

40th Anniversary

Forty Years of Service to the Nation: 1963-2003

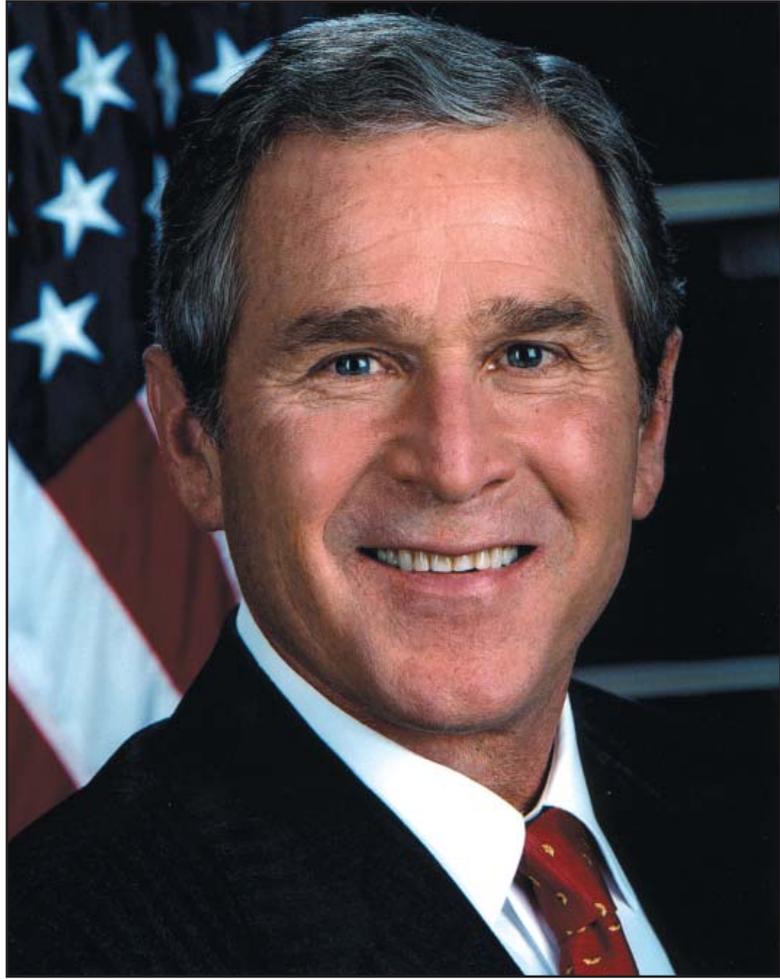


National
Communications
System



***40th
Anniversary
1963 - 2003***

**National
Communications
System**



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.

A handwritten signature in black ink, appearing to read "George W. Bush". The signature is written in a cursive, flowing style with a long horizontal stroke at the end.

Table of Contents

PART 1

BUILDING THE FOUNDATION

The Growing Need For Communications Management.....2

Planning Begins.....5

Changing Role.....9

PART 2

REDEFINING THE AGENDA

Growing National Security Telecommunications Initiatives..... 16

New Policy On National Security Telecommunications.....19

Critical Beginnings.....24

Expanding Agenda.....28

PART 3

EARLY RECOGNITION, EMERGING RESPONSE

Early Critical Infrastructure Protection Efforts.....40

Federal Critical Infrastructure Protection Policy.....41

Continuing Role in Critical Infrastructure Protection.....43

Instituting the Critical Infrastructure Protection Agenda.....46

PART 4

READY TO SERVE

Response To The September 11, 2001, Terrorist Attacks.....56

Activities Post-September 11, 2001.....57

Changes In The Federal Government.....63

Conclusion.....65

Introduction

The National Communications System's (NCS) celebration of its 40th birthday marks the anniversary of many significant telecommunications national security and emergency preparedness (NS/EP) efforts. In 1962, the Cuban missile crisis brought the world to the brink of nuclear war. Tensions ran extremely high, and the inadequacy of communications systems between the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state exacerbated the situation. In response, President John F. Kennedy enacted a plan to ensure communications infrastructures were better supported during times of national emergencies.

President Kennedy's plan led to the establishment of the NCS, for which maintaining a strong telecommunications infrastructure and securing lines of communication for the Government became the core mission. While the NCS's initial goals centered on maintaining and protecting the telecommunications infrastructure in the event of a nuclear strike, its goals gradually evolved with the growth of the Internet, the threat of a cyber attack, and the terrorist attacks of September 11, 2001. The present ever-looming threat of a cyber, chemical, biological, or nuclear attack keeps the NCS diligent in its preparation and response activities.

Four decades after the creation of the NCS, both the communications and the threat environment have dramatically changed. From the telephone lines that run across the United States, to the high-speed fiber optic cables that stretch under the seas connecting the globe, communication drives the world's political and economic well being. How has the NCS evolved with these changes? How has the organization prepared for the future? Is the original mission still relevant? On the verge of a new era, the NCS stands ready to face new challenges from an ever-changing world.

APPENDIX

END NOTES.....A-1

ACRONYMS.....B-1

BIBLIOGRAPHY.....C-1

CHRONOLOGY.....D-1

GLOSSARY.....E-1

Part 1

BUILDING THE FOUNDATION

Part 1

Building the Foundation

THE GROWING NEED FOR COMMUNICATIONS MANAGEMENT

Since the advent of the telegraph in the 1840s, electrical communications have played a vital role in Presidential decision-making and national security. Presidents as early as Abraham Lincoln depended upon telecommunications to send orders, follow the progress of troops, and communicate with foreign allies during times of war. As communications systems developed and became increasingly complex, the need emerged for better organization and management of the Government's communications resources. This need first came to the attention of the White House during the Administration of President Dwight D. Eisenhower.

Early in 1959, the Eisenhower Cabinet discussed the need for a detailed plan to build a unified communications system, to better serve the Government in times of peace and emergency.¹ These discussions led to the February 16, 1962, issuance of Executive Order (E.O.) 10995, *Assigning Telecommunications Management Functions*,² establishing the Office of Director of Telecommunications Management, within the Executive Office of the President (E.O.P), to centralize leadership for telecommunications policy at the White House and achieve a balanced and well-planned national and international telecommunications program. However, a nearly disastrous communications failure during the 1962 Cuban Missile Crisis resulted in an abrupt shift of the communications priorities outlined in E.O. 10995. President Kennedy, who succeeded President Eisenhower in 1961, issued a memorandum ordering the immediate development of a national communications system for enhanced communications capability in support of Presidential decision-making in times of crisis. The Cuban Missile Crisis served as the catalyst for the formal creation of the NCS.

President Kennedy on the phone in the Oval Office.



THE CUBAN MISSILE CRISIS: 1962

On October 26, 1962, Soviet Premier Nikita Khrushchev offered to withdraw Soviet missiles from Cuba in exchange for an American pledge not to invade the island nation. However, the United States was only hours away from a decision to proceed with an air strike and land invasion of Cuba, and procedural and technical delays in the transmission and receipt of this vital message nearly precipitated a disastrous incident. After a communications delay of 12 hours, the Russian message offering to withdraw finally arrived, deescalating tensions between the two nations and laying the basis for an agreement that would avert a potential nuclear event. This nearly catastrophic communications failure brought to light a number of communications deficiencies. The incident led President Kennedy to direct the National Security

Council (NSC) to investigate national security communications, including leader-to-leader exchanges. In addition, Kennedy used this opportunity to review internal Government communications processes. He established the Interdependent Committee on Communications, dedicated to eliminating deficiencies in the Nation's communications networks, which support the President and other key decision makers.³

ESTABLISHMENT OF THE NATIONAL COMMUNICATIONS SYSTEM: 1963

For nearly 8 months, the Committee on Communications explored the Federal Government's emergency communications. Ultimately, the committee confirmed the interdependence of the military, diplomatic, and civilian agencies of Government on one another's resources in times of crisis, and concluded that the missing link was a common communications system connecting all the agencies. To address this need, the committee recommended the creation of a survivable national communications system to serve the communications needs of the President, the Department of Defense (DOD), essential diplomatic and intelligence activities, and key nonmilitary civilian leaders during times of crisis.

President Kennedy issued a Presidential Memorandum on August 21, 1963, *Establishment of the National Communications System*,⁴ which directed the formation of a system to deliver enhanced communications support to critical Government functions during times of national crisis. The new communications system would link, improve, and gradually extend the communications facilities and components of the various Federal agencies. Included in the Memorandum were two documents outlining the NCS's organizational framework and work plan: *Procedures and Working Relationships for the NCS's*, dated August 21, 1963, and *Statement of Initial Tasks for the NCS*, dated August 6, 1963. These documents set the tone and direction of the NCS's long-range planning for the 1960s.



National Communications System Member Organizations

- | | |
|--|---|
| ▶ U.S. Department of State* | ▶ Federal Emergency Management Agency |
| ▶ U.S. Department of the Treasury | ▶ The Joint Staff |
| ▶ U.S. Department of Defense* | ▶ General Services Administration* |
| ▶ U.S. Department of Justice | ▶ National Aeronautics and Space Administration* |
| ▶ U.S. Department of the Interior | ▶ Nuclear Regulatory Commission |
| ▶ U.S. Department of Agriculture | ▶ National Telecommunications and Information Administration |
| ▶ U.S. Department of Commerce | ▶ National Security Agency |
| ▶ U.S. Department of Health and Human Services | ▶ United States Postal Service |
| ▶ U.S. Department of Transportation | ▶ Federal Reserve Board |
| ▶ U.S. Department of Energy | ▶ Federal Communications Commission |
| ▶ Department of Veteran Affairs | ▶ Federal Aviation Agency (now the Federal Aviation Administration)** |
| ▶ Department of Homeland Security | |
| ▶ Central Intelligence Agency* | |

* One of the six initial Government agencies appointed to participate in the NCS activities

** One of the six initial Government agencies appointed to participate in the NCS activities—no longer a member organization

As defined by the *Procedures and Working Relationships for the NCS* document, the organization’s structure would be two-tiered with two executive-level positions: the Director of Telecommunications Management and Special Assistant to the President for Telecommunications. The President decreed these positions to be held by the same individual, and named Science Advisor Jerome B. Wiesner to these positions on an acting basis. At the Cabinet level, there would be one NCS Executive Agent. The President appointed Secretary of Defense Robert S. McNamara to this post and directed him to name an NCS Manager.

Given that the new system linked the communications systems of several Federal agencies, the *Procedures and Working Relationships for the NCS* identified the communications assets of six agencies (the General Services Administration (GSA), the DOD, the Department of State (DOS), the Federal Aviation Agency (now the Federal Aviation Administration), the National Aeronautics and Space Administration, and the Central Intelligence Agency) for the NCS. Each organization was to appoint a full-time NCS representatives.

Mr. Wiesner worked closely with the President’s National Security Advisor, the Director of the Office of Science and Technology (now the Office of Science and Technology Policy (OSTP)) and the Director of the Bureau of the Budget (now the Office of Management and Budget (OMB)). In addition, he promoted the interagency coordination necessary for building a multi-agency system and worked with the Bureau of the Budget to develop the guidelines and procedures for financing the NCS. Program planning, however, would originate with the Manager, NCS, with advice from the operating agencies.⁵ NCS-designated assets and any required improvements and modifications were to be funded by the operating agencies.

Washington to Moscow Hot Line

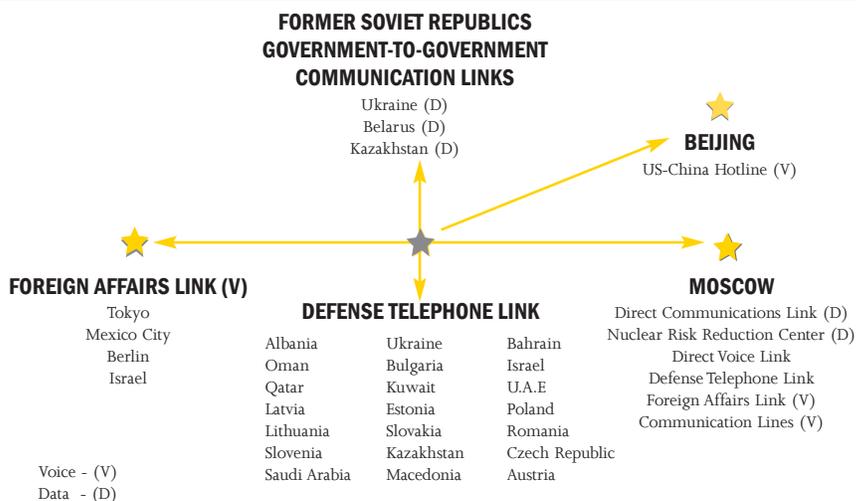
During the Cuban Missile Crisis of October 1962, one of the major communications trouble spots centered on the exchange of private messages between President John F. Kennedy and Soviet Premier Nikita Khrushchev. For this reason, the crisis pushed the need for a direct, timely, and

private communications link between U.S. and Soviet superpower leaders to the forefront of the communications agenda. As a result, the two Governments approved and developed a duplex cable circuit, known as the “Hot Line,” to link the countries. The Hot Line

became operational on August 30, 1963, and as technology progressed operators modernized the Hot Line with a satellite hookup and high-speed facsimile capabilities.

The communications link continues intact and has proven successful on many accounts. U.S. leadership first exercised the link in real time during the 1967 Arab-Israeli Six Day War to resolve a dangerous interaction between Soviet and U.S. fleets in the Mediterranean Sea, and then used it a second time during the 1973 Arab-Israeli War. Throughout the 1991 Gulf War, Presidents George H. W. Bush and Mikhail Gorbachev used the Hot Line to communicate with each other. Most recently, Presidents George W. Bush and Vladimir Putin used the Hot Line to discuss plans to rebuild Iraq following the 2003 Iraq War.

Since the inception of the Washington to Moscow Hot Line, the Hot Line has expanded to connect the President with leaders around the world.



PLANNING BEGINS

Soon after the President issued the 1963 Memorandum, the NCS began planning the development of a new communications system. On August 30, 1963, the NCS opened a direct teletype link between Washington and Moscow, designated the Washington-to-Moscow Hot Line. The Hot Line marked the beginning of the NCS's successful history of consistent provisions for communications capabilities to the Government.

The newly appointed NCS officials were dedicated to the tasks outlined in the *Statement of Initial Tasks* for building a new Government communications system. In his first duty as NCS Executive Agent, Secretary McNamara appointed Solis Horwitz, DOD, as Assistant to the Executive Agent, and Army Lieutenant General Alfred E. Starbird, Director, Defense Communications Agency (DCA) (now the Defense Information Systems Agency (DISA)), as Manager, NCS. General Starbird became the principal NCS technical planner, responsible for designing the system and developing plans for its operational management.⁶

The Executive Agent, and subsequently the Manager, NCS, was responsible for building the NCS organizational framework for the President's approval and implementation. As outlined in the *Statement of Initial Tasks*, the following tasks were assigned to the Manager, NCS:

- Prepare an initial near-term plan and then a series of annual long-range plans that would project in detail the NCS's evolution;
- Select communications assets for inclusion in the NCS;
- Identify the Government departments or agencies responsible for installing, operating, maintaining, and modifying each subsystem or component;
- Develop detailed organizational plans for operating and managing the NCS, including a circuit restoration program;
- Address standards associated with the Government's telecommunications requirements;
- Develop a plan to allocate radio frequencies;
- Develop an NCS test and exercise plan;
- Formulate a research program on emerging technology; and
- Organize and staff NCS activity.

As identified in the *Statement of Initial Tasks*, the near-term and long-range concept plans were to identify NCS objectives and requirements and to list those Federal agencies' communications assets that should become part of the new system. NCS requirements not fully met by present systems were to be identified and recommendations drawn up for the necessary modifications and improvements.

General Starbird initiated planning for an integrated system to link Government long-haul networks both procedurally and technically. This system would comprise common-user networks, dedicated networks, and Hot Line circuits, and would provide capabilities for the command and control of military forces, continuity of Government, and management of foreign crises. However, after completion of six long-range concept plans, the NCS changed its focus from a single communications system to achieving system interoperability among the Federal agencies and departments.

FIRST LONG-RANGE CONCEPT PLAN: 1964

General Starbird submitted the first of six NCS long-range concept plans to the Executive Agent in August 1964. In October 1963, General Starbird completed the NCS near-term plan, which presented an inventory of the communications assets of several Federal agencies, and became the basis for the first long-range plan. General Starbird identified 32 candidate communications assets for the system. The long-range concept plan also designated the Defense Communications System (DCS) as the survivable secure portion and national security component of the NCS and the Federal Telecommunications System (FTS) as the voice and data network for civilian agencies. The Manager emphasized that the creation of an efficient and economical NCS required the willingness of all operating agencies to make the necessary commitments.⁷ On October 31, 1965, retired Army Lieutenant General James D. O’Connell, the newly appointed Director of Telecommunications Management and Special Assistant to the President for Telecommunications approved the first NCS long-range plan as a planning document.⁸

Although President Kennedy’s assassination occurred before the completion of the first long-range NCS plan, his successor, President Lyndon B. Johnson, strongly supported the concept of a single unified Government communications system and approved the 1964 *National Plan for Emergency Preparedness*, which incorporated General Starbird’s first long-range plan. The 1964 *National Plan* defined the NCS as “the unified Governmental communications system, responsive to a single Executive Agent, derived from linking together, improving, and extending the communications facilities and components of the various Federal agencies.”⁹

SECOND LONG-RANGE CONCEPT PLAN: 1966

Following the approval of the 1964 *National Plan* (including the first long-range plan), General Starbird launched efforts for a second long-range concept plan. The objective was to outline plans for the Executive Agent to manage the NCS’s surviving assets during a Presidentially declared emergency and plans for interconnectivity, system survivability, and priority preemption.

To better position the NCS, General Starbird formed the Office of the Manager, NCS (OMNCS) in January 1966. Personnel from civil agencies, the military service, and agencies in the DOD comprised the OMNCS staff and addressed the needs of those agencies providing their communications assets to the NCS.

A primary issue addressed in the second long-range plan was the designation of an official to manage the NCS components during an emergency. Although both President Kennedy’s 1963 Memorandum and President Johnson’s 1964 *National Plan* empowered the Executive Agent to manage the NCS in an emergency, this designation conflicted with department and agency communications charters whose assets would be part of the NCS. To resolve this conflict, the FTS, operated by the GSA, would support the civilian side of Government and each Federal agency would continue to operate its own networks in the event of an emergency.

The second long-range plan also sought to outline the creation of a survivable, interconnected, and unified system. The plan defined a survivable system as one with sufficient primary or alternate routes to handle essential traffic after a nuclear attack. It would be supported by an operational management system and a precedence system for moving information according to the assigned priorities. To achieve this goal, General Starbird and the OMNCS examined existing communications resources, restoration priority, system management, and research and development. Because there was no database listing the communications resources of the NCS member agencies, the OMNCS began a program to inventory networks and facilities, particularly the major switched networks. The result of this work was NCS Memorandum No. 1-64, *Restoration Priority and Message Precedence Systems for the NCS*. Implemented in December 1965, the Memorandum provided for the initial categorization of circuit requirements by NCS operating agencies. To build the necessary operational management system to support a survivable system, the Executive Agent created the

NCS Operations Center, collocated with DCA's Operations Center complex; additionally, he established the NCS Emergency Action Group, composed of NCS operating agency representatives, who would convene to begin processing emergency telecommunications circuit requests.¹⁰

During this time, the OMNCS determined that: (1) an interconnected system would progressively link key NCS networks to enable the NCS to function as a "coherent single system," and (2) that a unified system would require the cooperation and involvement of the operating agencies. This goal was to be achieved by linking two or more of the major switched networks serving Government agencies. During the 1960s, efforts focused primarily on linking the voice and data networks of DOD's DCS with those of the GSA's FTS and on the operating procedures to affect these changes. Steps were also taken to interconnect the State Department's Diplomatic Telecommunications System with the DCS. To advance the mission of interconnectivity, the NCS proposed the development of system standards, an area of NCS attention for many years into the future.

In the summer of 1966, the OMNCS sent the completed second long-range plan to the White House for approval. Included in the second plan was a revised NCS mission statement that described building the NCS by "joining together technically and operationally the separate telecommunications systems of several executive branch departments and agencies...Such systems were to be improved progressively and so interlinked that the aggregate will function as if it were a coherent single system."¹¹ The plan directed the Manager to develop

"[The NCS's] impact is being felt in terms of increased communications flexibility, survivability, and economy, and in the creation of an atmosphere of mutual support and joint planning within the departments and agencies of the Executive Branch."

"organizational arrangements and necessary procedures for the NCS which will accomplish effective allocation, reallocation, and arranging for restoral of circuits and channels and other assets of the NCS."¹² Secretary McNamara commented that the plan "reflects the evolution of the NCS from a bold concept and a fledgling organization, [that is], one of a telecommunications super-management group cutting across agency lines to an effective viable organization. Its impact is being felt in terms of increased communications flexibility, survivability, and economy, and in the creation of an atmosphere of mutual support and joint planning within the departments and agencies of the Executive Branch."¹³ Despite the progress reflected in the second long-range plan, the White House expressed concern about the timely completion of a final system plan. The White House requested, in addition to the long-range concept plans, the Executive Agent prepare an interim NCS concept plan for the 1970s.¹⁴

THIRD AND FOURTH LONG-RANGE CONCEPT PLANS: 1968

In March 1968, the NCS published the third NCS long-range concept plan, followed by the publication of the fourth long-range concept plan in December of 1968. Reaffirming earlier NCS plans identifying the DCS and FTS as basic system elements, both plans included a three-part research program for survivability, interconnectivity, and unified planning to improve the communications network. The survivability studies addressed precedence systems, interconnected U.S. networks, emergency operations, effects of Electromagnetic Pulse (EMP), continuity of operations, and priority systems restoration.

Interconnectivity studies focused on finding technical solutions to network linking and developing hardware, software, and procedural standards. Unified planning continued to lag behind as the Executive Agent again urged the Manager to promote "an atmosphere of mutual support and joint planning" among the operating agencies. However, neither the third nor the fourth NCS long-range concept plans defined a final system concept for Presidential approval.

INTERIM NCS CONCEPT PLAN: 1968 - 1970

The White House staff renewed its call for an NCS interim concept plan for the 1970s “as a matter of urgency.”¹⁵ In response, the NCS devised a plan to establish and develop an integrated Government communications system by linking, improving, and extending, on an evolutionary basis, the communications facilities and components of the various Federal agencies. Reaching this goal would require the agencies to depart from “the present state of system fragmentation,” and, through a program of “common concepts, doctrine, system design, planning, and engineering, arrive at a national communications system which provides interconnection and ultimately the interoperability which the President should expect.”¹⁶ To reach this goal, the new NCS Manager, Air Force Lieutenant General Richard P. Klocko, explained to agencies that he intended “to develop, in coordination with the NCS operating agencies, specific design concepts, standards and criteria, and technical and operational system planning guidance, to establish the parameters for the future NCS configuration.”¹⁷

The NCS sent this plan for an integrated Government communications system to the White House in the summer 1968, but never implemented the plan. By the fall 1968, many involved in the project doubted the feasibility of establishing the NCS as a single unified system.¹⁸ Faced with the need to consider other alternatives, General Klocko completed a study in the fall 1969 that revised the concepts intended in earlier plans and proposed a national communications network in place of an integrated Government communications system. The proposed network would serve as a Government common carrier designed to satisfy the Government’s overall trunking needs.¹⁹

The Origin of the Internet

The modern Internet is one of mankind’s greatest technological achievements. Its origin, much like that of the National Communications System (NCS), is rooted in the defense of our country in the event of a communications emergency.

A key enabler for the growth of the Internet occurred in 1958, when Bell Labs created the first modem. The invention allowed computers to achieve interconnectivity over great distances for the first time. This concept, however, was not put into practical use for another 7 years, when two computers in Massachusetts and California connected over a low-speed phone line.

The Department of Defense (DOD), through its main research and development

branch, the Defense Advanced Research Projects Agency (DARPA), used the results of the initial interconnectivity experiments to initiate an experiment in linking critical defense computers. The DOD initiated the experiment because the department feared that a nuclear strike against the United States could disrupt communication lines, resulting in a loss of military command and control of its missiles and bombers. The Advanced Research Projects Agency Network (ARPANET), as it would be called, would effectively decentralize command and control so that if an enemy destroyed major cities, the U.S. military could still have control of its nuclear arms for a counterattack.

ARPANET, the direct forerunner of the modern Internet, was first tested on October 29, 1969, when Mr. Charley Kline (working from the University of California at Los Angeles) attempted to connect to a computer at Stanford Research Institute. The system crashed as Mr. Kline was typing the letter “G” of LOGIN. However, further tests of this system proved to be very successful. As more and more computers connected to ARPANET, the system generated greater file sharing and communications ability. Similar to the NCS, the course and mission of the Internet have evolved over time to form an entity of much greater impact than anticipated.

Moving forward, the OMNCS continued to formulate an interim NCS concept plan for the 1970s, focusing on a national communications network under the direction of a Federal committee for the NCS. This committee was comprised of representatives from Federal departments and agencies — including the NCS operating agencies — and would be responsible for the NCS’s evolution to a unified Governmental communications system.²⁰ However, in the fall 1970, the House Committee on Appropriations added to the NCS’s organizational difficulties by deleting all planning funds. Along with opposition from the operating agencies, this Congressional action prompted the NCS to reassess its role and postpone work on the interim plan.

CHANGING ROLE

In 1968, the President’s Communications Task Force — after a comprehensive review of U.S. communications policy — called for an expanded Government role in the long-range planning, policy formulation, coordination, and mission support for the Nation’s communications activities. However, as the 1970s began, and early expectations for a unified Government communications system had not been realized, Federal departments and agencies questioned the NCS’s mission and role.²¹

The Bureau of the Budget, upon completion of an independent study of Governmental organizations in communications, recommended reorganizing and strengthening the NCS. In July 1969, the General Accounting Office assessed the NCS and recommended President Richard M. Nixon consider establishing a new organization with the “stature, authority, and resources sufficient to provide a strong central focal point in telecommunications matters.”²² However, in December 1969, the White House published its own assessment and recommended the NCS retain its organizational arrangements until the White House could complete further studies.²³

REORGANIZATION: 1970

In February 1970, the White House completed its studies and the President unveiled plans to abolish both the Office of the Director of Telecommunications Management and the position of Special Assistant to the President for Telecommunications. He opted to replace them with the new Office of Telecommunications Policy (OTP) within the E.O.P. to oversee the NCS process. These plans were officially implemented in September 1970 with the issuance of E.O. 11556, *Assigning Telecommunications Functions*.²⁴

E.O. 11556 significantly reduced the NCS visibility and priority, as the White House sought to shift from a single-issue communications program to a more balanced consideration for a range of communications policy and management issues. The White House appointed Clay T. Whitehead as the OTP Director, serving as the President’s principal advisor on telecommunications. Empowered to set forth plans, policies, and programs to promote both national and international communications interests, Mr. Whitehead was to take executive branch leadership in promoting standards, new technology, interoperability, privacy, security, mobilization, and spectrum use and conducting economic, technical, and system studies. The President also mandated the OTP Director to identify competing, overlapping, duplicative, or inefficient telecommunications programs and to make recommendations concerning the scope and funding of these programs.

Mr. Whitehead rejected many of the basic concepts underpinning the long-range planning for the NCS. He felt the original purpose of the NCS had been joint planning and coordination, rather than total system integration. He canceled the decision to interconnect the FTS and DCS networks — a key provision in the original NCS plans²⁵ — and opposed the idea of a single communications manager in national security or any other area.

FIFTH AND SIXTH LONG-RANGE CONCEPT PLANS: 1971

Debate swirled around the NCS's future role and structure, as General Klocko resumed work on the annual NCS long-range concept plans. While the NCS never published the fifth plan, the agency did forward its sixth (and final) long-range concept plan to the White House in July 1971. Although, Melvin Laird, Executive Agent, NCS, and General Klocko, Manager, NCS, rationalized a unified national communications system, the operating agencies were unable to reach an agreement for a unified system.

