSD), to analyze and reduce cyber threats and vulnerabilities, disseminate threat warning information, coordinate incident response, and provide technical assistance in continuity of operations and recovery planning. While the NCSD and the NCS operate as separate DHS entities, their missions both involve ensuring safe, secure, and reliable communications infrastructure, and thus remain organically collaborative in nature.

A year after NCSD formed, the division unveiled its National Cyber Alert System, developed to offer Americans timely and actionable information to better secure their computer systems. The Department tapped the U.S. Computer Readiness Team to facilitate the alert system, among its efforts to coordinate preemptive and responsive methods against cyber attacks across the Nation.

DHS released the National Response Plan (NRP) in January of 2005, in accordance with Homeland Security Presidential Directive-5, establishing a national, unified approach to managing domestic security incidents. The NRP



### Historic Milestone

The NCS was among 22 agencies on March 1, 2003, formally transitioned into DHS, which replaced DOD as the NCS Executive Agent.

formed a comprehensive enhancement of the Government's ability to manage domestic incidents and coordinate among State, local, and tribal governments, and the private sector. The plan incorporated best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrated these disciplines into a unified structure. The NRP remains an evolving body of work, under constant review for its relevancy to homeland security needs and innovations, and the NCS provides support operations in the form of Emergency Response Training seminars and exercises. In 2008, a revised NRP was named the National Response Framework (NRF), to better align the document with its intent and to encourage the continued development and refinement of all-hazards emergency plans. The NRP remained in effect until the NRF took effect in March of 2008.

### Hurricane Katrina

Hurricane Katrina began forming on August 23, 2005, as a tropical storm over the Bahamas. The storm became a hurricane just two hours before it made landfall in Florida on the morning of August 25, and rapidly intensified upon entering the Gulf Coast. On August 27, the hurricane reached Category 3 intensity and nearly doubled in size. By the morning of August 28, Katrina had intensified to a Category 5, and at 1 p.m. that afternoon, it had peaked in strength, wielding winds of 175 mph.

US Coast Guard Petty Officer Second Class (PO2) Shawn Beaty scans the horizon looking for survivors from the crew door of his HH-60 Jayhawk helicopter during a search and rescue mission over the city in New Orleans, Louisiana, during Hurricane Katrina relief operations. (DOD photo by PO2 Nyxolyno Cangemi)



The surge battered the Gulf Coast, devastating multiple Mississippi cities. In New Orleans, Louisiana, nearly every flood protection levee in the metropolitan area failed, and 80 percent of the city was under water for weeks. At least 1,836 people died in Hurricane Katrina and in the subsequent floods, making it the deadliest U.S. hurricane since 1928, and exposing harsh realities about the need for strengthened NS/EP programs at all levels of response.

Satellite imagery of Hurricane Katrina hovering over the Gulf Coast.

The destruction debilitated communications in many of the effected regions. A single disabled fiber-optic cable or malfunctioning computer program can potentially disrupt thousands of wireline and wireless paths, congesting public telephone networks in spite of carrier backup systems. Many Louisiana responders found that, with jammed outgoing trunks, the loss of two central offices at a local phone company, and the loss of the area's primary long distance carrier, GETS was essential to continuity of operations, and allowed for the coordination of critical

supply shipments. Without GETS, many areas would have been completely cut off from communications—especially Baton Rouge, where contact with the state emergency operations center was critical to recovery efforts.

The NCS also heavily utilized the NCC's SHARed RESources (SHARES) High Frequency (HF) Radio Program in the midst of the Hurricane Katrina aftermath. The SHARES program coordinates the assets of over 1,000 HF radio stations worldwide to voluntarily pass emergency messages when normal communications are destroyed or unavailable.

At one point in the critical days following the hurricane, the SHARES Radio Room fielded a call from a Maryland civilian radio operator who had intercepted a report of 100 students and nuns stranded by flooding, trapped on the fifth floor of a building at Xavier College in New Orleans. SHARES coordinated with a Coast Guard air traffic control unit, at the time positioned in Mobile, Alabama, which relayed the rescue information to its helicopters in the crisis area, and all 100 people were rescued.

During the first 72 hours of the Hurricane Katrina crisis, an estimated 3,000 emergency messages and situation reports for the federal sector passed through SHARES. In the first week, SHARES worked closely with state and civilian emergency communications organizations to assist and facilitate an estimated 50,000 emergency messages.

### **Lessons Learned: Creating A Network of People**

The hurricane season of 2005 dealt a heavy cache of lessons learned. Those lessons underscored the criticality of communications infrastructures to the security of the Nation and highlighted the foundation of the IT and communications sectors to the activities of daily life and prosperity—financial services, transportation systems, Government, online commerce, health care, manufacturing, and emergency services and emergency communications.

## **DHS established the Office of Cyber Security and Communications to work with public and private sectors toward ensuring the availability, resiliency, security and interoperability of network services.**

Recognizing the imminence of change and progress within these infrastructures, DHS has connected the NCS to several collaborative veins that focus the mission of communications security to accommodate the evolving landscape. Within the next decade, the convergence of communications technology into a single, advanced, integrated IP network that includes local and long distance voice, video, and data will support an ever-widening and globalized array of services. DHS established the Office of Cybersecurity and Communications (CS&C) to work with public and private sectors toward ensuring the availability, resiliency, security, and interoperability of network services. CS&C's work is channeled through the NCS, NCSD, and the Office of Emergency Communications (OEC), established in 2007 under CS&C. The NCS, the NCSD, and the OEC have an ongoing partnership to foster public, private, and international alliances to enhance the preparedness of communications infrastructures. The NCS and the OEC, in partnership with industry and first responder communities, actively seek to develop the equipment and technologies that meet the defined requirements



Recognizing the imminence of change and progress within the Nation's IT and communications sectors, DHS and the NCS are working collaboratively to maintain communications security.

of the emergency response community, providing security, reliability, scalability, and affordability. Meeting these requirements is necessary for existing technologies and emerging technologies, including the convergence from circuit-switched telecommunications to broadband. The NCS also is bolstering its GETS/WPS outreach efforts among Government, industry, and first responder communities and has developed a capability for converging GETS into the next generation IP environment.

### **Using a Global Vision to Connect, Secure and Prepare the Nation**

For 45 years, the NCS has provided services to the Nation that have endured decades, through crisis, progress, and technological evolution. Domestic and international tensions created unprecedented communication challenges in the 1960s, while the expansion of the telecommunication industry in the 1970s and the technology boom of the 1980s and 1990s complicated the policy and strategy landscapes.

While the 21st century has dealt a torrent of entirely new challenges, the NCS has responded with a progressive approach that draws on a well-laid historical foundation and injects the modern security and preparedness innovations that will guide NS/EP plans into the future.



Homeland  
Security