A second point of contention was the explosive growth of telecommunications technology, especially computer technology. By the early 1970s, computers instituted an era of rapid change, creating both major telecommunications system design opportunities and challenges for the NCS. The interaction between Automatic Data Processing and telecommunications network functionality also raised a host of regulatory and policy issues, introducing the Federal Communications Commission (FCC) as a major player in the evolution of Federal telecommunications systems and policies.

Not long after the NCS submitted the sixth long-range plan to the White House, the new NCS Manager, Air Force Lieutenant General Gordon T. Gould, Jr., began his own review of the NCS program. Instead of defending a single universal system, as his predecessors had done, General Gould concluded that “the concept of a single integrated NCS is unrealistic and further expenditure of effort aimed at that goal would be unwarranted.”²⁶

REVISED AGENDA: EARLY 1970S

Secretary Laird approved General Gould's conclusions, and in April 1972, wrote a letter to Mr. Whitehead informing him the NCS was discarding the concept of a universal single system and would concentrate “on the more modest but operationally worthwhile goal of interoperability — a lesser, but understood, level of integration.”²⁷ From that point, the Government would view the NCS as a confederation of

“From that point, the Government would view the NCS as a confederation of telecommunications networks, run by a consortium of Federal agencies.”

telecommunications networks, run by a consortium of Federal agencies. The NCS would achieve their goals through coordinated planning, interoperability, and system standardization in an evolutionary environment.²⁸ The agencies involved widely applauded this approach.

The NCS proceeded with its mandate from the 1963 Memorandum but no longer focused on creating a unified Government system. However, the OMNCS continued to focus on the structure and operational management of communications during emergencies, paying particular attention to E.O. 11490, *Assigning Emergency Preparedness Functions to Federal Departments and Agencies*,²⁹ October 1969, and related documents. The NCS concluded that President Nixon should amend E.O. 11490 to limit and integrate the roles of several agencies, including the NCS.³⁰ In a related move, Federal emergency plans gave the NCS operational management and planning responsibilities in other emergency communications areas, such as management and control of telecommunications resources of all Federal agencies in times of war, and preparation and planning for Presidentially declared domestic emergencies, such as natural disasters.

The NCS also became involved in the question of industry standards, particularly for interoperability and survivability. In August 1972, the Federal Standards Program administered by GSA assigned responsibility for the development and coordination of Federal Telecommunications Standards to the NCS. The purpose was to develop, coordinate, and issue the technical and procedural standards required to achieve operational compatibility among functionally similar telecommunications networks. The NCS urged the FCC to set industry standards relative to NS/EP requirements.

In addition, the NCS also sought to increase the cohesiveness and effectiveness of the Federal telecommunications community's participation in national and international standards development programs, including the Federal Information Processing Standards Program. Federal systems not only needed to be able to interoperate with each other, but also with State and local Government, the private sector, and foreign systems.³¹

General Gould pressed for a program for priority restoration of circuits, to ensure the availability of critical circuits in national emergencies, and the NCS developed the Restoration Priority Review Board to address this issue throughout the 1970s.

In this same period, the NCS also addressed the potential threat of the EMP phenomena to the communications infrastructure. In 1966, the second NCS long-range plan had identified EMP as a major threat to commercial carrier systems. In 1978, in response to this potential danger, and with advice from the Federal Telecommunications Standards Committee, Navy Vice Admiral Samuel L. Gravely, Jr., and the NCS Manager initiated an effort to develop Federal standards for protecting telecommunications facilities from EMP damage.

By the mid-1970s, the NCS had developed a significant body of knowledge on a wide range of telecommunications topics. In an effort to share this information, the OMNCS — in 1976 — began publishing and distributing annual NCS research reports.³²

MANAGEMENT CHANGES: 1978

The resignation of President Nixon in 1974 left the future of many White House programs, including the NCS, in uncertain positions as the new Administration of President Gerald R. Ford sought to establish and affirm its leadership role.

When President Nixon created the OTP in 1970, he tasked the office with relating its coordination and review of acquisition programs with the assigned responsibilities of DOD, GSA, and OMB. In 1973, OTP issued Circular 12, which outlined a coordination concept where various Government agencies would serve as lead agencies responsible for particular mission-oriented systems. OTP was responsible for reviewing progress and providing planning guidance to these lead agencies, including DOD.³³

In 1974, OTP concluded that this approach had not worked well because of continued confusion and overlap regarding the roles and functions of OTP, OMB, DOD, and GSA. The OTP proposed that a major realignment of the Administration's telecommunications responsibilities and an increase in its day-by-day involvement were required to resolve these conflicts. This view implied a broader charter, a larger budget, and a considerable increase in the size of the staff.³⁴

Yet, none of these implied changes were forthcoming. In 1977, the Carter Administration took office and launched its own analysis of communications management. President Jimmy Carter issued E.O. 12046, *Relating to the Transfer of Telecommunications Functions*, in March 1978, disbanding the OTP and transferring its functions, including those associated with the NCS, to the Executive agencies that had traditionally handled such matters. Under E.O. 12046, NCS activity transferred to the NSC, which assumed responsibility for the development of policies, plans, programs, standards for mobilization, and use of the Nation's telecommunications resources during emergencies. President Carter tasked the OSTP with implementing these functions under the NSC's policy guidance.³⁵

President Carter transferred other telecommunications functions previously managed by the OTP to a new office within the Department of Commerce — the Assistant Secretary for Communications and Information, from which evolved the National Telecommunications and Information Administration (NTIA). Under E.O. 12046,

the Secretary of Commerce served as President Carter's principal advisor on telecommunications policy and regulation. OMB retained its powerful role of budget oversight and served as President Carter's principal advisor on procurement and management of Federal telecommunications systems, including the NCS.³⁶

NEW STRATEGIC THREAT: LATE 1970s

In 1978, new intelligence pointed to the rapid growth of the Soviet nuclear threat, particularly the number and accuracy of Soviet intermediate- and long-range nuclear warhead ballistic missiles. This discovery prompted the President's National Security Advisor Dr. Zbigniew Brzezinski to seek "leadership protection" through improved command and control communications — a call reminiscent of President Kennedy's order 15 years earlier. The National Security Advisor also expressed concern about the impacts of deregulation and the possible divestiture of AT&T, the Nation's major telecommunications carrier, on survivable and restorable telecommunications networks as emergency services were provided to the Government under an exclusive agreement with the AT&T Long Lines Department.³⁷

"[President Carter] directed the NCS to place 'substantial reliance' on the private sector for advice and assistance."

Echoing White House concerns about the possible AT&T divestiture, the NCS recommended that President Carter issue a national policy statement on the importance of national security telecommunications with the intent to increase the survivability of the commercial networks that serve national security interests by influencing the way that

private telecommunications service providers constructed their networks and systems. To this end, the NCS urged the FCC to use its regulatory powers to take an active, aggressive role to promote national security telecommunications.

With national security telecommunications high on the Nation's agenda, in May 1978, the NSC, the OSTP, and the NCS Executive Agent (now Defense Secretary Harold Brown), joined to issue a lengthy Memorandum of Understanding, which delineated the Executive Agent's responsibilities in national security telecommunications; developing and coordinating plans, programs, and standards for the mobilization and use of the Nation's telecommunications resources in any emergency.³⁸

President Carter also took action on telecommunications policy during this time. In November 1979, he issued Presidential Directive 53, which called for the creation of a communications facility adequate 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."³⁹ He directed the NCS to place "substantial reliance" on the private sector for advice and assistance.⁴⁰

Soviet Nuclear Missile in the Red Square - The growth of the Soviet nuclear threat resulted in an increased focus on national security telecommunications.



Although uncertainty remained about who was responsible for implementing this new national security telecommunications policy, the NCS, with the backing of the NSC, soon emerged as the key coordinating organization. An NSC Steering Group, formed to coordinate implementation of the new policy guidance, tasked the NCS to prepare and direct the implementation of a National Security Telecommunications Policy Implementation Concept Plan. By the summer of 1980, the Steering Group drafted and approved a planning approach and directed the NCS to prepare a final strategic plan for implementing the new national security telecommunications policy.

Coordinating the technical, regulatory, and policy aspects of the Concept Plan with Federal agencies and commercial carriers proved a considerable challenge for Army Lieutenant General William J. Hilsman who succeeded Admiral Gravely as the new NCS Manager. Although the NSC urged General Hilsman to assume executive branch leadership, he realized he needed a direct mandate to do so. The President had not named the Manager or any other organizational head to take charge of system implementation. Secretary Brown noted in a Memorandum to the NSC, “Some Government organizations do not recognize or accept the role of the NCS,”⁴¹ as implied in the President’s instructions, and it might be appropriate to announce to the community that General Hilsman as the Manager, NCS, is fully responsible for coordinating the implementation of the national security telecommunications policy within the Federal Government.⁴²

The Steering Group, however, turned to more immediate problems confronting the development of a national security telecommunications capability: the economic and structural changes taking place in the telecommunications industry.

Until the late 1970s, Government networks and AT&T’s Bell System, the latter functioning de facto as the Government’s system manager, supplied emergency communications for the President and key civilian and military officials. However, the Department of Justice’s (DOJ) 1974 lawsuit seeking the breakup of the Bell System, which resulted in an increasing number of telecommunications service providers, jeopardized this long-range and well-defined relationship. In the fall of 1980, the NSC anticipated the end of the singular arrangement with AT&T and tasked the Executive Agent to review the Federal Government’s dependence on commercial carriers.⁴³

In December 1980, a month before President Carter left office, General Hilsman briefed the Steering Group on the Executive Agent’s findings, confirming what was already widely known: the Government had developed an overwhelming reliance on common and specialized carriers, and these carriers were vulnerable to a wide range of disruptions. To develop solutions to address this concern, the NCS member agencies’ representatives grouped issues for study under three headings: technical, managerial, and national communications policy. The technical initiatives, under this study, focused on system survivability and interoperability. The managerial initiatives emphasized the need for a Government focal point for national telecommunications security and for joint industry-Government planning. Lastly, the policy initiatives stressed the importance of communications legislation pending before Congress.

Collectively, these initiatives became the building blocks for the national security telecommunications enhancement program of the 1980s. A few weeks after his inauguration, President Ronald Reagan pledged to fulfill President Carter’s national security telecommunications objectives and to strive for practical results for the communications network as soon as possible.

Part 2

**REDEFINING THE
AGENDA**

Part 2

Redefining the Agenda

The momentum toward major improvements in national security telecommunications accelerated rapidly in the 1980s with the Reagan Administration. The new Administration was forced to respond to trends complicating the national security and economic environment. These trends included:

- The proliferation of Government-owned and Government-leased networks with apparently little regard for interoperability;
- The fast pace of technological change bringing new opportunities for system improvements;
- The increasing numbers of industry players created by divestiture and deregulation; and
- The resurgent role of Congress, the courts, and the regulatory agencies in orchestrating a new economic and legal setting for telecommunications.

To address these challenges, the Government moved to consider telecommunications for both wartime and domestic emergencies as one entity, referred to as NS/EP telecommunications.⁴⁴ This concept led to a new agenda for the NCS.

In January 1981, the Reagan Administration reaffirmed E.O. 12046, the executive order that disbanded the OTP and transferred telecommunications authorities and responsibilities to the White House and other Federal agencies. President Reagan then increased the number of organizations involved with NS/EP telecommunications planning. In December 1981, the White House created the Emergency Mobilization Preparedness Board to devise plans for harnessing the Nation's mobilization potential.⁴⁵ William E. Clark, the President's National Security Advisor chaired the board, composed of representatives from more than 20 Federal departments and agencies.

GROWING NATIONAL SECURITY TELECOMMUNICATIONS INITIATIVES

National security telecommunications initiatives became a priority in 1982 as the NCS sought to carry out the NSC mandate to provide "telecommunications facilities adequate to satisfy the needs of the Nation during and after any national emergency." To strengthen the working relationship between the NCS and other agencies, the NSC Steering Group, formed in 1978, quickly established a working group. The steering group tasked this subordinate organization to research and define issues before they were brought to the steering group. Issues would be organized into three categories for deliberation: survivability and interoperability, management, and policy.

There were six programs for survivability and interoperability:

- In June 1982, the NCS undertook work on a commercial satellite survivability initiative;
- The working group defined six technical tasks in a common and specialized carrier transmission systems initiative to identify survivability and durability enhancements that could be built into the common and specialized carrier transmission systems;
- The NCS also began work on a second contract in 1982 to undertake network design and engineering studies on class 4/5 switches to determine how to route essential telephone traffic through the Public Switched Network (PSN) when large portions of the PSN's hierarchical routing structure had been damaged or destroyed;
- Following approval by the DOD to permit a limited flow of FTS traffic into and out of the Automatic Voice Network (AUTOVON), the Defense Commercial Communications Office issued a contract in December 1982 to implement the AUTOVON/FTS interconnect initiative, with an initial operational capability scheduled for September 1983;
- The group worked to develop a national emergency amateur radio operations plan: In June 1982, the NSC Steering Group approved the NCS recommendation to develop the largely untapped resource of the Nation's 400,000 or more amateur radio operators. The steering group established close coordination with the American Radio Relay League and the Military Affiliate Radio System for a national emergency amateur radio operations plan; and
- The working group also initiated studies surrounding the EMP phenomena.

In addition, the Steering Group studied several management initiatives, including the creation of a joint industry/Government planning body to address the changes taking place in the telecommunications industry and to bridge the growing gap between industry and Government.

ESTABLISHMENT OF THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE: 1982

President Reagan's establishment of the President's National Security Telecommunications Advisory Committee (NSTAC) in 1982 met the need for an industry/Government body. In 1978, the White House sought to insulate itself from changes within the telecommunications industry by encouraging the FCC to use its regulatory powers to influence the design of the growing number of U.S. commercial carrier systems. The White House had also instructed the Manager, NCS, to become involved with the host of new private-sector telecommunications providers and seek their advice and assistance in achieving national security goals.

In 1978, General Paschall, Manager, NCS voiced his opposition to the DOJ's 1974 antitrust lawsuit against AT&T, which he stated was as an attempt "to fragment the integrated national aspects of the Nation's telecommunications networks." When the DOJ issued the Modification of Final Judgment, divesting the Bell Companies from AT&T, in January 1982, General Hilsman moved quickly to establish a new industry/Government relationship with not only AT&T, but also the many new service and equipment providers and information-processing companies. In March 1982, he initiated the first of two national security telecommunications conferences, inviting the chief executive officers of 30 telecommunications and information processing companies. General Hilsman then followed the second conference in July 1982, with a series of industry/Government working group meetings that identified three major issues for attention: commercial satellite survivability, joint network planning, and Automated Information Processing (AIP) survivability.

Meanwhile, the OMNCS provided staff support to the NCS Executive Agent, Defense Secretary Caspar W. Weinberger, in his efforts to obtain NS/EP legislation from Congress. Testifying before congressional hearings in 1982 on the impact of the AT&T antitrust lawsuit on NS/EP telecommunications capabilities, General Hilsman suggested four NS/EP legislative initiatives: (1) pervasive recognition in the law of the critical importance of the communications industry to NS/EP; (2) legislative safeguards for all telecommunications carriers engaging in joint network planning and management; (3) statutory permission for any telecommunications carrier to provide an end-to-end service during times of emergency; and (4) assurances from Congress that provisions of the law could be implemented in an industry environment free from conflicting regulatory initiatives or jurisdictional conflicts.

While Congress did not act on General Hilsman’s suggestions, the conferences and meetings organized by General Hilsman ultimately led to the issuance of E.O. 12382, *President’s National Security Telecommunications Advisory Committee*, signed by President Reagan on September 13, 1982, establishing the NSTAC.⁴⁶ Composed of a maximum of 30 industry leaders, E.O. 12382 tasked the NSTAC to bring the President and the NCS Executive Agent the knowledge, expertise, and insight of the telecommunications industry on issues of national security telecommunications policy. Moving quickly into its new responsibilities, the NSTAC created the Industry Executive Subcommittee (IES) as its subordinate working body to prepare and draft NSTAC recommendations to the President.

ESTABLISHMENT OF THE EMERGENCY COMMUNICATIONS WORKING GROUP: 1982

Concurrently, the President also formed the Emergency Communications Working Group (ECWG) in 1982, appointing the NCS Manager as the ECWG chair, with the NTIA Administrator appointed vice chair. The NCS, via the NSTAC and ECWG, became the Reagan Administration’s initial focal points for developing NS/EP telecommunications policy.

AT&T Divestiture

The January 1982 judgment ordering the breakup of the Bell System changed the telecommunications industry forever. Since 1914, AT&T had effectively maintained a monopoly over the telephone market and had grown to be one of the world’s largest corporations, providing the most efficient and modern telephone system in the world. Furthermore, during this time, AT&T developed a strong relationship with the Government, supplying emergency telecommunications and functioning as the *de facto* Government telecommunications system manager.

As AT&T’s dominance grew, both small entrepreneurs and the Federal Communications

Commission challenged the corporation in an effort to bring an end to the monopoly and pave the way for other service providers and equipment manufacturers. These concerns culminated in 1974, when the Department of Justice filed a suit against AT&T, charging it with the monopoly of various telecommunications services. The trials and negotiations related to the AT&T suit stretched 8 years and resulted in the breakup of the Bell System.

The divestiture not only set the foundation for the development of a competitive telecommunications market but also brought an end to the Government-AT&T relationship and raised concerns regarding the impact of the break-up on

national security and emergency preparedness (NS/EP) initiatives. The NCS and industry leaders recognized the need for a mechanism to coordinate industry/Government planning for NS/EP communications among the growing number of telecommunications providers and manufacturers. In September 1982, President Reagan established the President’s National Security Telecommunications Advisory Committee as the new coordinating body between industry and Government. Over 20 years later, this body continues to function as a model of industry/Government partnership.

The Emergency Mobilization Preparedness Board tasked the ECWG with preparing plans for communications in times of national emergencies. The result was the Communications National Plan of Action with eight implementation measures and 33 milestones. At the request of General Hilsman, ECWG also made an early attempt to look at the challenges arising from society's dependence on AIP and the merging of telecommunications and information-processing technologies.

Despite the relevance of the subject matter, both ECWG and its research program came under increased scrutiny. Opposition to ECWG grew in the executive branch. In early 1983, reports began to circulate that the Reagan Administration was revising President Carter's telecommunications policy statement to give the NCS a greater role in NS/EP telecommunications. The White House confirmed these reports in late 1983, when President Reagan issued new policy guidance that further consolidated the NCS's primacy as the Government focal point for NS/EP telecommunications activities.⁴⁷ In the next months, the NSC established a new telecommunications policy steering group, expanded the NCS membership to 22 members, and instructed the NCS to assume the functions of ECWG.⁴⁸

NEW POLICY ON NATIONAL SECURITY TELECOMMUNICATIONS

Under the President's new policy guidance, the Manager, NCS, was instructed to coordinate the development of plans for unrestricted access to the Nation's domestic communications resources in support of NS/EP telecommunications requirements. The President also invited his NSTAC to provide him and the Executive Agent with advice and information. Finally, President Reagan instructed all Federal Government departments and agencies to incorporate the provisions of the new policy on national security telecommunications when modifying their current communications facilities, systems, or networks, or when planning new capabilities.

The President's National Security Telecommunications Advisory Committee

The President's National Security Telecommunications Advisory Committee (NSTAC) provides the President with high-level industry-based advice and recommendations on a wide range of policy and technical issues related to telecommunications, information systems, information assurance, infrastructure protection, and other national security and emergency preparedness (NS/EP) matters.

The NSTAC has a solid tradition of turning ideas into action. At the end of every cycle, the NSTAC issues reports that include specific recommendations for the President. For example, the National Coordinating Center for

Telecommunications, an industry/Government coordination center for day-to-day operational support to NS/EP telecommunications, began as an NSTAC recommendation. Another program initiated through NSTAC is the Network Security Information Exchanges (NSIE), which meets regularly with a Government NSIE to address possible remedies to the potential exploitation of system vulnerabilities. The NSTAC also recommended the establishment of priority service programs for NS/EP users — the Telecommunications Service Priority program and the Wireless Priority Service (WPS) program.

Some of the more recent issues addressed by NSTAC include network vulnerabilities, wireless communications, information sharing, and trusted access to telecommunications facilities. Specifically, recent task force reports made recommendations on WPS, vulnerabilities in pervasive software/protocols, physical and wireless security, and Internet peering points. In keeping with its timeliness, many of the NSTAC's reports focused on how it can best assist the President in the post-September 11 world — marked by increasing cyber and physical threats to our Nation's critical infrastructures.

By the end of 1983, the Reagan Administration created an organizational structure that provided the Nation with an improved NS/EP telecommunications capability, focusing on the Manager, NCS, and the NSTAC. The next step was to codify this arrangement with the Federal Government. In view of the NCS's multi-agency responsibilities, it was no surprise that the organization received the task to draft a new executive order to sort and assign NS/EP telecommunications roles and responsibilities throughout the Federal establishment.

E.O. 12472 AND ASSIGNMENT OF NATIONAL SECURITY TELECOMMUNICATIONS AND EMERGENCY PREPAREDNESS FUNCTIONS: 1984

The NCS underwent a fundamental change on April 3, 1984, when President Reagan signed E.O. 12472, *Assignment of National Security Telecommunications and Emergency Preparedness Functions*.⁴⁹ E.O. 12472 superseded the August 1963 Presidential Memorandum that established the NCS⁵⁰ and outlined an organizational structure and technical path for creating an NS/EP telecommunications capability. As in the 1963 Memorandum, the purpose of the NCS was to serve the Federal Government under all conditions: crisis or emergency, attack, recovery, and reconstitution. However, in contrast to previous NCS policies and documents on telecommunications responsibilities, E.O. 12472 focused exclusively on NS/EP telecommunications. Under the order, the NCS would seek to use commercial, Government, and privately owned telecommunications resources in support of national leadership and continuity of Government for NS/EP purposes.

The executive order revitalized the structure of the NCS as an interagency organization and focal point for joint planning by industry and Government for NS/EP telecommunications. Although the central thrust of the NCS's mission continues to evolve, the responsibilities and organizational structure drawn by E.O. 12472 are in place today in an organization that successfully bridges the often-tumultuous relationship between private industry and Government.

The President's National Security Telecommunications Advisory Committee membership as of September 2003.



NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS: 1984

At the recommendation of the NSTAC, President Reagan established the National Coordinating Center for Telecommunications (NCC) to further facilitate NS/EP collaboration between industry and Government. During its early years, the NSTAC focused its efforts on concerns over the Government's growing reliance on commercial telecommunications services. As the telecommunications network continued to evolve, however, NS/EP communications planning and response also became increasingly complex and critically dependent on information infrastructures, demanding an innovative means of protecting the Nation's public and private communications assets.



In 1982, the NSTAC's first recommendation to the President was to create the NCC. E.O. 12472 provided the need for an organization such as the NCC to address the Nation's telecommunications preparedness. An industry/Government organization at the operational level, the NCC was established to assist in initiating, coordinating, restoring, and reconstituting NS/EP telecommunications services or facilities under all conditions of crisis or emergency or following physical and cyber incidents.

The NCC was established to provide a unique forum for industry and Government representatives to work together daily, as opposed to NSTAC's periodic and issue-related meetings. Additionally, the NCC was designed to operate as an emergency telecommunications coordination center during any emergency or crisis and provides an all-hazard telecommunications response capability. When it receives notification of critical Federal Government requirements, the NCC staff contacts its industry and Government representatives, and develops a coordinated, mutual response.

NCC member companies handle ninety-five percent of Government communications. However, other non-resident member companies provide representatives when needed and attend organizational meetings. Industry representatives at the NCC have both day-to-day and emergency operations roles. The industry leaders — AT&T, BellSouth, Qwest, SBC, Sprint, Verizon, and MCI — are all resident members.

In addition to OMNCS staff, many NCS organizations provide full time personnel to support the NCC; the NCC Manager also maintains a list of points of contacts for all NCS member organizations. The DOS, DOD, DOE, Department of Transportation, GSA, and the Federal Reserve Board currently provide Government detailees to the NCC.

Executive Order 12472

In 1984, President Reagan issued Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which greatly broadened the responsibilities and capabilities of the National Communications Systems (NCS). With the issuance of this Executive Order, the NCS mission expanded to include assisting the President, National Security Council, Office of Science and Technology Policy, and Office of Management and

Budget in exercising certain telecommunications functions and responsibilities as well as in serving as the focal point for industry/Government telecommunications planning. The NCS also assumed responsibility for directing and coordinating emergency telecommunications services if the President has to declare his emergency war power authority. Additionally, the order authorized creation of the Committee of Principals, a body

comprising Federal departments and agencies that have telecommunications facilities of significance to national security and emergency preparedness. In February 2003, E.O. 13286 designated the Secretary of Homeland Security as the NCS Executive Agent. E.O. 13286 also added the White House Homeland Security Council to the list of agencies advised by the NCS.

EXPANDING NATIONAL COMMUNICATIONS SYSTEM FUNCTIONS

The formation of the NSTAC and the NCC helped to shape an environment of industry and Government collaboration that would make possible the realization of E.O. 12472. Under that mandate, the Secretary of Defense remained the NCS Executive Agent to promote unified planning and operations among NCS member organizations. In consultation with Government agency leaders, the President tasked the Executive Agent to recommend the assignment of tasks and activities to NCS members to the NSC, the OSTP Director, and the OMB Director. In addition, the President tasked the Executive Agent with providing staff support and technical assistance to the NSTAC. These responsibilities would be accomplished primarily through the Manager, NCS, who was responsible for recommending an evolutionary telecommunications architecture and preparing plans and procedures for a circuit priority restoration system.

“The NCS felt they could accomplish these objectives in an environment marked by rapid changes in the U.S. telecommunications industry, accelerated growth of new technologies and services, and dramatic changes in the strategic threat to the United States.”

By 1984, the NCS mission was to provide the President and the Federal Government with NS/EP telecommunications services, primarily leased from commercial carriers — not to build a standalone system in which the Government would own some facilities and equipment. At the same

time, the NCS was to implement effective management controls for coordinating, and possibly directing, the operation and use of emergency telecommunications services when the President invokes emergency war powers functions under the provisions of Section 706 of the Communications Act of 1934.

To achieve these advancements, the NCS took three approaches:

- Influenced the adoption of standards supportive of NS/EP telecommunications requirements;
- Encouraged PSN providers to incorporate particular technology features into their systems for NS/EP telecommunications; and
- Programmed, implemented, and funded NS/EP-oriented improvements in the PSN that the carriers otherwise would not adopt.

The NCS felt they could accomplish these objectives in an environment marked by rapid changes in the U.S. telecommunications industry, accelerated growth of new technologies and services, and dramatic changes in the strategic threat to the United States.

THE COMMITTEE OF PRINCIPALS AND COUNCIL OF REPRESENTATIVES

The mission mandated by E.O. 12472 not only required the collaboration of industry and Government but also encourage cross-agency collaboration within the Government, especially given the NCS’s structure as a multi-agency body. In 1964, the NCS roster of operating agencies and assets listed 11 operating agencies (up from six in 1963) and 31 communications systems assets. Successive long-range plans in the 1960s added new assets and deleted others. However, after 1970, the NCS temporarily discarded the practice of identifying agency communications assets, and it was not until the reorganization of Federal telecommunications activities in 1978 that it resumed identifying assets.

E.O. 12472 opened the way for the formation of two bodies that were meant to act as the mechanism for inter-agency collaboration. The concept was not new. In the 1970s, General Gould met with agency principals and representatives to outline views on how the NCS should function under the new OTP.

Prior to those meetings, the NCS functioned as a responsibility of the DOD, with the Manager, NCS (who was also the Director of the DCA) interfacing with the operating agencies only when the occasion required. With the replacement of the single integrated communications system concept by the consortium approach, General Gould saw the need to strengthen a collective position in which the principals and representatives could help shape the agenda for the NCS in the 1970s and beyond. Each member department and agency of the NCS was to provide a Principal member and a delegate representative to sit on two interagency advisory bodies. It was General Gould's view that the NCS operating agency principals and representatives should provide leadership to defining a new concept and addressing a host of important telecommunications issues, including standards, communications satellites, computers, and digital communications. The Manager also noted the increasing Congressional attention to telecommunications and the need for the principals and representatives, as well as the Manager, to monitor and provide inputs to Congressional deliberations.⁵¹

In 1978, Air Force Lieutenant General Lee M. Paschall, General Gould's replacement as the NCS Manager, reaffirmed the role of these two informal bodies by chairing periodic meetings of the principals to gather their advice. The NCS Deputy Manager also began meeting regularly with the NCS representatives.⁵² By 1982, according to General Hilsman, the NCS operating agency members were playing "a predominant role in the formulation of telecommunications policy and the solution of mutual problems."⁵³ However, it was not until 1984 that the principals and representatives, as organizational bodies, became official entities of the NCS organizational structure.

In response to E.O. 12472, the NCS officially formed the Committee of Principals (COP), with the Council of Representative (COR) as its subordinate organization. The NCS established the COP as a forum, which meets semi-annually for members to review, evaluate, and present views and recommendations on current or prospective NCS programs to the Manager, the Executive Agent, and the White House. The OMNCS provides staff support for the COP, COR, and their subgroups. Prior to COP meetings, the COR meets to consider relevant initiatives for consideration by the principals. The COP may task the COR to study and report on specific issues. The COP, in turn, is to recommend which reports it will forward to the E.O.P. for further deliberation and action.

The Committee of Principals and Council of Representatives

The Committee of Principals (COP) is a Presidentially designated interagency group established to provide advice and recommendations on national security and emergency preparedness (NS/EP) telecommunications matters to the President. The Council of Representatives (COR) is the subordinate body of the COP. The COP is comprised of high-level Government officials representing 23 Federal departments and agencies across Government with operational, policy, regulatory, economic, and law enforcement responsibilities. As an interagency group, the COP serves as a forum for

members to review, evaluate, and present views on current or prospective national policies and to recommend relevant action or programs to the Manager, NCS, the Executive Agent (the Secretary of Homeland Security), and the Executive Office of the President (EOP).

In the new homeland security environment, information sharing and interagency coordination are essential in ensuring Government's ability to prevent and respond to an attack. The COP has embraced the goals of homeland security and is dedicated to fostering close interagency relationships and

providing the President with timely advice on NS/EP telecommunications matters. The activities of the COP include examining how diverse and redundant telecommunications facilities can improve the reliability of NS/EP communications services for Government users and evaluating telecommunications priority services programs. Through its activities, the COP demonstrates a commitment to ensuring that telecommunications services will be available to the Government and that the various Government agencies can communicate with each other, in the event of an attack.

CRITICAL BEGINNINGS

Building on its strong relationship with both industry and Government agencies, during the mid-1980s, the NCS began work on several initiatives that would prove significant in coming years. Focusing on establishing programs that furthered the effort to ensure essential NS/EP telecommunications, the NCS developed: (1) the Network Design and Analysis Capability (NDAC) as a process to analyze the ability of the Nation's telecommunications resources to meet NS/EP requirements; (2) the National Level NS/EP Telecommunications Program (NLP) as an initiative dedicated to developing a single telecommunications nuclear response and recovery plan; (3) the Telecommunications Service Priority (TSP) Program to ensure priority telecommunications service to Federal, State, and local Governments and private users in the event of a nuclear attack or other emergency; and (4) the Shared Resources-High Frequency Radio Program (SHARES-HF) as a single interagency high frequency radio program to relay critical NS/EP messages in the event of an emergency.

NETWORK DESIGN AND ANALYSIS CAPABILITY: 1984

As directed by E.O. 12472, the NCS developed the Network Design and Analysis Capability (NDAC) to analyze the ability of current U.S. telecommunications networks to meet NS/EP requirements and evaluate the need for additional capabilities. Furthermore, the NCS designed the NDAC to enable the NCS to study potential natural and manmade disruptions to the PSN, analyze interdependencies, develop models and methodologies to identify vulnerabilities and congestion, and identify solutions for network effectiveness. Engineers also designed the NDAC to predict and help mitigate network damage caused by accident or attack. Through the NDAC, the OMNCS was equipped to review the operation of the PSN, including the Public Switched Telephone Network (PSTN), Internet Protocol (IP) networks, Internet telephony, and next-generation packet switched IP networks, under various conditions. Still in use today, the NDAC is comprised of software tools, models, and telecommunications databases used to assess network performance, perform modeling and simulation, and visualize network topologies. Core to NCS network performance analysis, the NDAC has been continually refined and expanded through software updates and development of more powerful application modules.

The NDAC's extensive network modeling and simulation capabilities include analytical models and methods for discrete event and continuous simulation. An integral component of the NDAC is the OMNCS Telecommunications Resource Database, which is the most comprehensive and current description of the U.S. communications infrastructure and the source for its many offerings and capabilities. With NDAC modeling tools and its own resource database, OMNCS network performance modeling services include:

- Analyzing the effects of traffic congestion in both wireline and wireless telecommunications networks;
- Evaluating the vulnerability, survivability, and reliability of networks during local and regional outages or emergencies;
- Evaluating the trade-offs and performance benefits of alternative deployable technologies before implementation; and
- Integrating user requirements into network designs to optimize system-wide capacity.

THE NATIONAL LEVEL PROGRAM: 1986

In an effort to further advance its programs and activities dedicated to telecommunications NS/EP, the NCS developed the National Level Program (NLP) during the height of the Cold War as a single initiative encompassing the development and implementation of several programs, to formulate a comprehensive telecommunications nuclear response and recovery plan. The NLP was to include national level programs, conducted within the NCS structure, that require significant Government resources for their pre-implementation, implementation, and recurring costs. These programs would ensure the provision of NS/EP telecommunications for the Federal Government during a nuclear war. In addition, the NLP would provide enhanced communications features in the peacetime and crisis/mobilization time periods. In 1986, the White House approved funding for the first NLP, marking a milestone in the NCS mission to develop an NS/EP telecommunications capability. In the NLP, the NCS projected the evolution of capabilities that enhanced the routing, survivability, connectivity, and interoperability of the PSN. The component programs of the NLP, during the mid-1980s, were the Commercial Network Survivability (CNS), Commercial Satellite Communications (SATCOM) Interconnectivity (CSI), and the Nationwide Emergency Telecommunications Service (NETS).

The CNS and CSI programs focused on reconstituting the commercial carrier networks, especially reconnecting islands of isolated users and long-distance switches by maximizing the features of survivability and interoperability of the commercial carriers.⁵⁴ Specifically, the NCS designed the CSI program to provide communications via commercial satellite connectivity between isolated enclaves of the PSN in a

The Network Design and Analysis Capability

Since concept inception in 1985, the Network Design and Analysis Capability (NDAC) has supported the telecommunications network analysis needs of the United States Government. On the basis of data received from its private sector partnerships, the NDAC built a nationwide and current map of the public switched network (PSN). Using this map, the NDAC undertakes extensive network modeling and simulation capabilities, such as baseline, vulnerability, impact, and interdependency analyses.

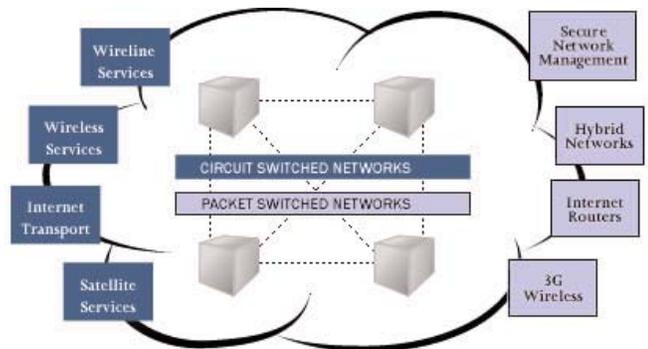
Baseline analyses characterize the telecommunications infrastructure by depicting its assets so that decision-makers and emergency responders can determine which assets are important for continuous availability of telecommunications service.

Through vulnerability analyses, decision-makers gain information about interdependencies and weaknesses that offer the potential for exploitation by adversaries. Impact analyses depict how vulnerabilities in the telecommunications infrastructure will degrade the security and reliability of the network. Studying the effect of weapons of mass destruction on the PSN is an example of an impact analysis.

Lastly, technicians conduct interdependency analyses to examine how a critical infrastructure depends on another infrastructure for its operations. For

example, an interdependency analysis may examine to what extent a denial of service in the telecommunication infrastructure may damage the financial services infrastructure.

The NDAC has a wide scope of capabilities as depicted in the diagram.



Current capabilities analyze voice, switching, and long haul transmission

Future capabilities will expand to model the integrated information services planned for the next generation

post-nuclear attack environment.⁵⁵ The NCS developed the CNS program to enhance the short-haul connectivity of commercial and Government telecommunications networks in support of NS/EP telecommunications needs. Throughout the Cold War era, these programs remained integral parts of the NLP and were continuously updated to incorporate the most recent switching, satellite, and software technologies. However, as the NS/EP telecommunications environment changed in the post-Cold War era, the NCS eventually terminated these programs.

Although engineers originally designed the NETS program to re-establish nationwide communications in the event of a nuclear war, the NETS program (now known as the Government Emergency Telecommunications System (GETS)) evolved in the post-Cold War era and became the centerpiece of the NLP.⁵⁶ The NETS concept first originated in the late 1970s with requirements for improving telecommunications capabilities serving the Federal Government during emergencies. In the fall 1980, an AT&T study of class 4/5 switches, which provide local direct telephone service for most end users, concluded that the switches had a relatively high probability of surviving a nuclear conflict. It was technically feasible and desirable to build a nationwide network of class 4/5 switches that could survive nuclear attack. Drawing on this conclusion, an NCS follow-on network engineering study sought to determine how telecommunications could route essential telephone traffic through the PSN when large portions of the upper hierarchical routing structure (above the class 4/5 level) had been destroyed or damaged. By August 1981, the NCS study evolved into the NETS Program. The NCS issued its first NETS Program Plan on November 30, 1982, and projected an initial operating capability for July 1987, and a final operating capability one year later. The NETS Program received new impetus with E.O. 12472 and the revised funding formula of 1985.

As the NETS Program approached implementation, COP members became increasingly uneasy about the availability of emergency power to support the PSN. In August 1986, the OMB responded to this concern by asking Air Force Lieutenant General Winston D. Powers to review the program in his role as the NCS Manager. General Powers requested that the National Research Council (NRC) of the National Academy of Sciences prepare an in-depth review of the program's potential vulnerabilities and technical longevity and to review alternative technical approaches. The NRC concluded that the NLP was on the correct path and was employing a technically viable approach for ensuring essential NS/EP telecommunications, despite vulnerabilities such as the need for long-duration backup power and refueling and for greater availability of trained telecommunications personnel.⁵⁷

Following this report, the NETS Program continued to expand, adding new local and inter-exchange carriers and increasing its possible users from 4,000 to nearly 25,000. By the end of the 1980s, NETS was rapidly

approaching the implementation phase, yet, concern lingered. A COP subcommittee established to review the NLP — including the threat, user requirements, program risks, technology alternatives, and cost components — concluded that based on the power vulnerability of PSN, the NETS Program did not adequately meet requirements, and consequently, the COP declined to recommend the NLP for White House approval.⁵⁸

In response to the concerns raised by the COP and others, the OMB directed the Manager, NCS, to delay implementing the NETS Program for two years and to restructure the NLP to address the following issues: enduring electric power, technical alternatives, cost savings, and the strategic impact of the Soviet Union's breakup.

The TSP program was critical in the aftermath of the September 11, 2001, terrorist attacks, particularly in the restoration of Wall Street on September 17, 2001. Photos courtesy of Verizon



Army Lieutenant General Thurman D. Rodgers, Manager, NCS, appointed a panel of experts to further review the NLP. The panel issued a recommendation in October 1991 to replace the NLP with a PSN-based technical approach to take full advantage of carrier-funded improvements for substantial cost savings to the Government.⁵⁹ Although the White House endorsed the NLP's restructuring, in October 1991, the President's National Security Advisor, Brent Scowcroft, issued a memorandum reminding the NCS community of the policy guidance and functional requirements governing the development of an NS/EP telecommunications capability. In the memorandum, Scowcroft stated that E.O. 12472, remained the primary policy guidance, while President Reagan's E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, of November 18, 1988, was primary guidance on the functional responsibilities for NS/EP Federal departments and agencies.

General Scowcroft also emphasized the functional requirements integral to NCS plans:

(1) voice-band service in support of Presidential communications; (2) interoperability with resources of selected Government or private facilities or networks through the application of standards; (3) survivability and endurance in the interconnection of surviving users; (4) international interface for access to and egress from international service; (5) nationwide coverage supporting the national security leadership; and (6) interagency emergency operations providing priority services for NS/EP traffic.⁶⁰ Although the NCS never fully implemented NETS, the program provided the necessary groundwork for the evolution of future NCS programs and the structure envisioned by the NLP built the foundation upon which the NCS now coordinates with its member organizations.

TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM: 1988

In December 1984, the NSTAC recognized the pressing need for a system to provide priority provisioning and restoration of NS/EP services for Governments as well as private users. In February 1985, the NSTAC's IES formed the Telecommunications Service Priority Program (TSP) Task Force to assist the OMNCS in forming the TSP system. For more than five years, the TSP Task Force worked with a COR subcommittee to address the provisioning of new or changed service, restoration of existing service, and the maintenance, legal, and regulatory issues associated with priority treatment.

As a result of the successful collaboration between the NSTAC and the COR, the FCC passed a Report and Order (R&O) on November 17, 1988, officially establishing the TSP Program. The R&O represented a new approach to assigning priorities and served as the regulatory, administrative, and operational framework for priority provisioning and restoration. The FCC also authorized and required service vendors to provision and restore services with TSP assignments before restoring services without such assignments.

In March 1990, the NCS formed the TSP Oversight Committee (OC) of 17 members from industry and Federal and State Governments appointed by General John Myers, Manager, NCS. During its first year, the TSP OC focused on State and local implementation, and on September 10, 1990, the TSP System achieved initial operating capabilities, just in time to support Desert Storm Operations in the Persian Gulf. The program did not become fully operational, however, until March 1993.

SHARED RESOURCES-HIGH FREQUENCY RADIO PROGRAM: 1989

Approved by the Executive Office in January 1989 under the mandate of E.O. 12472, Shared Resources-High Frequency Radio Program (SHARES-HF) is a single interagency system for emergency message handling that brings together the HF radio resources of Federal, State, and industry organizations, when circumstances either destroy or prevent normal communications for the transmission of NS/EP information.

SHARES was developed as a forum for the Federal Government community to address issues affecting HF radio interoperability. The SHARES-HF Interoperability Working Group (IWG), created as a permanent standing committee under the NCS COR, was designed to guide the SHARES radio network and for fostering interoperability of Federal HF radio systems through analysis of regulatory, procedural, and technical issues. The SHARES-HF IWG currently consists of 146 members, representing Federal, State, and industry entities.

The SHARES program, along with the other NCS programs and processes established during the 1980s, demonstrated the NCS's clear agenda to address NS/EP telecommunications matters. Specifically, the industry and Government relationships established during the 1980s helped pave the way to address new telecommunications challenges of the 1990s.

EXPANDING AGENDA

For the NCS, the late 1980s and early 1990s were times of expansion and reengineering of programs and policy. Radical new challenges posed by exploding advances in technology and worldwide political change required that the NCS adjust its role and the way it approached the provisioning of NS/EP telecommunications. No longer could the NCS, the NCC, and the NSTAC focus primarily on planning a response to a nuclear incident. Serious new risks to the Nation's telecommunications infrastructure were developing in addition to the nuclear threat. The NCS agenda expanded to respond to these new issues, increasingly emphasizing response to natural and manmade disasters, public events of significance, and localized conflicts.

The NCS also began to broaden its focus to include international telecommunications, as the economic, political, and technological effects of foreign providers on the U.S. NS/EP telecommunications demanded NCS reaction and adjustment. New technology pushed NCS planning into a world of software-based architectures that provided users with services and capabilities uniquely their own, while still residing within the PSN. From 1992 to 1997, the NCS underwent a change as dramatic as its restructuring under E.O. 12472.

GROWTH OF THE INTERNET

The Internet had as profound an impact on communications as any voice-based system. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is simultaneously a capability for worldwide broadcasting, a mechanism for information dissemination, and a medium for collaboration and interaction among individuals. Most importantly, it is

available without regard to geographic location. It has closely connected the world and irreversibly altered what we have come to expect of business, our future, and ourselves. In order to effectively address the growth of the Internet and its subsequent impact on NS/EP concerns related to the telecommunications networks, the NCS undertook several new activities including the implementation of new programs.

NETWORK SECURITY INFORMATION EXCHANGES: 1990

In April 1990, the Chairman of the NSC's Policy Coordinating Committee-National Security Telecommunications and Information Systems requested that the NCS

The SHARES Master Control Station—a transportable SHARES station that can provide emergency message handling from any location.



Manager identify what action should be taken by industry and Government to protect critical national security telecommunications from the “hacker” threat. In early 1990, General Myers requested the NSTAC provide industry’s perspective on network security issues. In response to the NSC tasking, the NCS and the NSTAC established separate, but closely coordinated, NSIE’s for both the industry and the Government. In May 1991, each NSIE finalized their charters and Government departments and agencies and NSTAC companies designated their NSIE representatives, chairmen, and vice-chairmen. Beginning with the first meeting in June 1991, the Government and NSTAC NSIEs have met jointly approximately every 2 months. The NSIEs function as a working forum on issues involving penetration or manipulation of software and databases, which affect NS/EP telecommunications. The NSIEs share information with these objectives:

- Learning more about intrusions into and vulnerabilities affecting the Public Network (PN);
- 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 network security recommendations to the President.

The Government NSIE members represent departments and agencies that are NS/EP telecommunications service users, part of the law enforcement community, or have information relating to network security threats and vulnerabilities. The NSTAC NSIE representatives include subject matter experts in prevention, detection, investigation of penetration of telecommunications software or professionals with security and investigative responsibilities. The NSTAC IES must approve the participation of NSTAC companies in the NSTAC NSIE.

The original NSIE charters envisioned a real-time operational response function; however, the NSTAC NSIE members eliminated the response function as it implied the NSIEs had authority over network response and recovery. Although individual representatives may have operational responsibilities within their own companies or Government departments and agencies, the NSIEs as organizations do not.

The priority for representatives to the NSIE is to first protect and maintain their own networks and then communicate with other NSIE representatives. Although NSIE representatives share their information at bi-monthly meetings, when events warrant a more rapid response, representatives communicate with each other ad hoc to rapidly contain, respond to, and recover from an incident and mitigate its impact. NSIE representatives have developed an informal accelerated information-sharing capability, and through the NSIE, Government gains industry points-of-contact who can confirm events, vulnerabilities, and mitigation strategies.

The NSIEs are a crucial component of the bridge between industry and Government. When the NSIEs were first established in 1991, Government advocated avoiding risk at whatever the cost to industry or Government. As industry and Government representatives began to interact more closely, Government developed an understanding of industry’s concerns.

Participation in the NSIE gives industry members a more comprehensive view of the environment in which they operate and access to the experiences of other companies in handling an incident or vulnerability or making security decisions. Participation in the NSIE, in turn, gives Government departments, agencies, and entities information on vulnerabilities and insights into how industry detects and responds to intrusions and incidents affecting the PSN-information the Government then uses to make its systems and networks more secure.

NATIONAL INFORMATION INFRASTRUCTURE: 1993

The Internet embodies the key underlying technical idea of open-architecture networking. In an open-architecture network, individual networks can be separately designed and developed, each with its own unique user interface and in accordance with its own specific environment and user requirements. In practical terms, the Internet is a medium through which these vastly different systems can connect to exchange information quickly and efficiently. This rapid unimpeded flow of information — not only over the Internet, but also over other interconnected computer and information systems — has generated a massive communications infrastructure.

The Internet, the various public, private, and proprietary networks, online services, computer support systems, and other emerging information technologies are collectively known as the National Information Infrastructure (NII).⁶¹ This infrastructure includes an ever-expanding range of equipment such as cameras, scanners, keyboards, telephones, facsimile (fax) machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers, and many other media.⁶²

By the early 1990s, the Government's dependence on the interconnection of information systems had become an important part of communications. When President William J. Clinton took office in 1993, he was already aware of the NII's potential to transform the lifestyle of ordinary citizens, change the way the country conducted business transactions, and deliver a variety of Government services. Recognizing that changes of this magnitude would raise important policy and technology issues, he created a framework for addressing these issues under the leadership of Secretary of Commerce Ron Brown. The Administration released *The National Information Infrastructure: An Agenda for Action* on September 15, 1993, to establish this framework and guide its components. The *Agenda for Action* sought to facilitate a partnership among business, labor, academia, the public, and Government to ensure the development of a coherent policy for the NII.

The Clinton Administration created the U.S. Advisory Council on the NII to represent the perspectives of the private sector, and chartered the Government's interagency Information Infrastructure Task Force (IITF) to articulate and coordinate the Administration's vision of the NII. The *Agenda for Action* recognized the importance of the NCS's continuing work in reducing the vulnerability of the Nation's telecommunications systems. NSTAC was also called upon in the *Agenda for Action* to continue to offer advice to the President on NS/EP telecommunications issues, work with the FCC's Network Reliability Council (later to become the National Reliability and Interoperability Council), and complement the work of the U.S. Advisory Council on the NII. In response to this direction, the NSTAC established its NII Task Force. In this framework, industry and Government focused on the impact the NII might have on network security, NS/EP capabilities, and privacy. Other priorities included defining the roles of the private and public sectors in considering the effects of current and proposed regulation, integrating the NII with manufacturing and electronic commerce, and improving the delivery of health care and educational programs.

EXPANDING THE VISION AND STRATEGY: 1994

When E.O. 12472 redefined the NCS mission in 1984, it addressed communications concerns in a world at the height of the nuclear weapons buildup. At that time, the NCS mission was to *Assist the President... in (1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this order [E.O. 12472]; and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.*⁶³

Today the NCS mission addresses a widening spectrum of disruptive and destructive threats, including nuclear incidents, terrorist activities, civil disorder, information warfare, natural disasters, and nefarious cyber attacks. Regional conflicts, domestic disturbances, and the adverse use of high technology (such as, electronic intrusion/disruption) challenge our national security and our ability to respond. These profound

changes in the threat and the rapid insertion of new technologies highlighted a need for restructuring throughout the Federal Government. In response, the NCS broadened its response capability to meet an ever-increasing array of new challenges such as the computer intrusion threat, growth and diversity in the telecommunications environment, and a more sophisticated terrorist threat. The NCS now focuses on ensuring common and ubiquitous communications services are available during any crisis to support critical Government functions.

This change in focus is a direct result of several legislative initiatives begun in 1993. At that time, President Clinton requested an extensive study of the Federal Government's ability to effectively perform its functions and duties.⁶⁴ The result of that 6-month study of Government operations, the *Report of the National Performance Review (NPR)*, called upon certain Federal departments and agencies to make necessary changes to "create a Government that works better and costs less."

Concurrently with the NPR study, the Director, OSTP, issued a memorandum on NS/EP telecommunications that provided the foundation for restructuring the NCS. The memorandum directed the Manager, NCS, to take the steps necessary to enhance the National Telecommunications Management Structure (NTMS) to ensure a flexible, integrated response capability to manage the Nation's telecommunications assets "across the full spectrum of domestic and national security emergencies."⁶⁵ This guidance paved the way for expansion of the NTMS mission to more closely reflect that of the NCS and encompass emergency telecommunications response following natural and man-made disasters and emergencies.

During this time, Army Lieutenant General Alonzo E. Short, Jr., serving as the NCS Manager, also determined that the NCS could benefit from a reexamination of its operations in light of changes in the threat, rapid advances in

"The NCS team, in partnership with industry, ensures immediate, interoperable, and secure global information services to support national security requirements and preparedness for emergency response to all hazards."

technology, the NPR report, a declining Federal budget, and the new NTMS mission defined by the Director, OSTP. This appraisal encompassed a review of NCS authorities, identification of issues for resolution, and the synthesis of strategic goals. General Short established the Office of Strategic Planning on April 1, 1994, to assist in developing the new strategy.

In an off-site meeting in October 1994, the COP created a new purpose, mission, and vision for the NCS and delineated issues for task forces to resolve.⁶⁶ The COP's vision statement for the NCS incorporated an inevitable paradigm shift from communications technology to information technology: *The NCS team, in partnership with industry, ensures immediate, interoperable, and secure global information services to support national security requirements and preparedness for emergency response to all hazards.*⁶⁷

To achieve this vision, the COP stated that the NCS mission is to "[l]ead the planning, coordination, and integration of Government telecommunications capabilities to ensure access to, and use of critical information services required for effective response in an all-hazards environment."⁶⁸

NATIONAL COMMUNICATIONS SYSTEM STRATEGIC PLAN: 1996

On November 1, 1995, the NCS restructured the OMNCS for the first time in more than a decade, with its offices realigned into functional divisions based on complementary programs, services, and activities. The Manager and Deputy Manager remained the guiding authority for the NCS. However, below the Deputy Manager, clearer lines of authority and specialization divided the OMNCS into five areas: Programs, Operations, Plans and Resources, Customer Service and Information Assurance, and Technology and Standards.

In response to the COP mission statement for the NCS and concurrent with the OMNCS restructuring, the NCS set seven goals in its strategic plan as a road map to achieving its vision established in 1994. The NCS adopted its Strategic Plan in January 1996, “ensuring the Government has the telecommunications capabilities to gain access to and use critical information services in an all-hazards environment.”⁶⁹ With the seven goals, the plan delineated 28 objectives and supporting strategies for the NCS’s transition into the 21st century. In February 1998, the OMNCS reviewed the NCS Strategic Plan and began the development of performance measures for assessing NCS progress against its objectives.

The NCS adopted the strategic plan to guide the organization through the new technology-driven, highly sophisticated, and continuously evolving NS/EP telecommunications environment. When President Reagan issued E.O. 12472, continuity of Government and of operations was the principal NCS concern. Emergency personnel, who now respond to the spectrum of disasters, depend on NS/EP telecommunications to efficiently and effectively react to hurricanes, floods, earthquakes, and acts of terrorism, forcing the NCS to broaden the definition of its customers.

GROWING EMERGENCY RESPONSE EFFORTS

Ensuring communications for a ready, informed, and equipped emergency response team has always posed a serious challenge to disaster and recovery operations. In 1995, the NCS, in conjunction with the Federal Emergency Management Agency (FEMA), identified all the communications requirements for a disaster area and then implemented effective solutions to improve communications capabilities.⁷⁰ They discovered the need for emergency response personnel to exchange information with different parties anywhere and anytime with security and flexibility. At the same time, they needed to access, retrieve, and communicate a wide range of distributed information from the disaster area, the disaster field office, regional offices, and department and agency headquarters. Finally, the NCS and FEMA determined that the Internet, which was revolutionizing information exchange, could support many of these wide-ranging communications needs.

Reemphasis on the need for such a capability in a disaster area occurred when Hurricane Marilyn severely damaged the telecommunications infrastructure of the U.S. Virgin Islands in September 1995. In response, the OMNCS designed an emergency response telecommunications and information-processing package using off-the-shelf components and software. Emergency personnel could carry the Emergency Response Fly-Away Kit to a disaster site from OMNCS headquarters and enhance the ability of on-site emergency response personnel to communicate to or from anywhere in the United States quickly and effectively via voice, data, and video.

Additionally, the OMNCS developed the Emergency Response Link (ERLink) to take advantage of the Internet’s versatility and ubiquity. ERLink provides a Web site for Federal Response Plan participants to upload and retrieve response reports and documents, based on the Internet’s World Wide Web technology. Links to agencies also provide a wide array of response-related information. Agencies participating in ERLink determine the type of information they will provide to the system and who in the ERLink community will have access to it. Authorized NS/EP participants can download documents and reports, eliminating the need to send response information out in hard copy or e-mail format and simplifying the dissemination of information. ERLink made its first pilot test on September 17, 1996, with the participation of the Departments of Transportation, Commerce, and the Interior; the Nuclear Regulatory Commission; GSA; the U.S. Army Corps of Engineers; and the State of California.⁷¹ The OMNCS began transitioning ERLink to its operations component in 1997.

While ERLink provides a location for authorized NS/EP participants to obtain essential information, the NCS recognized that it should also develop systems to ensure NS/EP personnel have the ability to communicate in the event of a crisis. To achieve this goal, the NCS enhanced and updated the relevant programs of the NLP and developed both GETS and the Wireless Priority Service (WPS) programs.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

The OMNCS established the Government Emergency Telecommunications Service (GETS) to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in NS/EP missions. The NCS designed GETS to replace NETS and changed the technological thrust of the former NETS Program by shifting from hardware solutions toward software-based solutions that offered greater system flexibility and efficiency at a lower cost.⁷²

GETS is a telecommunications service provided by the NCS that supports Federal, State, and local Government, industry, and non-profit organization personnel in performing NS/EP missions. GETS provides emergency access and priority processing in the local and long distance segments of the PSN. Its intended use was for an emergency or crisis situation during which the probability of completing a call over normal or other alternate telecommunication means has significantly decreased. The program ensures GETS users experience a high rate of call completion during network congestion or outages arising from natural or manmade disasters. GETS reached its full operating capability on September 30, 2001.

The GETS program is a nationwide capability for switched-voice and voice-band data communications using the surviving switching and transmission facilities of the PSN, augmented by selected Government networks, like FTS 2000 and the Defense Switched Network. GETS was developed because of increased vulnerability from system failures during emergencies. Although backup systems are in place, disruptions in service can still occur. Recent events have shown that natural disasters, power outages, fiber cable cuts, and software problems can cripple the telephone services of entire regions. Additionally, congestion in the PSN, such as the “Mother’s Day phenomenon,”⁷³ can prevent access to circuits. During times of emergency, crisis, or war, personnel with NS/EP missions need their calls to go through — and GETS addresses this need.

GETS allows the NS/EP community to communicate over existing PSN paths with a high likelihood of call completion during the most severe conditions of high-traffic congestion and disruption. Users can access GETS by dialing a Personal Identification Number (PIN) on common telephone equipment, such as a standard desk set, a secure telephone unit such as the Secure Telephone Unit-Third Generation, facsimile, or modem. The use of unique PINs ensures that only authorized users can access the service.

As the PSN evolves into packet-based technology supporting voice traffic, the GETS Program Management Office is working with industry to maximize their substantial investment in the circuit-switched network. New technologies, such as nationwide fiber optic networks and high-speed digital switching, are continually being implemented in the wireline structure. The GETS program will continue to take advantage of these new capabilities as technologies become economically and technologically more viable.



WIRELESS PRIORITY SERVICE

The introduction of wireless services — identified as strategically critical — added new dimensions to the NS/EP telecommunications environment. New wireless technologies, like mobile satellite services, land mobile radio and specialized mobile radio, and personal communications services, had major implications for the NS/EP community. Digitization of wireless systems and the consequent interoperability impact on facsimile data and secure voice prompted the NSTAC to establish a Wireless Services Task Force (WSTF) in 1991. The WSTF scoped NS/EP issues associated

with wireless services and advised the OMNCS how to minimize any adverse effects of emerging digital mobile communications standards and technologies on mobile NS/EP users.⁷⁴

In July 1994, the WSTF established the Cellular Priority Access Service Subgroup to investigate technical, administrative, and regulatory issues associated with deployment of a nationwide priority access capability for NS/EP cellular users. The NSTAC subsequently recommended the establishment of such a service for NS/EP users. In 1996, the FCC published the first R&O on Priority Access Service (PAS), and the NCS began working with industry and Government to begin implementation. After seeking feedback on wireless priority access, the FCC issued a second R&O on PAS in July 2000, establishing the regulatory, administrative, and operational framework to enable commercial mobile radio service providers to offer WPS to NS/EP personnel.

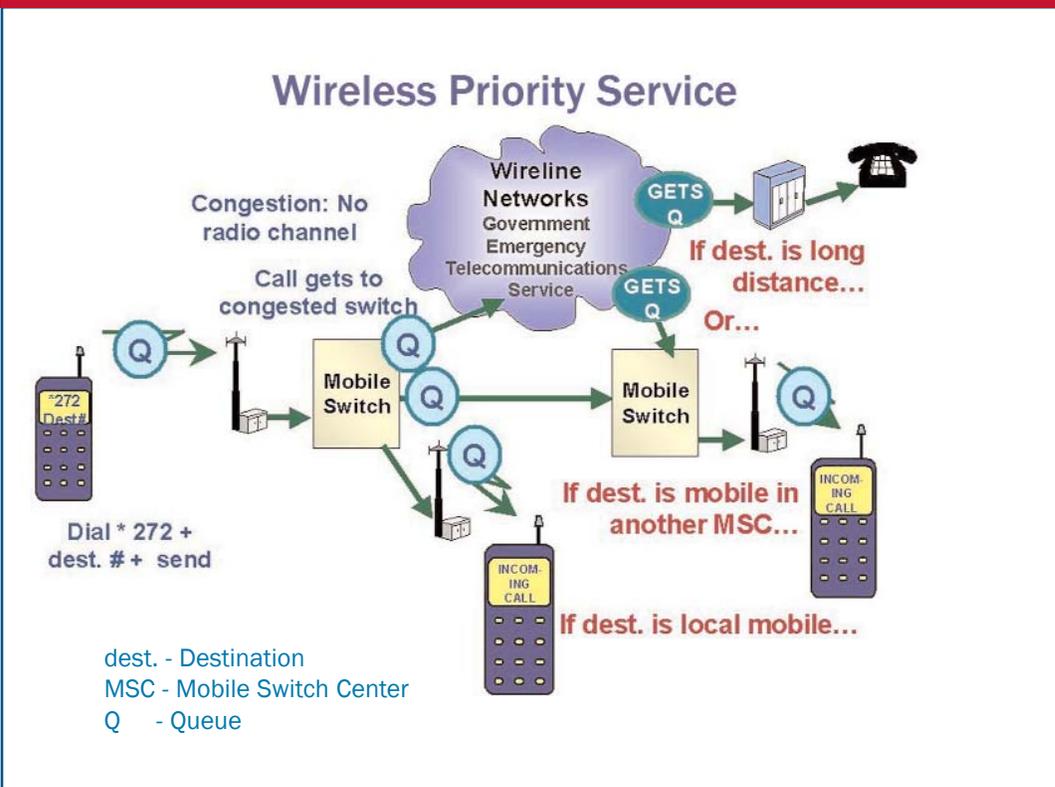
WPS serves as the wireless complement to the wireline GETS. GETS utilizes the PSTN to provide enhanced wireline priority service to authorized NS/EP personnel. WPS service is granted only to key NS/EP leadership personnel — WPS is not intended for use by all emergency service personnel. The NCS authorizes and encourages WPS users to use GETS to better their probability of completing their NS/EP call during periods of wireless and wireline network congestion, such as during the terrorist attacks of September 11, 2001. The NCS continues to work toward reaching full operational capability of WPS as soon as possible.

THE NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS AND EMERGENCY RESPONSE

Because of the tremendous technological advances affecting emergency response telecommunications in the mid- to late-1990s, emergency responders have come to rely on GETS and WPS for telecommunications connectivity during and following natural disasters and in support of NS/EP activities. However, as important as those technologies have become, they would be far less effective were it not for the parallel growth and technological progress of the organization responsible for coordinating nationwide emergency

telecommunications — the NCC.

Wireless Priority Service is expected to reach Full Operating Capability in December 2004.



Industry and Government partnership in preparing for and planning for emergency response activities is critical to ensure seamless response capability. The NCC created a strong synergy between the telecommunications industry and Government. The commercial telecommunications industry owns the majority of telecommunications assets, including the facilities, equipment, and personnel trained

to restore NS/EP services. These industry assets become the primary resources for the Government during disaster response operations. Industry representatives work from their offices within the NCC, and are in direct contact with their company senior management and key operations centers. This enables the NCC to respond with exceptional effectiveness in emergency and disaster situations.

This cooperative relationship succeeds because industry representatives and NCC personnel work together before, during, and after emergencies to ensure a seamless response capability. NCC operational exercises such as the Federal Radiological Emergency Response Plan exercise (April 1995), the Health and Medical Services tabletop exercise (December 1996), and the ERLink exercise (April 1997), prepared NS/EP personnel to function effectively. Through the NCC, industry and Government prepare joint reports after any disaster to analyze response activities, document lessons learned, and identify necessary improvements. However, none of these programs would run effectively without the ability of NCS personnel to promptly respond in the event of a crisis.

PLANNING, TRAINING, AND EXERCISE BRANCH

The readiness of NCS personnel to quickly respond to emergencies is critical to the success of NS/EP capabilities and programs. Training and exercise of NCS personnel had been ongoing for several years, but

Hurricane Isabel

The National Communications System (NCS) has assisted in the relief efforts relating to numerous natural disasters since its inception. In response to wildfires, ice storms, and hurricanes, the National Coordinating Center for Telecommunications (NCC) helped ensure that Federal, State, and local responders received national security and emergency preparedness telecommunications support during and after these disasters, and the NCS deployed Individual Mobilization Augmentees (IMA) to assist NCS Regional Managers serving as Federal Emergency Communications Coordinators in support of disaster response.

As the NCS completed 40 years of service, it mobilized in response to damage caused by Hurricane Isabel. In September 2003, Hurricane Isabel became the first Category 5 hurricane in the Atlantic since 1998 and made landfall in North Carolina as a

Category 2 hurricane crushing the East Coast from North Carolina to Pennsylvania. Isabel knocked out power for millions of people, and in Isabel's aftermath, the telecommunications infrastructure was debilitated by commercial power outages. The NCC itself experienced significant power outages resulting in local area network and e-mail problems. Fortunately, the NCS emergency response operations were able to continue through the use of backup power generators to provide a coordinated emergency response effort with the Department of Homeland Security and its Federal Emergency Management Agency (FEMA).

The NCS deployed three IMAs to disaster field offices in Raleigh, NC and Richmond, VA to assist NCS

regional managers serving as Federal emergency communications coordinators. In addition, the NCS Telecommunications Service Priority Office processed provisioning requests to support FEMA disaster field offices in Raleigh, NC; Richmond, VA; Washington, DC; Baltimore, MD; New Castle, DE; Elizabeth City, NC; New Bern, NC; and Harrisburg, PA.



in 1994, the OMNCS created the Training and Exercise Branch within its Operations Division to support the NCS NS/EP mission. This branch later became known as the Planning, Training, and Exercise Branch. The branch conducts training events and activities for OMNCS staff, NCS Regional Managers, NCS member organizations, and industry participants. The primary goal is to increase the emergency response community's ability to execute its responsibilities during all crises and emergencies.

The training seminars focus on provisioning emergency telecommunications service within a disaster site. Telecommunications Emergency Response Training (ERT) seminars are conducted in coordination with NCS member organizations, State Governments, and the telecommunications industry. NCS personnel conducted Phase I of the ERT seminars from May 1993 through April 1995 across the country in which the OMNCS concentrated on the overview of the Federal Response Plan and the Federal, State, and industry relationships to support Federal Response Plan Emergency Support Function 2 (Communications).

The OMNCS exercises and analyses cover many aspects of cooperation between industry and Government in NS/EP telecommunications, including tabletop exercises designed to examine telecommunications requirements and assess the capabilities of new technologies.

Individual Mobilization Augmentee Program

The National Communications System (NCS) established the Individual Mobilization Augmentee (IMA) Program in 1988 to provide skilled civilian and military reservists to enhance the efforts of the NCS and the National Coordinating Center for Telecommunications (NCC) during national crises and emergencies. The original mission of the NCS IMA Program was to provide

emergency telecommunications support to the Office of the Manager, NCS (OMNCS) during mobilization and wartime. More recently, the Government expanded the NCS IMA requirements to reflect the emergency telecommunications support mission to the full spectrum of wartime and peacetime contingencies, including Emergency Support Functions under the Federal Response Plan.

the first personnel to respond to crises and emergencies. When called, they deploy to support OMNCS headquarters in Arlington, Virginia, the NCC Emergency Operations Teams, the NCS Regional Managers, or the Federal Emergency Communications Coordinator at the Disaster Field Office.

Since program inception, IMAs have assisted in many critical telecommunications emergency response activities throughout the United States, including those stemming from the earthquakes in California and the Northwestern United States; terrorist bombings in Oklahoma City, the Atlanta Olympics, and the September 11 terrorist attacks in New York City; wildfires in the western and southwestern states; flooding in the Midwest; and numerous hurricanes and tropical storms since 1992 to present.

NCS IMA personnel augment NCS staff during national and regional crises and emergencies. They are geographically dispersed across the continental United States and are often among

Following natural disasters, Individual Mobilization Augmentees are geographically dispersed to impacted areas.



In addition to industry/Government cooperation, the NCS Augmentee Program demonstrates the strength of the NCS civilian and military partnerships in responding the natural disasters. The NCS established its Augmentee Program in 1988 to provide a cadre of skilled civilian and military reservists to enhance the efforts of the OMNCS, the NCC, and NCS Regional Managers during national crises and emergencies. The NCS Augmentee Program consists of two components: the civilian members of the National Defense Executive Reserve and the U.S. Army Reservists participating in the Individual Mobilization Augmentee (IMA) Program.

The NCS IMA Program is a valuable cost-effective resource of trained telecommunications experts who support the NCS mission during national security emergencies and natural disasters. NCS IMAs are normally U.S. Army Signal Corps field grade officers with staff officer experience, who demonstrate the leadership and organization skills required to fulfill the responsibilities expected of NCS IMAs. The original mission of the NCS IMA Program was to provide emergency telecommunications support to the OMNCS during mobilization and wartime. However, the program's evolution and expansion now reflects the all-hazard NCS mission of providing emergency telecommunications support to the full spectrum of wartime and peacetime contingencies.

The NCS geographically disperses its IMAs across the continental United States; therefore, the IMAs are often among the first personnel to respond to crises and emergencies. For example, following the Northridge earthquake in January 1994, the Oklahoma City bombing in April 1995, Hurricane Marilyn and Opal in September 1995, and the floods in the Pacific northwest in February 1996, NCS IMAs deployed to assist regional personnel and the Federal Emergency Communications Coordinator in the provision of telecommunications in the disaster areas.

Part 3

**EARLY
RECOGNITION,
EMERGING
RESPONSE**

Part 3

Early Recognition, Emerging Response

Modern society increasingly relies on advanced telecommunications, computers, and automated information systems in everyday life. A secure highly efficient information infrastructure is vital to the national security and economic growth of the United States, as both industry and the Government are heavily dependent on the information infrastructure for day-to-day operations and business transactions. The Nation's vital communications systems are vulnerable to attacks that could cause sustained outages and widespread disruption. Furthermore, the risk to these systems extends to other national infrastructures supporting American society. While all infrastructures are important and interdependent, telecommunications is so pervasive and heavily relied upon by the other infrastructures that it serves as an integrating focal point for Critical Infrastructure Protection (CIP). Finance, transportation, air space management, energy systems, and everyday business transactions depend on automated information networks to carry out their functions. The massive interconnection of computerized communications and information networks across public and private sectors has increased the vulnerability of the entire system and has given current and potential adversaries a point of attack against U.S. interests. For this reason, the protection of critical infrastructure is essential to the Nation's well being.

EARLY CRITICAL INFRASTRUCTURE PROTECTION EFFORTS

The NCS and NSTAC identified CIP as an important issue in the early 1990s. Recognizing the interdependencies between the energy and telecommunications industries, the NCS engaged leaders from the energy industry in work aimed at mitigating the associated vulnerability. The NCS and NSTAC worked bilaterally with the electric power industry to investigate electric power and telecommunications restoration procedures.

In 1990, the NSTAC recommended the Government organize a program for priority electric power restoration and fuel distribution to critical telecommunications users and providers. In 1991, the NSTAC formed a second Energy Task Force to advise the Government on energy priority initiatives for NS/EP telecommunications facilities. The reactivated task force assisted in developing the concept of the NCS's Telecommunications Electric Service Priority (TESP). Although TESP, which was a collaborative effort between the Department of Energy (DOE) and the NCS's TSP, has yet to be fully implemented, it represented the growing recognition of the interdependencies between the various infrastructures.

CRITICAL INFRASTRUCTURE PROTECTION: RECOGNIZING INTERDEPENDENCIES

In January 1995, during the NSTAC XVII Meeting, the National Security Agency (NSA) Director briefed the NSTAC Principals on threats to U.S. information systems and the need to improve security of the Nation's critical infrastructures. The NSTAC Principals discussed these issues and subsequently sent a letter in March

to President Bill Clinton stating: “The integrity of the Nation’s information systems, both Government and public, are increasingly at risk from intrusion and attack... [and that] other national infrastructures... [such as finance, air traffic, power, etc.] also depend on reliable and secure information systems, and could be at risk.”⁷⁵ President Clinton replied that he would “welcome the NSTAC’s continuing effort to work with the Administration to counter threats to our Nation’s information and telecommunications systems.”⁷⁶ The President further asked “the NSTAC Principals — with input from the full range of users of the NII — to provide me with your assessment of the national security and emergency preparedness requirements for our rapidly evolving information environment.”⁷⁷

In response to the President’s request, the NSTAC established the Information Assurance Task Force (IATF) in May 1995 — later renamed the Information Infrastructure Group (IIG) — to work with the Government to identify critical national infrastructures and to act as the focal point for the NSTAC’s information assurance activities.

“The integrity of the Nation’s information systems, both Government and public, are increasingly at risk from intrusion and attack... [and that] other national infrastructures... [such as finance, air traffic, power, etc.] also depend on reliable and secure information systems, and could be at risk.”

FEDERAL CRITICAL INFRASTRUCTURE PROTECTION POLICY

The tragic events surrounding both the bombing of the World Trade Center on September 26, 1993, and the bombing of the Alfred Murrah Federal Building in Oklahoma City on April 19, 1995, highlighted the certainty of future terrorism on American soil.

In response, President Clinton signed Presidential Decision Directive 39, U.S. Policy on Counterterrorism, (PDD-39) on June 21, 1995, describing the Administration’s new counter-terrorism policy. In an unclassified portion of PDD-39, he President directed the Attorney General Janet Reno to “chair a Cabinet Committee to review the vulnerability to terrorism of... critical national infrastructures and make recommendations to the President and the appropriate Cabinet member or Agency head” on how to protect those infrastructures.

The Telecommunications Act of 1996

The Telecommunications Act of 1996 called for the most comprehensive changes in the U.S. telecommunications industry since *The Communications Act of 1934*. The 1996 Act dramatically revolutionized competition and regulation in virtually all sectors of the communications industry, from local and long-distance telephone services, to cable television, broadcasting, and equipment manufacturing.

The 1996 Act opened the telecommunications marketplace to new service providers unfamiliar with potential

national security vulnerabilities and threats to their networks. In addition, increased competition paved the road for technological advances that could challenge the Government’s ability to provide secure, reliable, and interoperable national security and emergency preparedness (NS/EP) telecommunications.

To keep pace with the rapidly changing technological advances, the National Communications System (NCS) monitors and examines the implications of new technologies on NS/EP telecommunications. The NCS

responds to change by updating its programs to adequately meet the evolving environment demands. For example, the NCS implemented the Wireless Priority Service program to enable key Government officials’ priority access to the expanding cellular network in times of network congestion.

Meeting the challenges of this dynamic environment, the NCS continues to serve as a bridge between industry and Government, helping to ensure national security telecommunications to support the Federal Government.

Accordingly, in 1995, the Attorney General established a small interagency task force led by the Justice Department, called the Critical Infrastructure Working Group (CIWG).

The CIWG reported that although there were many pockets of expertise on CIP within the intelligence, law enforcement, and defense communities, no central coordinating mechanism existed among these communities. The CIWG concluded that an unprecedented amount of private sector participation would be required to adequately address the evolving problem. With its composition as an interagency body and its strong relationship with industry through the NSTAC, the NCS sat in a unique position to provide leadership and guidance for CIP efforts.

The U.S. Congress became aware of and concerned with the potential risks facing the Nation's vital infrastructures. In August 1995, U.S. Senator Jon Kyl of Arizona sponsored an amendment to the National Defense Authorization Act for fiscal year 1996. President Clinton signed the bill into law on February 10, 1996, and called on the White House to report the following: the national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions on strategic attacks by foreign nations, groups, or individuals, or any other entity against the NII; and the future of the NCS, which has performed the central role in ensuring NS/EP communications for essential U.S. Government and private sector users.

In the summer of 1996, the Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations held a series of hearings on security in cyberspace and heard from representatives of the NCS, the NSTAC, and other agencies of the executive and legislative branches, private industry, and academia. Facts presented in the testimonies made national news, as the hearings became a milestone in building awareness of the need for critical infrastructure protection.

On July 15, 1996 — the day before the final Senate hearing on security in cyberspace — the Clinton Administration issued E.O. 13010, *Critical Infrastructure Protection*. The executive order immediately established the President's Commission on Critical Infrastructure Protection (PCCIP) to:

- Assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures;
- Determine what legal and policy issues are raised by efforts to protect critical infrastructures;
- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats; and
- Propose any statutory or regulatory changes necessary to effect its recommendations.

The Clinton Administration designed the PCCIP as a commission of industry and Government, chaired full-time by a representative from the private sector and composed of representatives nominated by the heads of ten different Federal departments and agencies. The executive order identified eight infrastructures considered "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."⁷⁸ These infrastructures include: telecommunications, electric power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of Government. The PCCIP briefed NSTAC working groups and coordinated with the NSTAC on risk assessment projects of the core components of the Nation's economic and financial infrastructure. The commission submitted its final report on October 22, 1997, with seven strategic objectives and 78 recommendations, setting the stage for the broader elaboration of CIP policy within the Federal Government.

PRESIDENTIAL DECISION DIRECTIVE 63: 1998

Six months after the PCCIP submitted its report, President Clinton signed Presidential Decision Directive 63 (PDD-63), *Protecting America's Critical Infrastructures*, on March 22, 1998, with the main goal to develop a comprehensive strategy to bring to bear the knowledge and resources of the Federal Government and the private sector to assure the continuity and viability of the Nation's critical infrastructures. Because the private sector owns and operates most of the infrastructures, the directive aimed to forge a public-private partnership for comprehensive infrastructure protection. PDD-63 appointed a lead agency and liaison for each critical sector to engage the private sector through a sector coordinator. Infrastructure protection activities were then led by the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, which would report through the Assistant to the President for National Security Affairs.

Other structures established through PDD-63 included information sharing and analysis centers (ISACs), mechanisms by which the Government encourages the private sector to gather, analyze, and disseminate private sector information on critical infrastructure protection. The National Infrastructure Protection Center (NIPC), housed at the Federal Bureau of Investigation (FBI), worked with the ISACs and acted as the focal point for gathering information on threats to infrastructures. PDD-63 also established the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce, as well as the National Infrastructure Assurance Council, a panel appointed by President Clinton with representation from both major infrastructure providers and State and local Government officials.

The foundation of the NCS had always been based upon critical infrastructure protection activities referenced in PDD-63. Although the document did not articulate a formal NCS role in the national CIP strategy, both the NCS and the NSTAC IATF played crucial roles in building CIP policy.

CONTINUING ROLE IN CRITICAL INFRASTRUCTURE PROTECTION

While the Federal Government was building an initial awareness of CIP's importance, the NCS continued the work it had begun several years earlier. Validated by Federal initiatives including PDD-39 and PDD-63, the NCS continued its critical infrastructure protection initiative through a series of assessments conducted on the components of the Nation's infrastructure from 1995 through 1999.

TELECOMMUNICATIONS INFRASTRUCTURE RISK ASSESSMENT

In 1995, the NCS and NSTAC engaged in assessing risks to the telecommunications infrastructure. Government and NSTAC NSIEs published their report in December 1995, *An Assessment of the Risk to the Security of the Public Switched Network*, calling upon the Government to:

- Assess the security and robustness of the particular infrastructures at the national level relative to the identified threats to their networks and information systems;
- Determine the risks to the industries that derive from their dependence on the telecommunications infrastructure; and
- Examine the implications of trends in the industries' use of information systems and networks.

The NCS and the NSTAC IATF sought to leverage their 1995 findings to recommend that electric power, financial services, and transportation infrastructures be studied to assess and raise awareness of their dependence on telecommunications and information systems. As a result of these projects, the President requested the NSTAC to follow through on assessments of these infrastructures and as a result, the NSTAC forwarded several reports and recommendations to President Clinton on enhancing information security and critical infrastructure protection.⁷⁹

ELECTRIC POWER RISK ASSESSMENT

The NCS and the NSTAC IATF met with representatives from eight electric utilities, two industry associations, an electric power pool, equipment manufacturers, and industry consultants. The interviews showed the extent to which the electric power infrastructure depends upon the telecommunications infrastructure and information systems, in particular the Supervisory Control and Data Acquisition (SCADA) systems. The IATF concluded that such interdependencies between the infrastructures and associated vulnerabilities placed the electric power infrastructure at risk to denial-of-service attacks. From this work, the IATF submitted the *Electric Power Risk Assessment* in March 1997 at the NSTAC XIX Meeting and recommended that the President:

- Designate an appropriate department or agency to develop and conduct an ongoing program within the electric power industry to increase awareness of vulnerabilities and available solutions;
- Establish an NSTAC-like advisory committee to enhance industry and Government cooperation on regulatory changes affecting electric power; and
- Provide threat information and consider incentives for industry to work with Government to develop and deploy security features for the electric power industry.

FINANCIAL SERVICES RISK ASSESSMENT

To assess the risk to financial services, the NCS and the NSTAC IIG, in cooperation with the PCCIP, also conducted confidential interviews with financial institutions, including banks, securities credit firms, credit card associations, third-party processors, industry utilities, industry associations, and Federal regulatory agencies. The assessment found that, overall, the industry incorporated security into its fundamental risk controls as part of a system of independent, mutually reinforcing checks and balances within critical networks and systems. This system ensured integrity within the infrastructure. However, as with electric power risk, the IIG found increasing interdependence between financial services and telecommunications infrastructure.

Response '98

The National Communications System (NCS) regularly participates in training exercises to test and refine procedures and ensure its readiness in times of actual emergencies. In April 1998, the NCS's National Coordinating Center for Telecommunications (NCC) participated in an exercise designed to test their response to a natural disaster. The four-day, Federal Emergency Management Agency-sponsored exercise—dubbed RESPONSE-98—simulated a hurricane threat to the northeast United States and Canada.

The NCS coordinated industry participation among Bell Atlantic (now Verizon), Southern New England Telephone (now part of SBC), and the now-defunct National Telecommunications Alliance. The coordination efforts also included members of Emergency Operations Teams at the NCC and at five deployed locations as representatives of Emergency Support Function-2.

Participants deemed the exercise a success because it encouraged them to work together as a team, improve their coordination skills, and experience different

scenarios. In addition, participants gained valuable experience in many NCS programs, including the Government Emergency Telecommunications Service and the Shared Resources High Frequency Radio Program. Many participants also used the now-retired Emergency Response Link program as a means of sharing damage and response information.

While the industry was protected and prepared at the national level, the assessment did identify security issues and vulnerabilities associated with: (1) dependence on an increasingly deregulated telecommunications infrastructure; (2) the integration of dissimilar information systems and networks as a result of mergers and acquisitions within the financial services industry; and (3) the introduction of Web-based financial services. In a December 1997 report submitted at the NSTAC XX Meeting, the IIG recommended the President:

- Assign the appropriate department or agency to identify external threats and risk mitigation to the financial services infrastructure and facilitate information sharing between industry and Government;
- Assign the appropriate department or agency to work with the private sector to develop mutual agreeable solutions for background investigations for sensitive positions;
- Assign the appropriate department or agency to monitor the new and emerging areas of electronic money and commerce; and
- Ensure that NSTAC continues to have at least one member of the financial services industry.

The close relationship with the financial services sector continues today with financial services industry representation on the NSTAC.

TRANSPORTATION RISK ASSESSMENT

The IIG completed its Transportation Risk Assessment for NSTAC XXII in June 1999. Over two NSTAC cycles, the assessment team had conducted two workshops — Fort McPherson, Georgia, in September 1997 and Tampa, Florida, in March 1999 — bringing together representatives from major transportation companies, including airlines, multi-modal carriers, rail, highway, mass transit, and maritime. The task force concluded that the transportation industry is increasingly reliant upon information technology and the information infrastructure. While the infrastructure is very diverse and multimodal, the escalated use of interconnected information technology systems raised concerns for a potential large-scale disruption. There was a need, the assessment found, for greater awareness of security risks and interdependency issues in the industry. The NSTAC recommended that:

- The President support efforts of the recently released PDD-63 for outreach and awareness within the transportation infrastructure;
- The Government issue timely information on threats to the transportation industry;
- Government Research and Development programs design information assurance tools to address cyber threats to the transportation information infrastructure;
- The Government examine vulnerabilities of the Global Positioning System; and
- The Government stimulates inter-modal and inter-infrastructure information exchanges on threats, vulnerabilities, and best practices.

NSTAC risk assessments of electric power and transportation infrastructure highlighted the importance of secure SCADA systems. SCADA systems are ubiquitous in the electric power, transportation, and telecommunications industries. In the electric power, rail, and pipeline industries, SCADA systems provide the data essential for regulating systems, ensuring balancing, and facilitating generation and transmission.

These systems permit remote control of valves, compressors, and other critical pipeline components. Destruction of SCADA systems would result in serious damage to operations. The NCS and NSTAC called for coordinating R&D of such systems and examining their security implications.

Together, these NSTAC risk assessments highlighted the interdependencies between critical infrastructures and contributed significantly to the overall discourse on the emerging information assurance question, which eventually led to the establishment of the PCCIP and eventually PDD-63.

NATIONAL COORDINATING MECHANISM

Through the risk assessments, the NCS, NSTAC, and a growing number of industry and Government officials advocated a National Coordinating Mechanism (NCM) to deal with security vulnerabilities posed by the increased interdependency of infrastructures. While the NSTAC had initially considered an NCM for the telecommunications infrastructure, the NCS and NSTAC revised the NCM model to incorporate all infrastructures and develop organizational processes to supply senior Federal Government decision makers with real-time information from the components of critical national infrastructure. The NCM would be a joint industry/Government planning forum for infrastructure protection. At NSTAC XX in December 1997, the NSTAC recommended the President designate the appropriate Government departments and agencies to refine the NCM concept.

INSTITUTING THE CRITICAL INFRASTRUCTURE PROTECTION AGENDA

In January 2001, Mr. Richard Clarke, Special Advisor to the President for Cyberspace Security, forwarded two memoranda directing the NCS to complete several key tasks for critical infrastructure protection. The memoranda assigned the NCS a role in contributing to the ongoing development of the Cyber Warning Information Network (CWIN) (now known as the Critical Infrastructure Warning Information Network), assisting in developing a conceptual framework for a “synoptic view” of telecommunications networks, and developing a process for declassifying information to enable the Government to share timely and useful intrusion data with industry.

In response, the NCS formed the Integrated Product Team (IPT) to explore the mission and roles of the NCS in supporting telecommunications-specific and national-level CIP initiatives. In its study, the IPT considered national CIP priorities, roles, and key players; analyzed current roles played by the NCS; and identified potential new roles the organization could perform. The IPT interviewed representatives from many of the key stakeholders in the national critical infrastructure protection arena to identify current gaps and

“The NCS will, ‘In partnership with industry and Government, ensure immediate, interoperable, and assured information services for national security and emergency preparedness in all situations.’”

opportunities in national CIP efforts. Among the findings, the IPT concluded that many of the focal points lack data from industry and face significant barriers to coordination the current landscape. In addition, the IPT noted there is little coordination across infrastructures and many of the key Federal players lack information from industry.

Building on the OMNCS’s longstanding relationships with industry through NSTAC and the early risk assessments, the IPT formulated strategies and recommendations to position the NCS to become the recognized leader in Government for working with the telecommunications industry on CIP issues. To allow the new mission-related strategies to be pursued more effectively, the IPT developed a list of recommendations to reposition the NCS, including: (1) establishment of a standing Executive Coordination Committee (ECC) comprised of the division chiefs with industry representation; (2) resource planning to ensure support for the implementation of the OMNCS’s new organizational structure, strategies, and roles; and (3) reorganization of the NCS with the creation of a Critical Infrastructure Protection Division as the organizational focal point for CIP programs, initiatives, capabilities, and activities.

In response to the recommendation for an Executive Coordination Committee, the OMNCS established the Deputy Manager Advisory Committee (DMAC). The DMAC meets weekly and consists of the leadership in each NCS division. The goal of the meetings is to ensure coordination across the divisions as well as to advise the Manager, NCS, on larger issues relating to the NCS and its operating environment.

Also in 2001, the OMNCS reevaluated its vision statement and strategy in an executive business strategy planning exercise to ensure it was accurately positioning itself. The exercise reviewed mission, functions, and goals for the organization, as well as internal organizational structure, and division names. After several working sessions, the OMNCS refocused its vision based on the IPT findings, and the findings from the exercise. The new vision statement says the NCS will, “in partnership with industry and Government, ensure immediate, interoperable, and assured information services for national security and emergency preparedness in all situations.”

The OMNCS also responded to the IPT report by creating the CIP Division in May 2001 and realigning the organization to focus its efforts on four key initiatives:

- Ensuring new CIP-related requirements are satisfied without sacrificing the high quality of operational support and industry relationships developed over the past two decades in planning for and responding to emergencies;

Research and Development Exchanges

One of the President’s National Security Telecommunications Advisory Committee’s (NSTAC) more innovative tools for staying at the cutting edge of technology trends is its Research and Development (R&D) Exchanges. Historically, the broad purpose of the R&D Exchange program was to stimulate and facilitate a dialogue among industry, Government, and academia on emerging security technology R&D issues. To ensure that the NSTAC includes all stakeholders in the R&D community, the committee has partnered with the President’s Office of Science and Technology, the Commerce Department’s National Institute of Standards and Technology, and academic institutions in sponsoring R&D Exchanges. These exchanges have proven to be an excellent forum for discussing emerging R&D issues and making recommendations based upon the results.

Past exchanges addressed such security issues as the need for training more information technology security professionals, promoting the creation of Information Assurance Centers of Excellence in academia, and advancing trustworthiness in telecommunications and information systems related to national security and emergency preparedness (NS/EP).

The NSTAC continues to strive to conduct R&D Exchanges that evolve conceptually to meet the continual changes in technology and the political landscape and that include all stakeholders involved in protecting the

Nation’s NS/EP capabilities. Participation at NSTAC R&D events has grown from a small meeting of primarily Government representatives to a gathering of over 200 industry, Government, and academia representatives in various places across the United States. R&D Exchanges will continue to be a cornerstone of NSTAC outreach on issues vital to the success of the Nation’s NS/EP efforts.

NCS Staff members and industry representatives take notes and prepare comments during the Physical Breakout Session during the 2003 NSTAC R&D Exchange in Atlanta, Georgia.



- Integrating and realigning CIP-related projects and activities formerly managed by other OMNCS divisions into the CIP Division's organizational, management, and programmatic structure;
- Improving coordination of activities across the CIP Division; and
- Positioning the NCS as the recognized leader for CIP activities in the telecommunications infrastructure.

Building on its legacy of traditional responsibilities for NS/EP communications to support national efforts to address critical infrastructure threats and vulnerabilities, the NCS and its CIP Division realized the unique industry/Government mission of ensuring the availability of critical NS/EP telecommunications services across the full spectrum of emergencies.

OPERATIONAL ANALYSIS BRANCH

While the NCS created its CIP Division, the need emerged for an operational analysis branch. With the growing national interest in enhanced analysis tools, processes, and products, the NCS anticipated this requirement and began exploring the concept for an operational analysis capability — defined as “the analysis and interpretation of major trends, vulnerabilities, and interdependencies affecting the availability and security of the Nation's critical infrastructures.”

The NCS traditionally focused many of its analytic tools, techniques, and products on long-term systemic vulnerabilities affecting the performance of the PSN. Understanding the PSN's major trends and vulnerabilities was crucial to ensuring priority telecommunications programs, such as GETS, would meet the needs of the national leadership. But the NCS received a growing number of requests for new types of analyses of rapidly evolving threat or vulnerability scenarios more specifically targeted and distributed, such as cyber attacks against multiple targets. As the NCS assumed greater operational responsibilities for CIP and national security, it recognized the need for real-time or near-real-time analytic tools and products.

With long-term systemic tools, models, and data sets, operational analysis offers real-time evaluation and analysis of incidents for the operational elements responsible for managing them. Similarly, operational analysis involves building analytic models and simulation techniques to offer practical operational requirements for long-term tools. This method also helps in defining the types of data needed from infrastructure owners and operators.

The Operational Analysis Branch mission is to offer relevant, timely, and comprehensive analytic products to help ensure the availability and security of telecommunications services despite threats to or disruptions of the infrastructure. Through its relationship with the NDAC, the branch offers a full range of products: critical assets assessments; critical point-of-failure analyses; impact analyses; performance and vulnerability analyses; analysis processes and requirements development; and analysis tools development, testing, and evaluation.

THE CHALLENGES OF CONVERGENCE

As the communications network grew increasingly reliant upon the Internet, the NS/EP programs within the NCS faced new vulnerabilities. The NCS developed many of their key NS/EP programs throughout the 1980s and 1990s, and despite the evolving communications technologies during these times, these programs continued to reside within the PSN. As the communications network became increasingly reliant upon the Internet, the potential implications of the convergence of the PSN with the IP network to form the converged Next Generation Network (NGN) on the existing NS/EP programs, such as GETS and TSP, became a growing concern. Within the NS/EP telecommunications community, there were concerns regarding the operational ability of these programs in the event of a severe disruption of Internet service during the transition to the NGN. Moreover, the convergence of these networks integrated, more than ever before, traditional telecommunications concerns with CIP activities.

To address the concerns surrounding convergence, the NSTAC examined the dependence of NS/EP operations on the Internet, the implications of convergence on NS/EP telecommunications, and the converged network's ability to securely and reliably support NS/EP communications requirements. In the summer of 1999, the NSTAC Network Group issued a report that concluded the NS/EP community's direct dependence on the Internet for mission-critical operations was modest. Federal departments and agencies with NS/EP responsibilities were using the Internet mostly for outreach, information sharing, and electronic mail, and the NS/EP community was more inclined to depend on dedicated Transmission Control Protocol/IP networks (Intranets) for mission-critical NS/EP operations. Though many believed that Intranets offer greater control of network elements, disruptions to the Internet can affect the availability, reliability, and integrity of Intranets as well. As a result of this study, the NSTAC examined the potential impact of convergence on PSN-specific NS/EP priority service (GETS and TSP). This study resulted in the conclusion that new NGN capabilities would require enhancements to best satisfy specific NS/EP requirements.

In 2001, the NSTAC formed the Convergence Task Force (CTF) to analyze issues related to potential security and reliability vulnerabilities of converged networks. The CTF concluded the PSN was indeed becoming increasingly vulnerable as the converged network provided ample opportunities for individuals to gain access to, manipulate, and steal sensitive information via the PSN. In addition, the interoperation of the PSN intelligent network with the IP networks via existing unreliable gateways also presented vulnerabilities. The CTF recommended the implementation of signaling firewalls at network gateways and that embedded security capabilities be defined through standards. In addition, the CTF recommended additional analysis of converged network security vulnerabilities to gain further understanding of the potential consequences of the evolving NGN. As the NGN and the threat environment both evolve, the NCS continues work to evaluate and mitigate the vulnerabilities associated with convergence.

ALERTING AND COORDINATION NETWORK

With the potential vulnerability of the PSN network, the NCS further ensures NS/EP telecommunications through the Alerting and Coordination Network (ACN), a private network that gives its users a non-PSN-based switching capability for direct connectivity to State and local Government agencies, telecommunications service providers, and equipment manufacturers. It is operational at all times, seven days a week to support the NCC in both normal and emergency operations. The ACN functions as an emergency backup communications capability that could help coordinate response to and recovery from a widespread network outage.

When the PSN is inoperable, stressed, or congested, the ACN's stable emergency voice communications network connects telecommunications service providers' Emergency Operations Centers and Network Operations Centers to support coordination of NS/EP telecommunications network restoration, transmission of telecommunications requirements and priorities, and incident reporting.

ADVANCES IN STANDARDS AND TECHNOLOGY

During the late 1990s, the NCS also continued standards related work, which began in the early 1970s with the FTSC. The FTSC served as the primary mechanism for the NCS member organizations and other Government entities to participate in the Federal Telecommunications Standards Program work. The NCS Technology and Programs Division Chief chairs the FTSC.

In 1998, the FTSC worked with the International Telecommunications Union (ITU), concerning its International Mobile Telecommunications-2000 (IMT-2000) initiative. The IMT-2000 uses a "family of systems" concept to unify the existing diverse wireless systems into an interoperable global infrastructure capable of offering a wide range of services, meaning that different technologies offering the same type of service can be part of the standards family. The OMNCS studied the implications of IMT-2000 for NS/EP telecommunications, and supporting two of the IMT-2000 recommendations in particular,

Q.1701 and Q.1711. Q.1701 defines a framework for IMT-2000 networks; it also provides an overall framework for developing IMT-2000 signaling requirements. Q.1711 defines a network functional model for IMT-2000, identifying specific network functions that are necessary to support IMT-2000.

Whereas previous NS/EP telecommunications services have been designed around the circuit-switched infrastructure of the Public Switched Telephone Network, evolving converged and NGN are being planned around a packet-switched infrastructure. As technology evolves, it is increasingly clear that support for Emergency Telecommunications Services (ETS) needs to be included in the developing standards. Third generation, beyond wireless networks, as well as packet-switched networks, such as the Internet and the developing IP cable networks, are becoming increasingly more vital to the NS/EP community.

NCS Priority Services Team personnel are working with a number of national and international telecommunications industry standards organizations to ensure that evolving standards continue to support ETS. The ETS initiative designed by the NCS ensures that developing standards continue to support priority for emergency telecommunications regardless of the network topology. Some of the areas ETS addressed are: priority establishment, priority access, dynamic restoration, authentication, security, integrity, and management of emergency telecommunications in converging networks and the NGN.

The OMNCS is an active participant in the International Engineering Task Force (IETF) and T1 for the ETS program. In conjunction with this work, the IETF chartered a working group to examine ways to provide preferential treatment to calls (within the IP environment) in cases in which congestion occurs. In the late 1990s, the OMNCS, in support of NS/EP requirements, completed development of the Enhanced Priority Access and Channel Assignment (PACA-E) Stage 1 description. PACA-E extends PACA to NS/EP users of digital wireless PCS in the 1900-megahertz band and provides for treatment of call egress. The document outlines how it handles a PACA-E call and describes the service's interaction with other existing services.

Nationally, the NCS Technology and Programs Division routinely interacts with the American National Standards Institute Committee T1 for Telecommunications and the Telecommunications Industry Association committees concerning Third Generation Partnership Program. The OMNCS is an active member of the Alliance for Telecommunications Industry Solution Internet work Interoperability Test Coordination Committee which provides the opportunity to participate in industry testing of advanced services such as local number portability and priority services like GETS that are being offered to the NS/EP community via the public telecommunications infrastructure. The OMNCS is also an active participant in the industry forum Parlay, which is developing emergency telecommunications enabled applications programming interfaces for the NGN to include wireless networks.

The OMNCS continues to work in concert with standards-developing organizations to identify, evaluate, and influence those standards that can enhance the communications capabilities of the NS/EP users. Building on its history of partnership and cooperation, the OMNCS recognized the key to sustained success in the standards arena is partnership within National and international standards committees and industry forums, because such partnerships facilitate the inclusion of NS/EP requirements into the commercial marketplace.

TELECOMMUNICATIONS INFORMATION SHARING AND ANALYSIS CENTER

In response to PDD-63, which directed the White House to “consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center,” the NCS's National Coordinating Center for Telecommunications created the Telecommunications Information Sharing and Analysis Center (Telecom-ISAC) in March 2000 to support the responsibilities assigned to the NCS and the NCC by E.O. 12472 and the national CIP goals of industry and Government.

The NCC designed the Telecom-ISAC as an NCC function, under OMNCS oversight, with the specific purpose of: (1) facilitating voluntary collaboration and information sharing among its participants; (2) gathering information on vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, Government, and other sources, and analyzing the data with the goal of averting or mitigating impact upon the telecommunications infrastructure; (3) using data to establish baseline statistics and patterns and maintaining a library of historical data; and (4) sanitizing and disseminating information on accordance with sharing agreements established for that purpose by the Telecom-ISAC participants.⁸⁰ The Telecom-ISAC was the second ISAC established and continues to be the only one with representatives from both industry and Government.

The Telecom-ISAC operations built upon experience gained during the Year 2000 (Y2K) rollover. At that time, the NCC, in coordination with the Y2K Telecommunications Forum, developed a Y2K database to collect and monitor the status of the telecommunications infrastructure throughout the United States during the critical rollover period.⁸¹ In addition, the NCC established procedures and relationships to promote sharing of information related to Y2K. Coordination with the ITU enabled this information sharing to be worldwide. The NCC populated the database with information on Y2K efforts voluntarily reported by the major telecommunications carriers. Organizations signed information sharing agreements before the Y2K rollover, so that during the rollover itself, if companies reported incidents to the NCC, it shared this information with all the participating organizations worldwide.

Telecommunications Information Sharing and Analysis Center

On January 1, 2000, the President's National Coordinator for Security, Infrastructure Protection, and Counter-terrorism established the Telecommunications Information Sharing and Analysis Center (Telecom ISAC) as a function of the National Coordinating Center for Telecommunications (NCC). The Telecom ISAC was established in response to the issuance of Presidential Decision Directive 63 in 1998, which proposed that various sectors of the national economy establish ISACs, including the information and communications sector. The Telecom ISAC builds on the history of cooperation and established trusted relationships among the NCC members. The ISAC is made up of 32 members (29 companies and 3 associations) and facilitates voluntary collaboration and information sharing among its participants by gathering

information on vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, Government, and other sources.

The role of the Telecom ISAC includes analyzing the shared data with the goal of averting or mitigating adverse impacts upon the telecommunications infrastructure. This goal is supported by the Telecom ISAC's 24x7 Watch and Analysis Operation, which became fully functional in September 2001. The 24x7 Watch and Analysis Operation is composed of senior level information assurance analysts. The analysts are closely integrated with the Government NCC operations staff and the Telecom ISAC members, and are fed information by members, Government sources, and other liaison partners. The watch analysts use their technical

expertise to analyze the data supplied to them, and the results are ultimately disseminated as appropriate to help mitigate homeland, national, and economic security threats.

The Telecom ISAC has developed to be a central hub in facilitating the management and resolution of information network incidents. In 2002, for example, the Telecom ISAC provided a member company with its first notification of the NIMDA worm, resulting in the successful defense of the company's networks. That same company, in turn, was the first to notify the ISAC of problems associated with the simple network management protocol. Furthermore, in 2003, the Telecom ISAC assisted in the mitigation of the Blaster Worm and SoBig virus.

Moving forward, the Telecom-ISAC’s mission encompasses “all hazards” with potential to affect the telecommunications sector. Hazards may appear as outages, anomalies, or other events or incidents, including a coordinated attack, in any of the systems that constitute or support the national telecommunications infrastructure. As the Telecom-ISAC addresses these hazards, its primary emphasis is to analyze reported events and symptoms as rapidly as possible in order to avert or minimize impending damage to telecommunications operations. The secondary emphasis of the Telecom-ISAC is to establish causes after the event in order to prevent future recurrences.

Year 2000 Rollover Readiness and Support

The Year 2000 (Y2K) arrived with a great deal of fanfare, yet it was preceded by much apprehension about the stability of critical information networks leading up to the Y2K rollover. The National Coordinating Center for Telecommunications (NCC) was pivotal in ensuring the stability and functionality of critical networks. The NCC developed a Y2K database to collect and monitor the status of the telecommunications infrastructure during the critical rollover period.

Before the actual year-end rollover, the NCC tested its response capabilities. On September 9, 1999, test participants expressed concern that some systems would read the “9999” date code as an

end-of-file command sequence, causing a cascade of malfunctions within the networks. Testing the system involved the coordination of Federal Government agencies and participating telecommunications carriers, and the exchange of Y2K information in real time, confirming the functionality of the NCC Y2K database. The NCC gathered network status information from 47 carriers in 29 countries.

Test participants reported no difficulties, and they benefited from the opportunity to share information and test their procedures for the millennium rollover. In addition to testing the database, test participants tested and validated NCC Y2K response plans.

When the actual Y2K rollover occurred, the Web-based database registered more than 96,000 hits. SBC; Telecom Italia; Telekom Malaysia Berhad; Bell Atlantic and GTE (which merged to become Verizon); Sprint; Belgacom; Portugal Telecom and Saudi Telecom were major system users. In total, 82 companies in 41 countries reported the status of their networks during the Y2K rollover period. Government agencies, including the General Services Administration, Federal Communications Commission, Department of State, and Department of Defense, also participated in the information sharing system.

Part 4

READY TO SERVE

Part 4

Ready to Serve

RESPONSE TO THE SEPTEMBER 11, 2001, TERRORIST ATTACKS

On September 11, 2001, the United States suffered the worst terrorist attack ever perpetrated on the Nation'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.

Thousands of local businesses suffered during and following the attacks, and damage to the World Trade Center area severely impaired the local telecommunications assets of various service providers. The attacks crippled several critical switches, cut important cable lines, flooded cable vaults, and disrupted electricity to the area. Estimates indicate damage to 200,000 voice lines, 100,000 business lines, 3.6 million data circuits, and 10 cellular towers during the attack, causing severe communications congestion for emergency personnel and citizens alike.⁸² Despite the possible damage to their own company's network infrastructure, NSTAC member companies immediately began contacting NCS Deputy Manager Brenton Greene to learn how their companies might assist the NCS in its response efforts.

Immediately, the NCC began non-stop operations to support NS/EP communications between Federal, State, and local responders, to restore damaged communications lines in Arlington, Virginia, and New York City, and to provision new lines for the recovery and investigation activities. The NCC operated at four sites during this time: the NCC, FEMA, the Defense Department's Global Network Operations Support Center headquarters, and one remote continuity of operations location. The NCS further deployed IMAs to three FEMA regional operations centers.

In a typical week, the NCS receives an average of between 80 to 150 new TSP requests, however, in the two week time period following the attacks, the NCS issued more than 500 TSP requests to 46 different organizations, including the 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 the telecommunications companies restored Wall Street capabilities, the NCS continued to issue 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 7000 TSP provisioning and restoration requests were made, nearly 4,200 more than during the same period in the previous year.⁸³

GETS — the priority queuing capability for the PSN, available to eligible users since 1995 — proved its capabilities in the events following the September 11th attacks. The NCS issued over 1,000 new GETS emergency PINs — adding to the 45,000 cards already in circulation — during the two weeks following the attacks to several agencies, including 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 NSA. Of the thousands of GETS calls attempted by national leaders and emergency responders, more than 95 percent saw completion 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 center to coordinate efforts, identify problems, and share information on progress. It coordinated access for telecommunications service providers into the Manhattan “Red Zone” to ensure restoration of NS/EP communications and continued operation and viability of facilities, such as the refueling of emergency generators. 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.⁸⁴

ACTIVITIES POST-SEPTEMBER 11, 2001

The NCS, through the NSTAC, addressed the lessons learned from the unprecedented threat represented by the September 11, 2001, terrorist attacks. 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. Recommendations from the lessons learned included: (1) the need for standard access control procedures at disaster sites; (2) the need to deploy priority services for NS/EP users over wireless networks; (3) support for emergency telecommunications services standards; and (4) the need to protect critical infrastructure information that industry voluntarily shares with Government from disclosure under *The Freedom of Information Act*.⁸⁵

The Changing Threat

From 1945 to 1991, the Cold War dominated international affairs. During that period, the global competition between the United States and the Soviet Union took many forms: political, economic, ideological, and cultural, but overshadowing all was the threat of nuclear war.

One of the most intense stages of the Cold War occurred between 1958 and 1962, punctuated by the Cuban Missile Crisis from which the National Communications System (NCS) was born. When the United States discovered that the Soviet Union had begun secretly installing missile sites in Cuba that could be used to launch nuclear attacks on U.S. cities, the fear of imminent nuclear war gripped Americans.

The fall of the Berlin Wall in 1990 symbolized the end of the Cold War and the diminishing threat of nuclear attack on the United States. Today, however, Americans face a new threat — international terrorism — that the horrific attacks of September 11, 2001 made indelible in our minds. Terrorists seek to inflict mass casualties, both overseas and on American soil. Unlike the nuclear threat, the asymmetric terrorist threats are less dependent on state sponsorship and are, instead, formed through loose, transnational affiliations, making terrorist attacks more difficult to predict and prevent.

In addition to the physical security concerns amplified by the September 11 terrorist

attacks, cyber attacks are a growing concern to Americans. Since the relatively simple viruses of the early 1990s, the destructiveness, pace, and complexity of cyber attacks have increased exponentially. The speed and anonymity characteristic of these cyber attacks make distinguishing among the action of terrorist, criminals, and nation states extremely difficult. By leveraging its unique relationships built with industry and Government partners over 40 years, the NCS is ready to utilize its knowledge and technical capabilities to protect U.S. critical infrastructure and prevent attacks.

When the draft *National Strategy for Homeland Security* was released in September 2002, the NSTAC submitted to the President’s Critical Infrastructure Protection Board suggested revisions from the perspective of its member companies. The NSTAC underscored the need for a market-based approach to securing cyberspace and noted that even passive regulation should be considered a last resort — only when a clearly defined need for the common good could not be satisfied by relying on marketplace forces. The NSTAC welcomed the proposed role of the new Department of Homeland Security (DHS) in information and telecommunications CIP; however, it noted that a major shortcoming of the draft *National Strategy* was underestimation and underutilization of the roles that State and local Governments can play in investigating and prosecuting cyberspace attacks. Further, the NSTAC suggested that State and local Governments rely on the NCC for coordinating communications during disasters. The NCC has accepted this role and worked with State and local entities, since the terrorist attacks, to meet their requirements.

The NSTAC also commented positively on a draft recommendation encouraging Internet service providers to work with antivirus and software manufacturers to make it easier for home users and small businesses to obtain security software and automatic updates and supported a recommendation that the Federal Government review new secure network protocols as they are published to determine if they fill a security gap and are cost-effective to deploy. One of the NSTAC’s most detailed comments involved a proposal to establish a Cyberspace Network Operations Center (Cyberspace NOC) which would facilitate information sharing and coordination among Internet Service Providers, hardware and software vendors, IT security companies, computer emergency response teams, and ISACs. The Cyberspace NOC would monitor the health of the Internet and serve as a physical center or virtual information system.⁸⁶

CIP, network vulnerability, and infrastructure dependencies were also primary topics of NSTAC study in the early 2000s. Lessons learned from the September 11, 2001, response efforts led the NSTAC to study risks associated with consolidated telecommunications assets in telecom hotels, trusted access to critical facilities, and vulnerabilities in pervasive software and protocols used over the telecommunications networks. More recent studies have also focused on the security of NS/EP communications over satellite networks and on trusted access to facilities through improved background check processes.⁸⁷

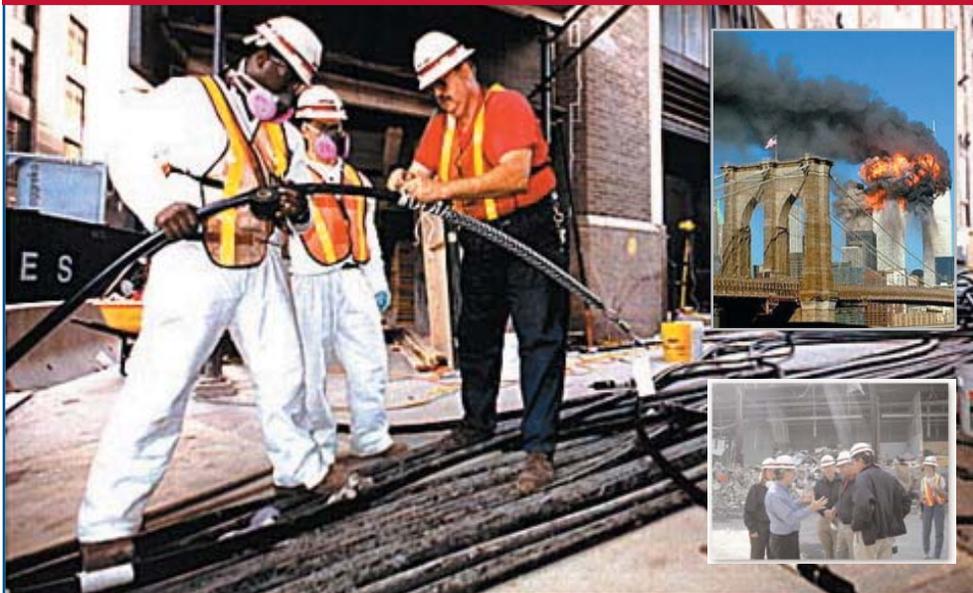
The NSTAC also performed information assurance risk assessments over a several year time period for the electric power, financial services, and transportation sectors. Most recently, the NSTAC established the Financial Services Task Force to define areas of critical concern to the financial services sector; determine

whether or how the telecom industry meets or addresses these concerns; and identify issue commonalities with other sectors.

**PROGRAMS
POST-SEPTEMBER 11, 2001**

The changing threat environment that has evolved from the terrorist attacks of September 11, 2001, has both raised awareness of the importance of the NCS programs and caused the NCS to update its existing programs and develop new programs to address the new homeland security concerns. In the

Following the September 11, 2001, terrorist attacks, Verizon employees worked to restore telecommunications services. Photos courtesy of Verizon.



immediate aftermath of the attacks, TSP had a key role in provisioning and restoring the telecommunication infrastructure, while GETS proved to be an invaluable program for connecting critical NS/EP personnel and Government officials during times of heavy network congestion. The reinforced value of both TSP and GETS instigated a renewed interest in the WPS program, enabling the program to reach Initial Operating Capability (IOC). Furthermore, the attacks provided the necessary momentum to return the CWIN program to the forefront of the President’s agenda. Lastly, the attacks highlighted the need for the development of two new programs, the Global Early Warning Information System (GEWIS) and the Emergency Notification System (ENS), to better address NS/EP concerns in the changing threat environment.

TELECOMMUNICATIONS SERVICE PRIORITY

In the wake of the September 11, 2001, terrorist attacks, the NCS Office of Priority Telecommunications (OPT), which houses the TSP program, played a significant role in the Nation’s response and recovery efforts. As the need for priority treatment of NS/EP communications capabilities was apparent, the number of TSP provisioning and restoration requests tripled in the months following the attack — during that period the OPT processed almost 5,000 provisioning and restoration requests.

Widespread awareness of TSP’s role in business continuity planning, the ongoing war on terrorism, and the OMNCS critical infrastructure rebuilding efforts drive the considerable increase in TSP Program recipients and TSP requests. As a result, the OPT is currently responsible for more than 50,000 TSP priority communications assignments. In the past year, the TSP user base added 70 new organizations, following significant increases in program awareness in the financial sector and State and local Governments.

The emphasis on reaching State and local NS/EP personnel, first responders, and private sector entities sponsored by Federal agencies, such as financial institutions, is evidenced by the OPT’s extensive TSP outreach and training initiatives, providing comprehensive TSP training to potential vendors, Federal, State, and local users, and emergency response coordinators. As the NCS joins DHS, it expects increased TSP Program participation from all critical infrastructures and Federal, State and local agencies and departments.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICES

Since the implementation of GETS’s operational capability, subscribers successfully used the program in a number of emergency situations. However, the breadth of GETS effectiveness endured a severe test during the terrorist attacks. On September 11, 2001, and in the days following, there were more than 18,000 GETS calls worldwide, with more than 10,000 in the New York City and Washington, D.C. areas. Callers completed 95 percent of 4,000 GETS calls placed to and from Manhattan immediately following the attacks and during the first week, despite heavy network congestion.

Salt Lake City Olympics

<p>In February 2002, the National Communications System (NCS) implemented an emergency Wireless Priority Service (WPS) capability as part of national security and emergency preparedness (NS/EP) communications planning and readiness efforts during 2002 Winter Olympic Games in Salt Lake City, Utah. Working with</p>	<p>the Federal Emergency Management Agency, the NCS mobilized Individual Mobilization Augmentees and NCS staff to provide emergency communications support during the Games. The WPS solution for the Olympics involved using enhanced satellite services, increased trunking, redirection of wireless user calls away from</p>	<p>congested areas, and supplemental wireless communications capabilities programmed on satellite communication handsets. Although NS/EP personnel did not need to use WPS for actual emergencies, response personnel were fully equipped to manage communications in the event of a crisis situation.</p>
--	---	--

The NCS saw similar completion rates with another 3,000 calls made in Arlington, Virginia over the same time period. Over 1,000 new GETS cards were issued from September 11, 2001, to September 28, 2001, adding to the 45,000 cards already in circulation at the time. More than 1,500 personnel utilized the service during this 17-day span to support emergency response efforts. Immediately following this period, GETS reached its full operating capability on September 30, 2001. In the time since the terrorist attacks, GETS interest continues growing, with a 40 percent increase in the number of GETS cards issued and a 35 percent increase in the number of organizations subscribing to the system.

WIRELESS PRIORITY SERVICE

The events of September 11, 2001, reinforced the value of TSP and GETS in emergency situations. However, the events of that day also made clear that the Nation needed a priority service delivered via wireless technologies to facilitate NS/EP communications in the event of damage to wireline networks. The NCS first identified this need after Federal emergency communications coordinators, along with other Federal, State, and local responders, encountered frequent blocking of cellular calls when responding to Hurricanes Andrew and Iniki in 1992. After renewed interest by President Bush and the first responder community following September 11, 2001, WPS became an operational reality.

To provide an immediate solution, the NCS negotiated with WPS service providers, T-Mobile (previously VoiceStream) and Globalstar. Tested in February 2002 at the Olympic Winter Games in Salt Lake City, the first full WPS deployment occurred in Washington, D.C., and New York City in May 2002. By November 2002, T-Mobile supported 2,084 WPS users in Washington and 725 in New York, for a total of 2,809 WPS cellular users, and Globalstar supported 1,506 customers.

Nationwide WPS is a more comprehensive wireless priority capability, which will include additional service providers. Beginning December 31, 2002, the Nationwide IOC consists of priority radio channel access at call origination. Nationwide FOC, which will offer increased probability of call completion during

times of widespread network congestion, will be implemented as soon as possible. The NCS is currently involved in the design and implementation of the WPS 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. The WPS FOC is projected to be an end-to-end service fully integrated with GETS. The NCS is also making the WPS user base, including State and local Governments and NS/EP entities, more aware of the service and its benefits.⁸⁸

Government Emergency Telecommunications Services card distribution growth from 1994 to 2002.



CRITICAL INFRASTRUCTURE WARNING INFORMATION NETWORK

The attacks on September 11, 2001, also highlighted vulnerabilities of the cyber information infrastructure on which both industry and the Government rely, and brought CWIN to the forefront of the Nation's critical infrastructure protection agenda. Several years in advance of the attacks, the NCS had explored the development of technical specifications and cost requirements for a system to facilitate immediate alert and notifications for threats to the cyber network to industry and Government partners. As a result, the NCS developed CWIN to provide a non-PSN-switched, non-Internet, private voice and data network with assured reliability under emergency conditions.

With CWIN, the NCS worked to:

- Develop a classified communications network among key Federal Government facilities;
- Develop an unclassified communications network among key Federal Government and industry sites;
- Develop operational procedures for information sharing;
- Administer installation of CWIN terminals at key Government and industry sites; and
- Train Government and industry authorized staff on CWIN use and procedures.

In May 2001, the NCS began responding to a White House request to plan and execute the deployment and operational management of CWIN. Beginning in mid-FY 2002, the NCC began deployment of a dedicated network to support CWIN operations at several existing and geographically dispersed Federal watch centers to include cyber operational elements of the Government, private corporations, and ISACs. In the *National Strategy to Secure Cyberspace*, February 2003, the President emphasized the need to expand the functions of the existing CWIN program to provide support to the DHS in coordinating crisis management for cyberspace.⁹⁰ The *National Strategy* emphasized that given the time constraints in an emergency situation, improved national cyber warning capabilities are essential. The enhanced CWIN program will serve the purpose of sharing alert and warning information with industry and Government. As the importance of securing the Nation's cyber network continues to grow, CWIN's role and importance in cyber security will continue to evolve.⁸⁹

GLOBAL EARLY WARNING INFORMATION SYSTEM

The September 11, 2001, terrorist attacks highlighted the need for increased awareness of threats to the Nation's critical infrastructure. The NCS began work on GEWIS following the terrorist attacks to meet this need through creating a "real-time" picture of potential threats throughout the cyber infrastructure. Still in the development stage, GEWIS is a prototype health assessment tool to provide information for early detection of significant Internet/inter-network performance events and anomalies, then corroborate the information and build 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.⁹¹

EMERGENCY NOTIFICATION SYSTEM

The events of September 11, 2001, demonstrated the need for the general population to be informed in times of crisis. To meet this need, the NCS is developing a national system to provide emergency notification or alerts to the general public. This new system, known as the ENS, will facilitate interoperability across existing systems, provide for data collection across infrastructures, 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 the service confirms delivery or until it makes a predetermined number of attempts to deliver its message.

ENS is currently operating as a pilot program, composed of three phases slated between October 2002 and October 2003. The goal is for the ENS notification program to include between “2,000-6,000 critical NS/EP personnel at top levels of Government, as well as between 50,000-250,000 Federal, State, and local Government and other public health and safety personnel.” The successful rollout of the ENS program will improve the general public and the Government’s ability to effectively respond to emergencies.⁹²

The President’s Strategies

Since the American populace became aware of homeland security concerns following the events of September 11, 2001, President George W. Bush has released a series of national

strategies aimed at providing guidance for the Nation’s homeland security efforts.

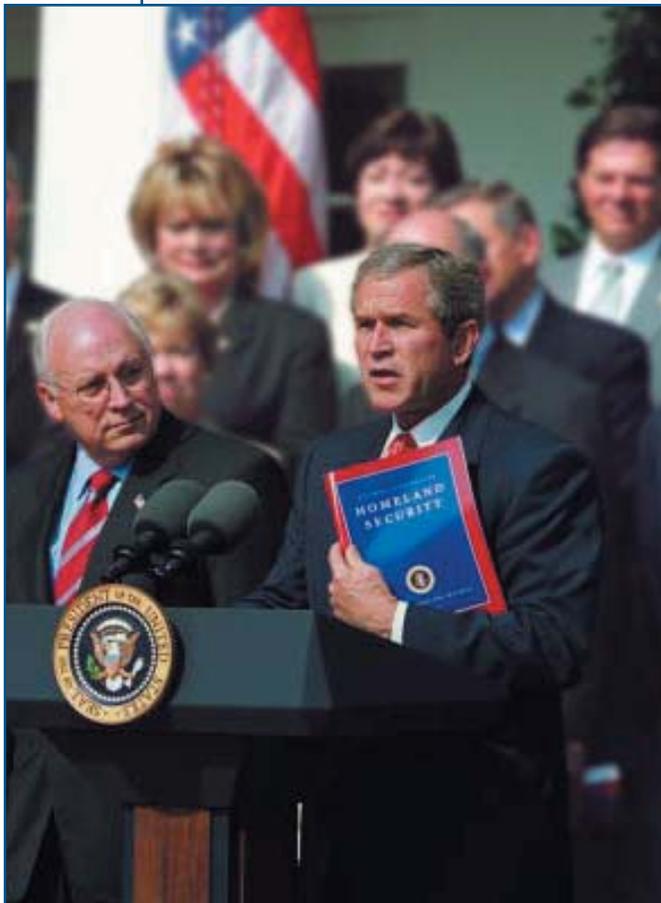
The Government released the first of the three strategies, the *National Strategy for Homeland Security*, in July 2002. This document outlines strategies and goals for improving homeland security and creates a foundation for organizing national security efforts at the Federal, State, and local levels.

To complement the first strategy, the White House released the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, in February 2003. This strategy identifies goals and outlines principles that will guide

nationwide efforts to secure critical infrastructures and assets vital to our public health and safety, national security, governance, economy, and public confidence.

Lastly, the White House released *The National Strategy to Secure Cyberspace* in February 2003. This strategy responds directly to the evolving cyber threat and relies heavily on leveraging existing public-private partnerships to secure the Nation’s critical infrastructures while building new partnerships. The President’s National Security Telecommunications Advisory Committee provided direct input into the creation of the strategy, working with White House personnel to ensure that the strategy is actionable and effective.

These documents are not expected to provide the complete script for securing the homeland; but collectively, they establish a means of focusing efforts towards a common goal.



CHANGES IN THE FEDERAL GOVERNMENT

Since September 11, 2001, the Federal Government has reexamined how best to contend with threats against our homeland. In October 2001, President Bush created the Office of Homeland Security (OHS) within the E.O.P. as the focal point for domestic security, and appointed Governor Tom Ridge from Pennsylvania to head the new office. After careful study, the OHS found responsibilities for homeland security dispersed among dozens of different agencies and identified a significant need to create a single Department with a single mission of homeland security.

Consequently, in a June 2002 national address, the President proposed the creation of the DHS, a Cabinet-level agency with a clear mission to serve as a “single, unified homeland security structure that will improve protection against today’s threats and be flexible enough to help meet the unknown threats of the future.”⁹³ The DHS serves as the central point for coordination and communication with State and local Governments, the private sector, and the public, and is to develop a major intelligence analysis capability to support homeland security operations. The Administration recommended the NCS transfer to the proposed DHS, along with the homeland security assets of the Departments of the Treasury, Justice, Commerce, Transportation, Energy, Health and Human Services, and FEMA.

In subsequent months, the Bush Administration continued to strengthen homeland defense by releasing the *National Strategy for Homeland Security*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, and the *National Strategy to Secure Cyberspace* as an overarching framework and guidance to Federal, State, and local Governments, the private sector, and the public for homeland security. The strategies helped the country’s leaders in both the public and private sectors to refocus on the need for stringent physical security, particularly, around critical infrastructures. The President emphasized the importance of securing the Nation’s cyber-related capabilities and assets, and publicized the NCS’s capabilities and functions as strengths in the Federal Government’s fight against terrorism.

After months of Congressional deliberation, the President signed *The Homeland Security Act of 2002* into law on November 25, 2002, resulting in the largest Government reorganization in half a century. The new law also signified the beginning of a new era for the NCS and its staff. After almost 40 years of dedicated service under the auspices of the Defense Department, the NCS would continue its mission to serve the Nation as a vital component of the new DHS.

THE NATIONAL COMMUNICATIONS SYSTEM IN THE DEPARTMENT OF HOMELAND SECURITY

Looking forward, the NCS will have enhanced opportunities as part of the DHS to continue serving the NS/EP community and protecting the Nation’s communications infrastructure. As a component of the Information Analysis and Infrastructure Protection Directorate (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 basis from which to organize protective measures to secure the homeland.

DHS officials selected the NCS for the IAIP because of the unique capabilities and assets it brings to the Directorate. The NCS’s experience in infrastructure protection and assurance, its watch center capabilities, its suite of National-level programs providing priority telecommunications services to the NS/EP community, and its strong industry relationships that have burgeoned through the NCC, Telecom-ISAC, and the NSTAC will all help enhance the IAIP and the DHS mission.

In response to President Bush’s proposal to create the new Department during his June 6, 2002, national address, the NCS immediately established a team to manage the transition process. This team worked transition issues and coordinated with the DHS Transition Planning Office (TPO), which was established by E.O. 13267, *Establishing a Transition Planning Office for the Department of Homeland Security Within the Office of Management and Budget*, on June 20, 2002.

In addition to responding to requests for information from the TPO, the transition team played an important role in educating officials involved in structuring the new Department on the NCS’s unique mission, programs, and National-level functions. The NCS Deputy Manager, Brenton Greene, and members of the transition team also worked closely with the other agencies entering the directorate early on to formulate strategies for how their capabilities could best be combined to execute the directorate’s mission. Other agencies selected to become a part of the new directorate included: the NIPC, the CIAO, the Federal Computer Incident Response Center, the DOE’s National Infrastructure Simulation and Analysis Center, and Energy Security and Assurance Program.

After President Bush signed the *Homeland Security Act of 2002* and DHS officials established a transition timeline, the NCS formed a transition operations working group to address specific transition topics. The working group monitored and initiated the transition of items including: information technology and communications, website, contracts and budgets, security clearances, personnel, and facilities. Meeting frequently, the working group ensured the NCS would have a smooth transition into the new Department.

The functions of the NCS, and other agencies entering the IAIP Directorate, officially transferred to the DHS on March 1, 2003. That week, the NCS held a ceremony to the transfer the Executive Agent responsibilities of the NCS from the Department of Defense to DHS. Former Managers, Deputy Managers, industry partners, and OMNCS employees were on hand to commemorate the occasion. In a passing of colors ceremony, Air Force Lieutenant General Harry D. Raduege, Jr., transferred the Executive Agent responsibilities to the DHS.

Executive Order Changes

<p>The terrorist attacks of September 11, 2001, shifted the Nation’s agenda to focus on new threats to the Nation’s homeland security. To meet the new homeland security requirements, the President enacted <i>The Homeland Security Act</i> on November 25, 2002, which established the Department of Homeland Security (DHS) and set into motion a major reorganization of the Government departments and agencies. As part of the reorganization plan, President Bush designated the NCS and its programs for transfer into the new department.</p>	<p>On February 28, 2003, President Bush enacted this transfer into law by signing omnibus Executive Order (E.O.) 13286, <i>Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security</i>, which transferred certain functions of various departments and agencies to the Secretary of Homeland Security. The omnibus E.O. included two E.O.’s related to functions of the NCS and its programs, changing them as follows:</p>	<p>E.O. 12472, <i>Assignment of National Security and Emergency Preparedness Telecommunications Functions</i>: Changed the Executive Agent of the NCS from the Secretary of Defense to the Secretary of Homeland Security and added homeland security objectives to the NCS mission.</p> <p>E.O. 12382, <i>President’s National Security Telecommunications Advisory Committee</i>: Added language requiring recommendations to the President to be forwarded through the Secretary of Homeland Security.</p>
---	--	---

In his remarks following the transfer, Army Major General Bruce Lawlor, the DHS Chief of Staff commented on the thought process behind the development of the Directorate: “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 also marked the end of the transition process and the beginning of the difficult task of integrating the capabilities of the NCS and the other five agencies.⁹⁴

On February 28, 2003, President Bush signed an omnibus of executive orders related to the transfer of many Government functions and activities to the new Department. Two of the executive orders and a new Homeland Security Presidential Directive 5 (HSPD-5) had direct bearing on for the NCS mission. E.O. 12472 was amended to state that the NCS Executive Agent would now be the Secretary of Homeland Security, and E.O. 12382 was amended to state that the NSTAC would also report to the President through the Secretary of Homeland Security. HSPD-5 ensures “that national security and emergency preparedness telecommunications services will be available in times of crisis for the President, other national leaders, and the emergency preparedness and response community.”

Over time, the NCS will integrate more of its functions into the IAIP Directorate and will take on additional roles, but it will continue to execute its Presidentially mandated mission to ensure the availability of NS/EP telecommunications to support national decision makers during times of crisis, as it has done for four decades.

CONCLUSION

For forty years the NCS has helped to protect our Nation’s critical telecommunications infrastructure. Through the years, it has adapted to the meet the ever-changing needs of our society and sought to ensure interoperable and survivable lines of communication are available to our leaders and first responders at all times.

Since its inception 40 years ago, the NCS has strengthened our country’s telecommunications infrastructure and ensured its safety. The core mission remains unchanged: *to protect our critical telecommunications infrastructure and provide the President with the necessary information to enable his informed decisions for telecommunications and NS/EP policy.*



APPENDIX

END NOTES

- 1 The White House, Memorandum, "Cabinet Agenda for Friday, January 25, 1959, Item B: The Development of a Unified Federal Civilian Communications System," January 20, 1959.
- 2 The White House, E.O. 10995, "Assigning Telecommunications Management Functions," February 16, 1962. The position of Director of Telecommunications Management was to be held by an Assistant Director of the Office of Emergency Planning.
- 3 National Security Action Memorandum 201 (NSAM-201), "Establishment of the Subcommittee on Communications," October 26, 1962.
- 4 The White House, Memorandum to the Heads of Executive Departments and Agencies, "Establishment of the National Communications System," August 21, 1963. This August 21 Memorandum was preceded by National Security Action Memorandum 252 (NSAM-252), July 11, 1963, which was identical to the August 21 memo except for one brief reference to the Central Intelligence Agency (CIA).
- 5 "Procedures and Working Relationships."
- 6 DOD Directive 5100.41.
- 7 LTG Alfred D. Starbird, Manager, NCS, to Executive Agent, NCS, "Submission of First Annual NCS Long-Range Plan," August 12, 1964.
- 8 Letter, James D. O'Connell, Jr. to Robert S. McNamara, October 1, 1965.
- 9 E.O.P., Office of Emergency Preparedness, *The National Plan for Emergency Preparedness*, December 1964, p. 55.
- 10 NCS Instruction 45-1 (NCSI 45-1), "NCS Operations Center Organizational Arrangements and Structure," July 28, 1965. Interim instructions had been issued the previous year in NCS Circular 130-2 (NCSC 130-2), "Interim Procedures for Processing CS Emergency Telecommunications Circuit Requirements," January 24, 1964, and approved by President Johnson in a Memorandum to Secretary McNamara on August 27, 1964. Related documents during this time period include: NCS Circular 70-1 (NCSC 70-1), "Operating Procedures for the NCS," June 22, 1964; NCS Instruction 55-1, "Procedures for Placing Into Effect the NCS Private Line Circuit Restoration Priority System," January 18, 1965; NCSC 70-2, *Technical Standards Manual*, March 1968; NCSC 70-3, "Performance Objectives for the NCS," August 13, 1968.
- 11 NCS, "Second Long-Range Plan for the National Communications System for Fiscal Year (FY) 1968-1972," July 27, 1966.
- 12 NCS, "Second Long-Range Plan for the National Communications System for FY 1968-1972," July 27, 1966.
- 13 Robert S. McNamara, Memorandum for the President, "Submission of the Second Annual Long-Range Plan for the NCS, FY 1968-1972," July 27, 1966.
- 14 Letter, J.D. O'Connell to Robert S. McNamara, October 31, 1966.
- 15 Letter, J.D. O'Connell to Melvin Laird, June 2, 1969.
- 16 Letter, LTG Richard P. Klocko, Manager, NCS, to William H. Goodman, Deputy Assistant Secretary of State for Communications, April 12, 1968. General Klocko envisioned a three-stage development for the NCS, beginning with what was available now, progressing through a step-by-step interconnection process, and ending with complete interoperability.
- 17 Ibid.
- 18 Letter, J.D. O'Connell to Clark M. Clifford, June 2, 1969.
- 19 NCS, *National Communications System Long-Range Development Concept*, February 11, 1971.
- 20 Ibid.
- 21 President's Task Force on Communications Policy, Final Report, December 7, 1968.
- 22 GAO, *Review of Status of Development Toward Establishment of a Unified National Communications System*, July 14, 1969.
- 23 White House Memorandum, Peter Flanigan to Melvin R. Laird, December 6, 1969.
- 24 The White House, E.O. 11556, "Assigning Telecommunications Functions," September 4, 1970.
- 25 Letter, Clay T. Whitehead to Robert M. O'Mahoney, February 8, 1972.
- 26 NCS Memorandum to Executive Agent, NCS, "NCS Long-Range Planning," April 12, 1972.
- 27 Letter, Clay T. Whitehead to E. Reichtin, May 25, 1972.
- 28 Letter, Executive Agent, NCS, to Clay T. Whitehead, Director, OTP, April 21, 1972.
- 29 The White House, E.O. 11490, "Assigning Emergency Preparedness Functions to Federal Departments and Agencies," October 30, 1969.
- 30 NCS Summary Plan, May 1972.

<p>31 National Communications System Circular 175-1 (NCSC 175-1), "Federal Telecommunications Standards Program," June 6, 1973.</p>	<p>Directive 47 (NSDD-47), "Emergency Mobilization Preparedness," July 22, 1982, defined preparedness policy and further identified the role of the EMPB. In reference to communications, NSDD-47 stated that it is "the policy of the United States to ensure that communications resources be available and adequate to respond to the Nation's needs."</p>
<p>32 National Communications System, Office of the Manager, NCS Instruction 205-1 (NCSI 205-1), "Reporting of Significant Telecommunications Research and Development Activities of the NCS Operating Agencies," March 29, 1976.</p>	<p>46 The White House, E.O. 12382, "President's National Security Telecommunications Advisory Committee," September 13, 1982. A forerunner of NSTAC was the short-lived National Security Council Advisory Board, formed in July 1981, and consisting of top executives from the common carriers. See National Security Council Memorandum, July 23, 1981.</p>
<p>33 Office of Telecommunications Policy, "Ad Hoc Review Group for Organization for Telecommunications within the Executive Branch," February 9, 1976, prepared by Charles C. Joyce, Jr.</p>	<p>47 The White House, National Security Decision Directive 97 (NSDD-97), "National Security Telecommunications Policy," August 3, 1983.</p>
<p>34 Ibid.</p>	<p>48 The White House, Memorandum for the Chairman, FCC, et al., "The National Communications System," October 7, 1983. A 23rd member, the Department of Health and Human Services, was added in 1987.</p>
<p>35 The White House, E.O. 12046, "Relating to the Transfer of Telecommunications Functions," March 27, 1978.</p>	<p>49 The White House, E.O. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984.</p>
<p>36 Ibid.</p>	<p>50 Ibid., Section 4, paragraph (b)(2).</p>
<p>37 Memorandum, National Security Council (Zbigniew Brzezinski) to Secretary of Defense, "Telecommunications and C3I Policy Issues," August 10, 1979.</p>	<p>51 NCS, "Highlights of Manager/Representatives Meeting, 20 December 1971," and "Manager, NCS/NCS Agency Principals Meeting, 28 January 1972," February 7, 1972.</p>
<p>38 Memorandum of Understanding Between the NSC, the OSTP, and the Executive Agent, NCS, June 5, 1978. See also, The White House, Memorandum for Heads of Departments, Agencies, etc., "National Security and Emergency Preparedness Telecommunications Management and Coordination Responsibilities," July 5, 1978.</p>	<p>52 NCS, <i>Organization and Functions Manual</i>, Office of the Manager, NCS, August 1978.</p>
<p>39 Presidential Directive 53 (PD-53), "National Security Telecommunications Policy," November 15, 1979.</p>	<p>53 NCS, "NCS Organization and Functions," June 1982.</p>
<p>40 Ibid.</p>	<p>54 NCS, <i>NCS FY 1998 Annual Report</i>, pp. 19-23.</p>
<p>41 Office of Telecommunications Policy. "Ad Hoc Review Group for Organization for Telecommunications within the Executive Branch," February 9, 1976, prepared by Charles C. Joyce, Jr. p. 35.</p>	<p>55 NCS, <i>NCS FY 1994 Annual Report</i>, p. 2-29.</p>
<p>42 The White House, E.O. 12046, "Relating to the Transfer of Telecommunications Functions," March 27, 1978.</p>	<p>56 Cohen, Michael L., "Government Communications in the Nuclear Age: Attempts to Develop a Nationwide Emergency Telecommunications Service," April 25, 1991. The unpublished manuscript traces the evolution of, and need for, a national emergency communications system during and after the Cold War, and presents some of the possible reasons why, after 30 years, the system first proposed by President Kennedy in 1963 has yet to be realized.</p>
<p>43 Ibid.</p>	<p>57 Ibid., pp. 53-57.</p>
<p>44 The term, "National Security and Emergency Preparedness Telecommunications," was first used in a Memorandum from the White House in July 1978. See White House to Executive Offices, "National Security and Emergency Preparedness Telecommunications Management and Coordination Responsibilities," July 5, 1978.</p>	
<p>45 The EMPB was established by Memorandum in December 1981. National Security Decision</p>	

58	Subcommittee Report to the NCS COP, "Review of the National Level NS/EP Telecommunications Program," May 29, 1990. See also Cohen, "Government Communications," pp. 86-88.	72	NCS, NCS FY 1992 Annual Report, pp. 2-15 to 2-21.
59	Panel of Experts Report to the Manager, NCS, "National Level NS/EP Telecommunications Program (NLP) Review," October 1991, pp. 48-53.	73	The "Mother's Day Phenomenon" is the almost yearly occurrence of an abnormally high number of telephone calls on Mother's Day. The calls flood the network, hindering access to circuits for priority users.
60	The White House, Memorandum for Executive Agent, NCS, "National Level Telecommunications Program Implementation and Functional Requirements," October 15, 1991.	74	NSTAC, Issue Review, December 1997, pp. 15-18.
61	The White House, E.O. 12864, "United States Advisory Council on the National Information Infrastructure (NII)," September 15, 1993.	75	Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States, March 20, 1995.
62	United States NII Virtual Library, co-sponsored by the President's Information Infrastructure Task Force and the Council on Competitiveness. Uniform Resource Locator: http://nii.nist.gov .	76	Letter from the President of the United States to the NSTAC, July 7, 1995.
63	E.O. 12472, April 3, 1984.	77	Ibid.
64	The White House, <i>Creating a Government that Works Better & Costs Less</i> , Report of the National Performance Review, September 7, 1993.	78	E.O. 13010, "Critical Infrastructure Protection," July 15, 1996.
65	Director, OSTP Memorandum, <i>National Security and Emergency Preparedness</i> , June 11, 1993.	79	See NIITF Final Report, March 1997; IATF Electric Power Risk Assessment, March 1997; IIG Financial Services Risk Assessment, October 1997; RVWG, <i>A Nation's Information at Risk: NII Risk Assessment</i> , February 1996.
66	As part of the NCS Vision 21 Total Quality Management Process established by the COP, three focus teams, or task forces, were formed to address 12 issues identified by the COP at their off-site meeting in October 1994. Focus Team 1, named to address NCS Process/Services/Image, concentrated on developing a process for selecting a COP Vice Chair. The team also identified opportunities for presenting NCS-related information to senior Federal Government officials and State and local emergency coordinators. Focus Team 2, Interoperability/Emerging Technology, researched and monitored Federal network security activities, emerging technologies, and satellite services available to the NCS during emergencies. Focus Team 3 concentrated on the NII, and identified potential Federal, State, and local NS/EP customers of the NII.	80	The National Coordinating Center for Telecommunications Homepage, www.ncs.gov/ncc .
67	During an off-site meeting in October 1994, the COP developed this vision statement, as documented in the NCS Strategic Plan.	81	NCS, NCS FY 2000 Annual Report, p. 15-III.
68	NCS, <i>Strategic Plan</i> , January 1996, p. 3.	82	The Verizon Service Standard, Issue Number 4, October 11, 2001, www.verizon.com .
69	Ibid., p. 5.	83	NCS Telecommunications News, NSTAC Special Edition 2003, "National Security Telecommunications Advisory Committee Plays a Significant Role in Emergency Services and Homeland Security."
70	OMNCS, <i>Disaster Area Architecture, Baseline Architecture and Near-Term Enhancement Report</i> , April 1995.	84	NCS, NCS FY 2001 Annual Report, p. 4-15.
71	NCS, NCS FY 1996 Annual Report, p. 3-3.	85	Letter from the NSTAC to the President of the United States, December 12, 2001.
		86	NSTAC Input to <i>The President's National Strategy to Secure Cyberspace</i> .
		87	See the 2003 NSTAC reports on the NCS website at www.ncs.gov .
		88	NCS Web site, www.ncs.gov .
		89	Ibid.
		90	<i>The President's National Strategy to Secure Cyberspace</i> , February 2003.
		91	NCS Web site, www.ncs.gov .
		92	Ibid.

<p>93 Remarks by the President of the United States in Address to the Nation, http://www.whitehouse.gov/news/releases/2002/06/20020606-8.html.</p>	<p>94 NCS Telecommunications News 2003-01, "National Communications System Transfers to the Department of Homeland Security."</p>
---	--

ACRONYMS

	A		
ACN	Alerting and Coordination Network	ERLink	Emergency Response Link
ADP	Automatic Data Processing	ERT	Emergency Response Training
AIN	Advanced Intelligent Network		
AIP	Automated Information Processing		F
AUTOVON	Automatic Voice Network	FAA	Federal Aviation Administration
		FBI	Federal Bureau of Investigation
		FCC	Federal Communications Commission
		FedCIRC	Federal Computer Incident Response Center
	C	FEMA	Federal Emergency Management Agency
CCPC	Civil Communications Planning Committee	FOC	Full Operating Capability
CCS	Common Channeling System	FRP	Federal Response Plan
CDMA	Code Division Multiple Access	FTS	Federal Telecommunications System
CEPTAG	Civil Emergency Planning Committee		
CIA	Central Intelligence Agency		G
CIAO	Critical Infrastructure Assurance Office	GAO	General Accounting Office
CIP	Critical Infrastructure Protection	GETS	Government Emergency Telecommunications Service
CIWG	Critical Infrastructure Working Group	GEWIS	Global Early Warning Information System
CNS	Commercial Network Survivability	GSA	General Services Administration
COP	Committee of Principals	GSM	Global Systems for Mobile Communications
COR	Council of Representatives		
CPAS	Cellular Priority Access Service		H
CSI	Commercial Satellite Communications Interconnectivity	HF	High Frequency
CSS	Commercial Satellite Survivability	HSD	Homeland Security Directive
CTF	Convergence Task Force		
CWIN	Critical infrastructure Warning Information Network		I
		IAIP	Information Analysis and Infrastructure Protection
	D	IATF	Information Assurance Task Force
DCA	Defense Communications Agency	IES	Industry Executive Subcommittee
DCS	Defense Communications System	IIG	Information Infrastructure Group
DHS	Department of Homeland Security	IITF	Information Infrastructure Task Force
DISA	Defense Information Systems Agency	IMA	Individual Mobilization Augmentees
DMAC	Deputy Manager Advisory Committee	IMT-2000	International Mobile Telecommunications-2000
DOD	Department of Defense	IP	Internet Protocol
DOE	Department of Energy	IPT	Integrated Product Team
DOJ	Department of Justice	ISAC	Information Sharing and Analysis Center
DOS	Department of State	ISP	Internet Service Provider
DTM	Director of Telecommunications Management	ITU	International Telecommunication Union
		IWG	Interoperability Working Group
	E		
ECC	Executive Coordination Committee		M
ECWG	Emergency Communications Working Group	MARS	Military Affiliate Radio System
EMP	Electromagnetic Pulse		
E.O.	Executive Order		
EOC	Emergency Operations Center		
E.O.P.	Executive Office of the President		
ERFAK	Emergency Response Fly-Away Kit		

BIBLIOGRAPHY

GENERAL LITERATURE

15 Years of Serving the President: 1982-1997. NSTAC Fifteenth Anniversary Publication, December 1997.

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company, 1971.

Bundy, McGeorge. *Danger and Survival*. New York: Vantage Books, 1990.

Koenig, Louis W. *The Chief Executive*. New York: Harcourt, Brace & World, 1964.

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Mac Millan Company, 1967.

Loomis, Richard T. *A History of the National Communications System: The First 25 Years, 1963-1988*. McLean, VA: The MITRE Corporation, 1990.

Erskine, George, and Joan Sulek. *The Evolving Framework for Federal National Security Emergency Preparedness Telecommunications Management*. McLean, VA: The MITRE Corporation, 1985.

National Research Council Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications. *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*. Washington: National Academy Press, 1989.

The President's National Security Telecommunications Advisory Committee, *Issue Review*, December 1997.

The President's National Security Telecommunications Advisory Committee, *Issue Review*, July 2001.

Sorenson, Theodore C. *Kennedy*. New York: Harper and Row, 1965.

Temin, Peter. *The Fall of the Bell System: A Study in Prices and Politics*. Cambridge, MA: University Press, 1987.

Thirty Years of Progress. *The Thirtieth Anniversary History of the National Communications System*. Washington, DC, 1993.

Weintal, Edward, and Charles Badett. *Facing the Brink: An Intimate Study of Crisis Diplomacy*. New York: Charles Scribner's Sons, 1967.

The Verizon Service Standard, Issue Number 4, October 11, 2001, www.verizon.com.

ANNUAL REPORTS

NCS Annual Reports, 1974-2002.

NCS National Level National Security and Emergency Preparedness Telecommunications Program for Fiscal Years 1986-1993.

EXECUTIVE ORDERS

E.O. 10995, "Assigning Telecommunications Management Functions," February 16, 1962.

E.O. 11490, "Assigning Emergency Preparedness Functions to Federal Departments and Agencies," October 30, 1969.

E.O. 11556, "Assigning Telecommunications Functions," September 4, 1970.

E.O. 12046, "Relating to the Transfer of Telecommunications Functions," March 27, 1978.

E.O. 12127, "Federal Emergency Management Agency," March 31, 1979.

E.O. 12382, "President's National Security Telecommunications Advisory Committee," September 13, 1982.

E.O. 12472, "Assignment of National Security and Emergency Preparedness Functions," April 13, 1984.

E.O. 12656, "Assignment of Emergency Preparedness Responsibilities," November 18, 1988.

E.O. 12862, "Setting Customer Service Standards," September 11, 1993.

E.O. 12864, "United States Advisory Council on the National Information Infrastructure," September 15, 1993.

E.O. 13010, "Critical Infrastructure Protection," July 15, 1996.

E.O. 13267, "Establishing a Transition Planning Office for the Department of Homeland Security Within the Office of Management and Budget," June 2002.

WHITE HOUSE DIRECTIVES

NSAM-66, *National Military Command System*, June 1962.

NSAM-201, *Interdepartmental Committee on Communications*, October 26, 1962.

NSAM-252, *Establishment of the National Communications System*, July 11, 1963.

E.O.P, *The National Plan for Emergency Preparedness*, December 1964.

PD-53, *National Security Telecommunications Policy*, November 15, 1979.

NSDD-26, *US Civil Defense Policy*, March 16, 1982.

NSDD-47, *Emergency Mobilization Preparedness*, July 22, 1982.

NSDD-85, *Eliminating the Threat from Ballistic Missiles*, March 25, 1983.

NSDD-97, *National Security Telecommunications Policy (unclassified version)*, August 3, 1983.

NSDD-145, *National Security Policy on Telecommunications and Automated Information Systems Security*, September 17, 1984.

NSDD-201, *National Security and Emergency Preparedness Telecommunications Funding*, December 17, 1985.

NSD-56, *National Security Emergency Preparedness Telecommunications Funding*, April 30, 1991.

PDD-39, *US. Policy on Counterterrorism*, June 21, 1995.

PDD-63, *Protecting America's Critical Infrastructures*, May 22, 1998.

HSPD-5, *Management of Domestic Incidents*, February 28, 2003.

CONGRESSIONAL DOCUMENTS

Holifield (Rep. Chester E. Holifield, D-CA) Committee, *Government Telecommunications Management*, 1965.

GAO, *Review of the Status of Development Toward Establishment of a Unified National Communications System*, July 14, 1969.

US. House of Representatives, *Telecommunications Policy Coordination Act of 1987*, H.R. 323, 100th Congress, 1st Session, January 6, 1987.

Public Law 100-235, "Computer Security Act of 1987," January 8, 1988.

FCC, *National Security Emergency Preparedness Telecommunications Service Priority System*, FCC General Docket No. 87-505, adopted October 27, 1988, and released November 17, 1988.

Committee on Energy and Commerce, U.S. House of Representatives, *Compilation of Selected Acts Within the Jurisdiction of the committee on Energy and Commerce: Communications Law, including Communications Acts of 1934, Communications Satellite Act of 1962, Additional Communications Statutes, Selected Provisions from the United States Code*, July 1991.

Public Law 104-104, "Telecommunications Act of 1996," February 8, 1996.

Public Law 107-296, "Homeland Security Act of 2002," November 25, 2002

MEMORANDA

White House, "Cabinet Agenda for Friday, January 23, Item B: The Development of a Unified Federal Civilian Communication System," January 20, 1959 (Robert Gray, Secretary to the Cabinet).

Presidential Memorandum to the Heads of Executive Departments and Agencies, "Establishment of the National Communications System," August 21, 1963.

White House, "Procedures and Working Relationships for the NCS, August 21, 1963; "Statement of Initial Tasks," August 21, 1963.

Secretary of Defense to Manager, NCS, "Report on Initial NCS Task 3," November 30, 1963. NCS Memorandum No. 2-63, "Approval of Initial Tasks 1 and 2," December 13, 1963.

Manager, NCS, to Executive Agent, NCS, "Submission of First Annual NCS Long-Range Plan," August 12, 1964.

White House to Executive Agent, NCS, "Restoration Priority and Precedence System for the National Communications System," August 27, 1964.

NCS to Director, Joint Staff, Manager, NCS, "Final Report on NCS Initial Task 10," January 7, 1965.

DCA, "Reorganization of the Office of the Manager, NCS," February 4, 1966.

<p>Secretary of Defense (Robert S. McNamara) to the President, "Submission of the Second Long-Range Plan for the NCS FY 1968-1972," July 27, 1966.</p> <p>NCS, "System Design Concept Description," February 27, 1968.</p> <p>OMNCS to the Major Operating Agencies, "NCS Long-Range Concept Follow-On Studies," November 15, 1968.</p> <p>Executive Agent, NCS, to Manager, NCS, "The NCS Long-Range Plan, FY 1969-1973."</p> <p>Military Communications-Electronics Board to Director, Joint Staff, "Representations on the Emergency Action Group (NEAG)," December 5, 1968.</p> <p>NCS Memorandum No. 2-69, "Interim Procedures for Application for Planning-Programming-Budgeting System (PPBS) Features in the NCS Planning Process," October 31, 1969.</p> <p>White House, "The Flanigan Paper," (Peter Flanigan, Assistant to the President) December 6, 1969.</p> <p>NCS Long-Range Planning Study Group to Distribution, "Meeting on NCS Long-Range Concept, 14 September 1971," September 23, 1971.</p> <p>NCS to Distribution, "Highlights of Manager, NCS/NCS Representatives Meeting, December 20, 1971," December 23, 1971.</p> <p>NCS to Distribution, "Manager, NCS/NCS Agency Principals Meeting, January 28, 1972," February 7, 1972.</p> <p>Manager, NCS (Lt.Gen Gordon T. Gould, Jr.) to Executive Agent, NCS, "NCS Long-Range Planning," April 12, 1972.</p> <p>NCS to Chairman, NCS Long-Range Planning Study Group, "Report of the NCS Long-Range Planning Study Group," July 3, 1972.</p> <p>NCS, "Overall Plan for the Operational Management of the NCS," July 27, 1972.</p> <p>Executive Agent, NCS, "National Security Communications Organization," June 22, 1973.</p> <p>NCS, "OTP Council Meeting," September 19, 1973, prepared by Joseph Rose, Deputy Manager, NCS.</p>	<p>Joseph Rose, Deputy Manager, NCS, "Analysis of OTP Circular 12 and Related Issues," October 19, 1973. NCS Memorandum No. 1-73, "Federal Government Focal Point for Electromagnetic Pulse (EMP) Information," November 16, 1973.</p> <p>Executive Agent, NCS, "Implementation of OTP Circular 12, Government Communications Planning Programs," December 7, 1973.</p> <p>OMB, "Reorganization of Emergency Preparedness and Response Programs," May 25, 1978.</p> <p>Memorandum of Understanding Between the National Security Council, the Office of Science and Technology Policy and the Executive Agent, NCS, June 5, 1978.</p> <p>White House, "National Security and Emergency Preparedness Telecommunications Management and Coordination Responsibilities," July 5, 1978.</p> <p>Executive Agent, NCS, to William Harsch, Chairman, "FEMA Activation Group, OMB, National Communications System (NCS) Role in NS/EP Telecommunications," December 6, 1978.</p> <p>Zbigniew Brezinski, NSC, to the Secretary of Defense, Telecommunications and C³I Policy Issues," August 10, 1979.</p> <p>Joseph Rose, Deputy Manager, NCS, "National Security Council Tasking to Assess Commercial Common Carrier Vulnerability and Develop Possible Guidance to Commercial Common Carriers and Government Agencies," September 25, 1980.</p> <p>White House, "Emergency Mobilization Preparedness Board," December 17, 1981.</p> <p>White House, Memorandum for the Secretary of State et al., "National Communications System," May 19, 1982.</p> <p>White House, "National Plan of Action on Emergency Mobilization Preparedness," April 27, 1983.</p> <p>White House, "Enlargement of the National Communications System," October 7, 1983.</p> <p>White House, "National Communications System," October 7, 1983.</p> <p>John M. Poindexter to Caspar W. Weinberger, "National Security Emergency Preparedness (NS/EP) Telecommunications Requirements Analysis," March 17, 1986.</p>
---	---

Colin L. Powell to Frank C. Carlucci, "National Security Emergency Preparedness (NSEP) Telecommunications Requirements Analysis, Phase 11," December 7, 1988.

Colin L. Powell to Manager, NCS, "National Communications Systems Interoperability (E.O. 12472)," January 9, 1989.

Duane P. Andrews to Manager, NCS, "Public Switched Network Action Plan," April 23, 1990.

Brent Scowcroft to Dick Cheney, "National Security Telecommunications Advisory Committee Activities," July 12, 1990.

Brent Scowcroft to Dick Cheney, "National Security Telecommunications Advisory Committee Activities," April 2, 1991.

The White House to Executive Agent, NCS, "National Level Telecommunications Program Implementation and Functional Requirements," October 15, 1991.

Duane P. Andrews to Manager, NCS, "FY94 National Level Telecommunications Program Funding Approval," December 8, 1992.

Anthony Lake to Les Aspin, "National Security Telecommunications Advisory Committee Recommendations," April 14, 1993.

John H. Gibbons to Manager, NCS, "National Security and Emergency Preparedness Telecommunications," June 11, 1993.

LETTERS

Jerome B. Wiesner to Solis Horwitz, January 24, 1964, subject: GSA's objections to the NCS program.

Jerome B. Wiesner to Bernard L. Boutin, January 24, 1964, subject: Role and purpose of the NCS.

James D. O'Connell, Jr. to Solis Horwitz, November 9, 1964, subject: NCS system integration.

James D. O'Connell, Jr. to Robert S. McNamara, October 1, 1965, subject: NCS Long-Range Plan.

Charles L. Schultze to Robert S. McNamara, September 20, 1966, subject: NCS budget planning.

James D. O'Connell to Robert S. McNamara, October 31, 1966, subject: Approval of *Second Annual Long-Range Plan* (FY 68-72).

James D. O'Connell to Solis Horwitz, March 20, 1968, subject: NCS budget concerns.

Lt Gen Richard P. Klocko to William H. Goodman, April 12, 1968, subject: General Klocko's comments on role and purpose of the NCS.

James D. O'Connell to Clark M. Clifford, April 24, 1968, subject: *The Third Annual NCS Long-Range Plan* (FY69-73).

Solis Horwitz to James D. O'Connell, August 12, 1968, subject: AUTOVON/FTS integration.

James D. O'Connell to Solis Horwitz, October 9, 1968, subject: Concept of the NCS for the 1970s.

Solis Horwitz to James D. O'Connell, December 20, 1968, subject: *Fourth Annual NCS Long-Range Plan*.

James D. O'Connell to Melvin Laird, June 2, 1969, subject: *Fourth Annual NCS Long-Range Plan*.

Robert F. Froehlke to W. E. Plummer, October 23, 1969, subject: Unified NCS concept.

Lt Gen Richard P. Klocko to Lt Gen Harold W. Grant, March 19, 1970, subject: NCS planning guidance.

D. L. Solomon to Clay T. Whitehead, July 26, 1971, subject: NCS Long-Range Plan, FY72-76.

Clay T. Whitehead to Robert M. O'Mahoney February 8, 1972, subject: Integration of FTS and AUTOVON.

Executive Agent, NCS to Clay T. Whitehead, Director, OTP: April 21, 1972, subject: Future role of the NCS.

Clay T. Whitehead to E. Rehtin, May 25, 1972, subject: Future role of the NCS.

E. Rehtin to Clay T. Whitehead, November 13, 1972, subject: Coordination of Government communications activities.

Clay T. Whitehead to E. Rehtin, February 20, 1973, subject: New goals for the NCS.

Office of Telecommunications Policy to the Assistant Secretary of Defense, June 18, 1973, subject: Establishment of Lead Agencies.

E. Rehtin to Clay T. Whitehead, September 28, 1973, subject: OTP's Government Communications Planning Program.

Charles C. Joyce to Executive Agent, NCS, January 15, 1974, subject: OTP Circular 12.

Charles C. Joyce to David L. Solomon, April 17, 1974, subject: OTP Circular 12.

Thomas C. Reed to Clay T. Whitehead, August 8, 1974, subject: NCS Annual Report, 1974.

Charles C. Joyce, Jr., to Thomas C. Reed, January 9, 1975, subject: OTP Circular 12 and role of the NCS.

David L. Solomon to Charles C. Joyce, Jr., July 2, 1975, subject: OTP Circular 12.

Thomas C. Reed to John Eger, November 12, 1975, subject: National Security Group (NSG) Summary Plan 1975.

LTG William J. Hilsman to MG Robert Schweitzer, February 23, 1981, subject: Implementation of PD-53.

David A. Stockman to Caspar W. Weinberger, August 19, 1982, subject: NCS budget.

Stuart E. Branch to LTG William J. Hilsman, November 22, 1982, subject: Leased international circuits.

General William J. Hilsman, Manager, NCS, to Stuart E. Branch, December 21, 1982, subject: Leased international circuits.

Rand V. Araskog to Ronald Reagan, August 19, 1983, subject: Inaugural meeting of NSTAC, December 14, 1982.

Ronald Reagan to Rand V. Araskog, February 21, 1984, subject: Performance of NSTAC.

Joseph V. Charyk to Robert C. McFarlane, June 18, 1984, subject: NSTAC recommendations.

Ronald Reagan to Joseph V. Charyk, December 10, 1984, subject: NSTAC recommendations.

Joseph V. Charyk to Robert C. McFarlane, January 8, 1985, subject: NSTAC recommendations.

Ronald Reagan to Rocco J. Marano, October 27, 1987, subject: Government's response to NSTAC recommendations.

Rocco J. Marano to the President, January 19, 1988, subject: NSTAC VIII meeting and recommendations.

Ronald Reagan to Rocco J. Marano, July 11, 1988, subject: NSTAC VIII recommendations.

Paul H. Henson to the President, November 14, 1988, subject: NSTAC IX executive report.

E. E. Hood, Jr., to the President, May 25, 1990, subject: NSTAC XI recommendations.

Duane P. Andrews to Brent Scowcroft, December 5, 1990, subject: NSTAC XI recommendations.

George Bush to Edward E. Hood, Jr., December 10, 1990, subject: NSTAC XI recommendations.

E. E. Hood, Jr. to the President, February 25, 1991, subject: NSTAC XII recommendations.

Duane P. Andrews to Brent Scowcroft, July 30, 1991, subject: NSTAC XII recommendations.

R. E. Allen to the President, January 22, 1992, subject: NSTAC XIII recommendations.

Dick Cheney to Brent Scowcroft, June 9, 1992, subject: NSTAC XIII recommendations.

George Bush to Robert E. Allen, July 6, 1992, subject: Government's response to NSTAC XIII recommendations.

Robert E. Allen to the President, February 22, 1993, subject: An overview of NSTAC accomplishments.

NSTAC September 11 "Lessons Learned" Letter to the President, December 2001.

NSTAC REPORTS

National Coordinating Mechanism Task Force Report, May 16, 1983.
Commercial Satellite Communications Survivability Report, prepared by CSS Task Force, Resource Enhancements Working Group, May 20, 1983.
Automated Information Processing Task: Force Report, June 10, 1983 (revised June 30, 1983).

Funding and Legal/Regulatory Assessment of the NSTAC Working Group Reports on the National Coordinating Mechanism and Commercial Satellite Survivability, prepared by the Funding and Regulatory Working Group (FRWG), June 22, 1983.

Final Report-Telecommunications System Survivability Industry Responses to 13 May 1983 Questionnaire, prepared by the NCS Joint Secretariat, August 1983.

Addendum to Commercial Satellite Communication Survivability Report of May 20, 1983, prepared by the CSS Task Force, December 15, 1983.

Electromagnetic Pulse Task Force: Status Report to the Industry Executive Subcommittee, January 12, 1984.

National Coordinating Mechanism Implementation Plan, prepared by the NCM Task Force, January 30, 1984.

Automated Information Processing Task Force Interim Report: Telecommunications Operational Support, February 15, 1984.

International Diplomatic Telecommunications Task Force Report, March 15, 1984.

International Diplomatic Telecommunications Task Force Report, July 24, 1984.

Automated Information Processing Task Force Final Report: Strategy and Recommendations for Achieving Enhanced NSEPALP Survivability, October 25, 1984.

Commercial Network Survivability Report, prepared by the CNS Task Force, October 1984.

Electromagnetic Pulse Report, prepared by the EMP Task Force, October 1984.

Funding Assessment of Automated Information Processing Initiatives, prepared by the AIP Task Force, March 1985.

Automated Information Processing Task Force Final Report: Addendum, prepared by AIP Task Force, April 1985.

Electromagnetic Pulse Final Report, prepared by the EMP Task Force, July 1985.

Commercial Network Survivability Final Report, August 1985.

Telecommunications Industry Mobilization (TIM) Final Report, Vol. I and II, prepared by the Joint Industry-Government TIM Group, September 1985.

National Security Emergency Preparedness Telecommunications Service Priority System: TSP System Concept (draft No. 3) March 1986.

Personnel Issues, prepared by the Joint Industry-Government Group, May 22, 1986.

Report of Industry Information Security (IIS) Task Force, Vol. I & II, November 1986.

Status Reports of the Joint Industry-Government Telecommunications Industry Mobilization Group, February 18, 1987.

Status Report of the Industry Information Security Task Force, October 1987.

Joint Industry-Government Telecommunications Industry Mobilization Group Reports, November 1987.

Final Report of the Industry Information Security Task Force, June 1988.

Telecommunications Systems Survivability Task Force Reports: Review of Government Actions in Response to NSTAC- Recommended Initiatives, June 1988.

Network Management, June 1988.

Electric Power Survivability Status Report, August 1988.

Joint Industry-Government Telecommunications Industry Mobilization Group Reports, September 1988.

Telecommunications Service Surge Requirements Status Report.

Government and Industry Mobilization Management Structure Final Report.

Maintenance of Stockpiles and Inventories Final Report.

Final Report of the Joint Industry Telecommunications Industry Mobilization Group, April 1989:

Assessment of Telecommunications Industry Mobilization Capabilities (Vol.1)

<p>Telecommunications Industry Mobilization Subject Reports (Vol.II)</p> <p>Report on Earthquake Hazards, developed by the Energy Task Force, April 25, 1989.</p> <p>Final Report of the Commercial Satellite Survivability Task Force, December 1989.</p> <p>Final Report of the Energy Task Force, February 1990.</p> <p>Final Report of the National Research Council (NRC Report) Task Force, March 1990.</p> <p>Final Report of the Telecommunications Service Priority Task Force, September 1990.</p> <p>Report of the Network Security Task Force, October 1990.</p> <p>Status Report of the Network Security Task Force, August 1991.</p> <p>Final Report of the Wireless Services Task Force, September 5, 1991.</p> <p>Final Report of the Enhanced Call Completion Task Force, July 1992.</p> <p>Final Report of the Network Security Task Force, Revised August 1992.</p> <p>Final Report of the Energy Task Force, April 1993.</p> <p>An Assessment of the Risk to the Security of Public Networks, December 12, 1995.</p> <p>Financial Services Risk Assessment Report, December 1997.</p> <p>Interim Transportation Information Infrastructure Risk Assessment Report, Volume I, December 1997.</p> <p>Information Assurance: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group, Volume II, December 1997.</p> <p>Transportation Information Infrastructure Risk Assessment Report, June 1999.</p> <p>Telecom Hotels Report, April 2003.</p> <p>Trusted Access Report, April 2003.</p> <p>First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software and Protocols Report, April 2003.</p>	<p>NSTAC XXV Issue Review, 20th Anniversary Edition 1982-2002.</p> <p>NCS ISSUANCES</p> <p>NCSD 1-1, National Communications System (NCS) Issuance System, November 1987.</p> <p>NCSD 1-2, National Communications System (NCS) Membership, November 1987.</p> <p>NCSD-2-1, NSEP Telecommunications Planning Process, January 1989.</p> <p>NCSD 2-2, National Level NS/EP Telecommunications Program (NLP) Funding, November 1987.</p> <p>NCSD 3-1, Telecommunications Service Priority System for NS/EP, July 1990.</p> <p>NCSD 3-3, Shared Resources (SHARES) High Frequency (HF) Radio Program, January 1989.</p> <p>NCSD 3-4, National Telecommunications Management Structure, May 1992.</p> <p>NCSD 3-8, Provisioning of Emergency Power in Support of NS/EP Telecommunications, April 1991.</p> <p>NCSD 4-1, Federal Telecommunications Standards Program, February 1991. (Replaced NCSD 175-1, Federal Telecommunication Standards Program.)</p> <p>NCSD 4-2, Focal Point for Electromagnetic Pulse Information, January 1992.</p> <p>NCS Circular 130-2, Interim Procedures for Processing NCS Emergency Telecommunications Circuit Requirements, January 24, 1964.</p> <p>NCS Circular 70-1, Operating Procedures for the NCS, June 22, 1964.</p> <p>NCS Circular 70-2, Technical Control Procedures, October 1965.</p> <p>NCS Circular 70-3, Performance Objectives for the NCS, August 13, 1968.</p> <p>NCS Circular 175-1, Federal Telecommunication Standards Program, June 6, 1973.</p> <p>NCS Instruction 85-1, Maintenance of NCS Records, May 18, 1964.</p>
--	--

NCS Instruction 55-1, *Procedures for Placing into Effect the NCS Private Line Circuit Restoration Priority System*, January 18, 1965.

NCS Instruction, 120-1, *NCS Annual Planning Review*, December 13, 1972.

NCS Instruction 45-1, *National Communications System Emergency Action Group*, May 19, 1975.

NCS Instruction 205-1, *Reporting of Significant Telecommunications Research and Development Activities of the NCS Operating Agencies*, March 29, 1976.

NCS Office Order 5-69, *Procedures for Staffing NCS Actions*, December 31, 1969.

NCS Office Order 1-70, *NCS Participation in Information Processing Standards Development*, January 9, 1970.

NCS Office Order 3-69, *Coordination Between the Office of the Manager, NCS, and the US Military Communications-Electronics Board*, May 20, 1970.

MISCELLANEOUS NCS RESOURCES

Briefing by the Manager, NCS, *Concept for the NCS for the 1970s*, November 23, 1970.

NCS, *Long-Range Development Concept for the 1970s*, February 11, 1971.

NCS, *Organization and Functions Manual*, August 1978.

NCS, *NCS Membership and Assets Review*, October 20, 1978.

NCS, *Organization and Functions*, June 1982.

NCS, *NS/EP Telecommunications Planning Process*, October 11, 1986.

NCS, *National Coordinating Center Operating Charter*, October 9, 1988.

NCS, *National Plan for Telecommunications Support in Non-Wartime Emergencies*, January 1992.

OMNCS, *National Coordinating Center for Telecommunications, Hurricane Andrew After-Action Report*, February, 1993.

NCS, *Joint Government/Industry Northridge Earthquake Task Force, Northridge Earthquake After-Action Report*, June 1994.

OMNCS, *Disaster Area Architecture, Baseline Architecture and Near-Term Enhancement Report*, April 1995.

Joint Government/Industry Emergency Response Planning Report, *A Report on the Joint Government/Industry Capability to Support a Network Security Indications, Warning, and Assessment Mission*, October 26, 1995.

NCS, *Strategic Plan*, January 1996.

MISCELLANEOUS GOVERNMENT/INDUSTRY RESOURCES

DODD 5100.41, *Arrangements for the Discharge of Executive Agent Responsibilities for the National Communications System*, October 5, 1963.

DODD 5100.41, *Arrangements for the Discharge of Executive Agent Responsibilities for the National Communications System*, January 19, 1972.

DODD 5100.41, *Executive Agent Responsibilities for the National Communications System*, July 23, 1979.

DODD 5100.30, *Worldwide Military Command and Control System*, December 2, 1971.

Press Release, DOD, *Regarding Department of Commerce's proposal to take over functions of DTM*, October 13, 1969.

OTP Circular 3300.5, *Federal Government Focal Point for Electromagnetic Pulse (EMP) Information*, December 30, 1971.

OTP Circular 12, *Government Communications Planning Program*, October 12, 1973.

OTP *Coordination of Government Communications Activities*, November 21, 1972.

Proceedings of the Seventeenth Annual Electronics and Aerospace Conference, NS/EP Telecommunications session papers: J. D. Sulek, "Joint Government/ Industry Planning;" J. F. Mullen, "Commercial Communications Satellite Survivability for National Security;" W. E. Belford, "National Coordinating Center for Telecommunications;" and T. E. Burns, "Automated Information Processing and Telecommunications," Institute of Electrical and Electronics Engineers, Inc., October 9, 1984.

Charter of the President's National Security Telecommunications Advisory Committee, October 23, 1989.

White House Press Release, "Telecommunications Reorganization," February 9, 1970.

White House Press Release, "National Security Industrial Responsiveness," January 9, 1991.

The White House, *Creating a Government that Works Better & Costs Less*, Report of the National Performance Review, September 7, 1993.

Bellcore, Local Exchange Carrier Mutual Aid Agreement, March 4, 1995.

The President's National Strategy for Homeland Security, September 2002.

The President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, March 2003.

The President's National Strategy to Secure Cyberspace, February 2003.

ELECTRONIC SOURCES AND RESOURCES

Locations of electronic information are technology dependent and subject to change without notice. Internet addresses in this bibliography are correct as of July 28, 2003.

Hauben, Michael. History of ARPANET: Behind the Net-
The untold history of the ARPANET.
<http://www.dei.isep.ipp.pt/docs/arpa.html>.

Laursen, Jesper Vissing. "The Internet Past, Present and Future-Internet & WWW History."
<http://www.vissing.dk/inthist.html>

Leiner, Barry M., et al., "A Brief History of the Internet,"
<http://www.isoc.org/internet/history/brief.shtml>.

"The New Telecommunications Marketplace: Radical Changes and Golden Opportunities." Remarks of FCC Commissioner Susan Ness as part of the Public Policy Forum Series, The Wharton School of the University of Pennsylvania, Philadelphia, Pennsylvania, February 22, 1996.

<http://www.fcc.gov/Speeches/Ness/spsn604.html>.

The National Communications System Home Page,
<http://www.ncs.gov>.

The Department of Homeland Security Home Page,
<http://www.dhs.gov>.

The FEMA Reference Library,
<http://www.fema.gov/library>.

The Internet Society, <http://www.isoc.org>.

United States National Information Infrastructure Virtual Library, co-sponsored by the President's Information Infrastructure Task Force and the Council on Competitiveness, <http://nii.nist.gov>.

CHRONOLOGY

EISENHOWER ADMINISTRATION (1953-1961)

1959

January Eisenhower Cabinet considers proposal for a Unified Federal Civilian Communications System.

1960

May Defense Communications System (DCS) and Defense Communications Agency (DCA) formed.

December Report to President-Elect Kennedy underscores need for better coordination of Federal communications activities.

KENNEDY ADMINISTRATION (1961-1963)

1961

March The DCA Operations Center activated. DCA begins exercising supervision and operational control of military long haul, point-to-point communications.

March DCA assumes operational direction of DCS.

1962

February Position of Director of Telecommunications Management (DTM) established by Executive Order (E.O.) 10995 with mission to coordinate the telecommunications activities of the Executive Branch.

March LTG Alfred D. Starbird, USA, is appointed to command of DCA.

June National Military Command System (NMCS) established by President Kennedy in National Security Action Memorandum (NSAM) 166. The Memorandum states that the NMCS “should be recognized as, and designated to be, the basis for...a unified, survivable national communications system.”

October Cuban Missile Crisis.

October The National Security Council (NSC) publishes NSAM-201, *Establishment of Subcommittee on Communications*, October 26, 1962. It established the interdepartmental Subcommittee on Communications, headed by William H. Orrick, Jr., then Deputy Under Secretary of State for Administration, to investigate communications failures during the Cuban Missile Crisis, and to make recommendations to eliminate deficiencies.

1963

February Federal Telecommunications System (FTS) established.

July In response to Orrick Committee recommendations, the NSC issues NSAM-252, July 11, 1963 (CONFIDENTIAL), directing the establishment of the National Communications System (NCS).

August	President Kennedy publishes unclassified version of NSAM-252 (Presidential Memorandum, August 21, 1963). Designates the DTM as Special Assistant to the President for Telecommunications (SAPT) to advise and assist him with respect to communications requirements and plans for the NCS. Secretary of Defense named the Executive Agent, NCS. The Director, DCA, General Starbird, named Manager, NCS. The purpose of the NCS is to provide the necessary communications for the Federal Government, particularly the President, under all conditions of emergency, including nuclear war.
August	As a direct result of the Cuban Missile Crisis, the U.S. and the USSR implement a joint Direct Communications Link teletype system providing a secure, reliable, and private means of communications between the Heads of State of the two countries. The Hot Line remains operational to this date.
October	The first NCS planning document, the Near-Term Plan, published. Inventories potential NCS communications resources.
October	Department of Defense Directive (DODD) 5100.41, "Arrangements for the Discharge of Executive Agent Responsibilities for the National Communications System," issued.
November	President Kennedy assassinated.

JOHNSON ADMINISTRATION (1963-1969)

1964

January	Procedures for processing NCS telecommunications circuit requirements published.
January	Institutional resistance to NCS surfaces as the General Services Administration (GSA) voices opposition to a "single" NCS under control of an Executive Agent (Secretary of Defense).
August	First Annual NCS Long-Range Plan published. DCS and FTS proposed as the two main components of NCS.
December	National Plan for Emergency Preparedness, published by the Johnson Administration. Repeats call for a "unified governmental communications system, responsive to a single Executive Agent."

1965

October	The First Annual NCS Long-Range Concept Plan approved for planning purposes by General James D. O'Connell.
November	The Holifield Committee, chaired by Rep. Chester E. Holifield, D-CA, calls for a greater delegation of powers to DTM to strengthen his role in managing Government telecommunications.

1966

January	Separate NCS organizational unit established by the Director, DCA.
----------------	--

September	Bureau of the Budget asks all NCS operating agencies to submit program and cost information for inclusion in the Bureau of Budget's Planning-Programming-Budget System process.
October	<i>Second Annual NCS Long-Range Concept Plan</i> published. Debate over NCS technical design and management arrangements continues. SAPT directs preparation of <i>Interim NCS Concept Plan</i> for the 1970s, separate from the annual planning process.
1967	
August	President Johnson appoints task force to study U.S. communications policy. In addition, Johnson tasks the Bureau of Budget to make a thorough study of existing governmental organizations in the field of communications and to propose needed modifications.
November	Lt. Gen. Richard P. Klocko, U.S. Air Force, succeeds General Starbird as Director, DCA, and Manager, NCS.
1968	
March	<i>Third Annual NCS Long-Range Concept Plan</i> forwarded to the White House.
April	In the face of continued opposition to a unified system, the Manager, NCS, writes to all agencies seeking to balance individual agency prerogatives with requirements for a unified system ordered by the President.
August	Executive Agent, NCS, forwards 1970s <i>Interim Concept Plan</i> to White House without recommendation. Plan calls for an "Integrated Government Communications System." The Department of Defense (DOD) resists and asks for further study.
November	The Bureau of Budget issues report strongly criticizing the Government's management of telecommunications. Urges a reorganized and strengthened NCS.
December	<i>Fourth Annual NCS Long-Range Concept Plan</i> forwarded to the White House. Little progress made toward a final NCS concept plan to be approved by the President. Separate task force formed to prepare <i>Interim NCS Concept Plan</i> for the 1970s.

NIXON ADMINISTRATION (1969-1974)

1969

July	General Accounting Office (GAO) issues report critical of NCS. Recommends White House create a new organization with the "stature, authority, and resources sufficient to provide a strong central focal point in telecommunications matters."
October	President Nixon signs E.O. 11490 clarifying emergency preparedness assignments.
December	White House study (Flanigan Report) calls for elimination of DTM and establishment of a new independent White House telecommunications office.

1970

- February** President’s Reorganization Plan No. 1 submitted to Congress. Calls for establishment of the Office of Telecommunications Policy (OTP) and elimination of DTM.
- September** NCS suspends planning until dispute over roles and prerogatives are resolved.
- September** E.O. 11556 promulgated, establishing OTP as an independent office within the Executive Office of the President (E.O.P). DTM abolished. OTP begins review of the Government’s telecommunications policy and resources.
- October** Congress deletes funds for NCS planning studies. Urges Executive Branch to strengthen NCS management structure or “abandon the entire concept.”

1971

- May** Congress reviews DOD Worldwide Communications Report. Report states that the performance of the DCS fell far short of meeting minimum standards for responsiveness to crisis situations. It concluded, “the heart of the problem is in the management of the communications at all levels...”
- July** NCS submitted *Sixth Annual NCS Long-Range Concept Plan* to White House. (Fifth long-range plan drafted but never published.) In the sixth plan, the NCS proposes a single, unified NCS communications network for the final time.
- September** Lt. Gen. Gordon T. Gould, USAF, succeeds General Klocko as Director, DCA, and Manager, NCS.
- December** DOD issues DODD 5100.30, naming the National Command Authority as the primary mission of the Worldwide Military Command and Control System (WWMCCS), and the NCS as the primary component of WWMCCS.

1972

- April** Executive Agent announces the elimination of a single integrated communications system as a goal of the NCS. The Executive Agent changes the focus of the NCS to interoperability. Organizationally the NCS now viewed as a confederation, with emphasis on consensus building among the representatives of the operating agencies.
- August** NCS assigned responsibility for the development and coordination of Federal telecommunications standards under the Federal Standardization Program administered by GSA.
- October** First meeting of the Federal Telecommunication Standards Committee.

1973

- October** OTP Circular 12 makes major revisions in the Government’s approach to communications organization and planning. Government communications services divided into general-purpose systems and mission-oriented systems, with DOD as Executive Agent, NCS, lead agency for national security systems, one of the four specialized mission areas identified by OTP. Net effect is to lower the NCS profile and make it one among a group of mission competing for funds.

FORD ADMINISTRATION (1974-1977)

1974

- July** Lt. Gen. Lee M. Paschall, U.S. Air Force, succeeds General Gould as Director, DCA, and Manager, NCS.
- July** NCS announces OTP Circular 12 does not alter its responsibilities outlined in Presidential Memorandum of August 21, 1963. The NCS continue to be responsive to both.
- August** First NCS Annual Report published. Published annually thereafter.

CARTER ADMINISTRATION (1977-1984)

1978

- January** Intelsat and Molniya satellite links, providing communications backup to the Hot Line, installed and now operational.
- March** E.O. 12046 signed by President Carter. Abolishes OTP and transfers telecommunications functions to NSC, Office of Science and Technology Policy (OSTP), and elsewhere. NSC responsible for the development of policy plans, programs, and standards for the mobilization and use of the Nation’s telecommunications resources during emergencies. OSTP given the task of implementing these functions under policy guidance of the NSC. Renewed emphasis on national security and emergency preparedness (NS/EP) telecommunications as the President’s National Security Advisor renews Kennedy’s call for “leadership protection” through enhanced command, control, and communications systems.
- June** Memorandum of Understanding signed between NSC, OSTP and Executive Agent, NCS, providing new tasking assignments for the NCS. Revitalizes the NCS, making it once again the focal point for emergency telecommunications in the Federal Government.
- July** U.S. District Court Judge Harold Green assigned Justice Department suit against AT&T.
- September** VADM Samuel L. Gravely, U.S. Navy, succeeds General Paschall as Director, DCA, and Manager, NCS.

1979

- November** Presidential Directive (PD) 53, “National Security Telecommunications Policy,” published. Calls for communications facilities adequate “to gather intelligence, conduct diplomacy, command and control our military forces provide continuity of government, and to reconstitute the political, economic, and social structure of the Nation.” Restates policy objectives of the August 21, 1963, Presidential Memorandum, but without end-product (a national communications system). PD-53 Steering Group set up to implement directive.

1980

- January** The NCS, assisted by the NCS Operating Agencies, prepares a draft *National Security Telecommunications Policy Implementation Concept Plan* for the implementation of PD-53 and briefs it to the Federal agencies serving on the NSC PD-53 Steering Group. Twenty-two PD-53 telecommunications initiatives identified by the Steering Group.

September	LTG William J. Hilsman, USA, succeeds Admiral Gravely as Director, DCA, and Manager, NCS.
September	AT&T undertakes a survivability study of class 4/5 switches in a nuclear war. AT&T concludes that their survivability is technically feasible and could be of use to support essential Government communications.
December	PD-53 Steering Group briefed on NCS findings regarding Government reliance on common carriers. NCS study confirms the Government's overwhelming reliance on common and specialized carriers and the vulnerability of these carriers to a variety of disruptions. Steering Group proposes a set of initiatives (known as the PD-53 initiatives), which became the building blocks of the NCS communications enhancement programs in the 1980s.

REAGAN ADMINISTRATION (1981-1989)

1981

January	Reagan Administration takes office. Endorses PD-53 objectives and E.O. 12046 reorganizing Federal telecommunications management.
June	At a Senate hearing, the Manager, NCS, questioned the issue of national security dependence on the Nation's Automated Information Processing (AIP) resources. NCS initiates examination of the NS/EP AIP issue.
July	Office of the Manager, NCS (OMNCS) launches major study of PD-53 initiatives.
November	Drawing on the AT&T study showing the feasibility of building an emergency communications service around surviving class 4/5 switches, the NCS launches a follow-on network engineering study to define routing through the Public Switched Network (PSN). By August 1981, the NCS study had evolved into the Nationwide Emergency Telecommunications Service (NETS) Program.
December	Emergency Mobilization Preparedness Board (EMPB) established by Presidential Memorandum, with the Emergency Communications Working Group (ECWG) as one of 12 EMPB working groups. The ECWG chaired by the Manager, NCS, with the Administrator, National Telecommunications and Information Administration, as vice chair

1982

January	On January 8, the Department of Justice and AT&T announce agreement to break up AT&T (the Modification of Final Judgment). On the following day, DCA/NCS begin preparing for AT&T divestiture.
March	Manager, NCS, identifies the National Coordinating Mechanism (NCM), AIP, and Commercial Satellite Survivability (CSS) issues as candidates for joint Government-industry study.
March	Manager, NCS, testifies before the House Telecommunications Subcommittee reaffirming "our previously expressed view that legislation is necessary to assure that our telecommunications industry, in concert with the government, can meet all urgent national requirements..."

June	The PD-53 Steering Committee appoints a PD-53 Working Group with the chair from OSTP and vice chair from the NCS.
July	The President approves National Security Decision Directive (NSDD) 47, <i>Emergency Mobilization Preparedness</i> , July 22, 1982. In NSDD-47, the President states that it is “the policy of the United States to ensure that communications resources be available and adequate to respond to the Nation’s needs,” and directs the EMPB to prepare a Plan of Action to implement NSDD-47.
September	National Security Telecommunications Advisory Committee (NSTAC) established by E.O. 12382 providing a legal framework for industry/Government joint planning to respond to the emergency telecommunications needs of the Federal Government. NSTAC is the result of the breakup of AT&T”. Prior to January 1982, AT&T supplied the Government’s emergency telecommunications needs.
November	First NETS Program Plan issued on November 30, 1982, projecting an Initial Operating Capability (IOC) for July 1987.
December	NSTAC I meets and approves three issues for study: NCM, CSS, and API.
December	Contract issued through the Defense Commercial Communications Office to implement the NCS-proposed Automatic Voice Network/FTS interconnect initiative with an IOC date of September 1983.
1983	
February	The NSTAC recommends to the President that a National Coordinating Center for Telecommunications (NCC) be established as the operational arm of this new industry/Government communications committee.
March	EMPB Plan of Action approved by the President. Contains 32 ECWG milestones or tasks, providing for an enhanced emergency communications capability. Milestones are to be the responsibility of various departments and agencies.
July	NSTAC II meets and formally recommends the establishment of the NCC as a mechanism for coordinating industry and Government responses to NS/EP telecommunications requirements. The NSDD-97 Steering Group enlarges the membership of the NCS to include 22 Federal departments and agencies. The NCS assumes the functions of the ECWG.
August	NCS updates national security telecommunications policy (NSDD-97, <i>National Security Telecommunications Policy</i> , August 3, 1983), replacing PD-53. The goal of the NCS is to assure a survivable telecommunications infrastructure, rather than a discrete communications system as originally envisioned in the 1960s. Gives NCS enlarged coordination and planning role. ECWG responsibilities assumed by the NCS.
September	Lt. Gen. Winston D. Powers, USAF, succeeds General Hilsman as Director, DCA, and Manager, NCS.

1984

- January** Court-ordered divestiture of the Bell System implemented.
- January** Interim NCC activated at the NCS, Arlington, Virginia. This joint industry/Government operation created to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications. The NCC manned by 11 telecommunications industry representatives, including the U.S. Telephone Association, together with representatives from NCS member agencies.
- February** President approves NSTAC-recommended projects. Presses for establishment of a permanent NCC.
- April** NSTAC III meets and recommends approval at the NCM Implementation Plan and a new CSS Program.
- April** Management of Federal emergency telecommunications resources reorganized under E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which superceded the 1963 Memorandum. The Committee of Principals (COP) is formalized as part of the NCS organization, along with the Executive Agent and the Manager, NCS. NCS emerges with enlarged powers and responsibilities to coordinate the establishment of an NS/EP telecommunications capability.
- September** NSDD-145, "National Policy on Telecommunications and Automated Information Systems Security," promulgated.
- October** DCA awards contract to ITT World Communications to establish a facsimile circuit over the Intelsat international satellite system.
- December** President approved NSTAC III recommendations, including the NCM Plan, except for the General Forum. NSTAC IV convenes. Two new issues adopted: Telecommunications Service Priority (TSP) and Telecommunications Industry Mobilization (TIM). NSTAC recommends industry play a larger role in NS/EP telecommunications planning and that the Government establish a focal point for AIP planning. Government-industry cooperation in the emergency telecommunications field now on strong footing.

1985

- January** Permanent Computer II NS/EP waiver granted to Bell Operating Companies and AT&T, making these organizations the exclusive points of contact, during emergencies, for 21 designated Federal systems. This decision is, in effect, a return to pre-divestiture arrangements in which AT&T Long Lines was solely responsible for providing communications to the Government in emergencies.
- March** NCC moves into permanent quarters at the NCS, Arlington, Virginia.
- June** "National Security Emergency Preparedness Telecommunications Procedures" issued by NCS pursuant to E.O. 12472.

July	DCA Instruction 3 10-135-1, “National Security Emergency Preparedness Telecommunications Procedures,” issued in support of DCA/NCS policy “that all commercially provided NS/EP telecommunications service requirements processed through DCA...comply with the procedures prescribed in this instruction.”
September	NSDD-188 establishes a new NS/EP Service Interagency Group to oversee all Federal Government NS/EP activities, including emergency communications.
October	In response to NSTAC IV recommendations, the President directs NCS to increase industry participation in NS/EP planning and to form a Government focal point for information on AIP survivability.
October	NSTAC V Meeting. Over the past three years NSTAC worked ten major issues, and made recommendations in six areas: NCM, CSS, AIP, International Diplomatic Telecommunications, Commercial Network Survivability (CNS), and Electromagnetic Pulse (EMP). The President directed the Executive Agent to pursue four of those six: NCM, CSS, EMP, and AIP.
November	A joint industry/Government TIM Group established, with representatives from NSTAC and NCS member agencies. Purpose to assist the Government in assessing TIM capabilities.
December	President signs NSDD-201, “NS/EP Telecommunications Funding,” setting forth Government policy on funding NS/EP improvements. Development costs funded by Executive Agent, NCS. Implementation and recurring costs to be shared among NCS member agencies.
1986	
May	NSTAC VI meeting. Industry’s TSP Task Force continues to assist Government in the development of the TSP System concept, which has been submitted to the Federal Communications Commission (FCC) for its action. A new; joint industry/Government TIM Group formed. NSTAC agrees to assist Government in implementing Industry Information Security (IIS) measures.
June	President Reagan informs Congress that the United States is strengthening the command and control network as the result of deploying Defense Satellite Communications System III.
August	In response to the COP’s concerns over rising NETS costs, the Office of Management and Budget asks NCS to conduct a comprehensive program review of NETS. The National Research Council of the National Academy of Sciences selected to conduct review.
August	E.O.P. approves the first National Level NS/EP Telecommunications Program (NLP) consisting of three elements: NETS, CNS, and Commercial SATCOM Interconnectivity.
October	E.O.P. approves the NCS “NS/EP Telecommunications Planning Process” report, prepared in support of E.O. 12472.

1987

- February** NSTAC VII meeting. NSTAC recommends that the Government's mobilization management structure be updated and that steps be taken to mitigate the potential loss of foreign-sourced semiconductors.
- February** House of Representatives' Committee on Government Operations requests GAO to "undertake a comprehensive review into all aspects of the NS/EP telecommunications program."
- April** GAO report, "Interoperability Among C3 Systems," lists three major causes for interoperability problems: (1) DOD's decentralized management structure; (2) lack of clearly defined joint requirements; (3) absence of an effectual central enforcement authority
- May** LTG John T. Myers, USA, succeeds General Powers as Director, DCA, and Manager, NCS.
- May** Department of Health and Human Services becomes 23rd member of the NCS COP.
- August** National Research Council concludes that the NETS Program is on the right path for providing a technically viable NS/EP telecommunications capability.
- October** In a letter to NSTAC, the President praises the NSTAC's sustained record of accomplishments. Assigns high priority to the TSP System as well as to making improvements in the National Telecommunications Management Structure (NTMS). President announces measures regarding dependence on foreign-sourced semiconductors and directs the Department of Energy (DOE) to work closely with NSTAC regarding survivability of electric power sources.
- November** NSTAC VIII meeting at Kennedy Space Center, Florida. NSTAC recommends that: (1) the NCS, in conjunction with industry, monitor the potential effects of mobilization on telecommunications industry personnel; (2) a mechanism be established to assess dependence on foreign sources; and (3) the President approve the NTMS implementation concept.

1988

- March** NCC participates in its first nationwide exercise of single sideband voice radio communications.
- May** NCC conducts high-frequency radio teletype tests with the North Atlantic Treaty Organization.
- July** In response to NSTAC VIII, the President approves the NTMS implementation concept and agrees that the Government and industry should continue monitoring potential effects of personnel call-ups. Also directs establishment of a mechanism to monitor effects of offshore dependence for identified Government needs. Reminds NSTAC that TSP remains the number one priority.
- August** NCS celebrates its 25th anniversary. A fully defined and implemented NS/EP telecommunications capability yet to be realized.

- September** NSTAC IX held in Washington, D.C. As a consequence of its IIS investigation, NSTAC recommends Government actions for major enhancements to telecommunications protection. NSTAC also recommends continued industry/Government work on TSS and TIM.
- November** FCC issues order establishing the TSP System, providing the regulatory, administrative, and operational framework for authorizing priority treatment for NS/EP telecommunications services, including procedures for restoration and provisioning.
- November** E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, signed by the President. The order refers to E.O. 12472 for guidance relative to NS/EP telecommunications functions. Each Government department and agency to work within the framework established by E.O. 12472 to ensure adequate NS/EP telecommunications support.

BUSH ADMINISTRATION (1989-1993)

1989

- January** The President’s National Security Advisor reminds the DOD community of the continuing need for an interoperable and survivable national telecommunications infrastructure, and directs the community to coordinate major telecommunications plans, programs, and system architecture with the OMNCS.
- April** National Security Directive 10, *National Security Telecommunications and Information System Policy Coordinating Committee (PCC)*, issued. The PCC replaces the NSDD-97 Steering Group, previously responsible for oversight of national security telecommunications policy implementation.
- June** NSTAC X meeting held in Washington, D.C. As a consequence of its extensive TIM study, NSTAC recommends Government actions regarding telecommunications service surge requirements, dependence on other infrastructure systems, and jurisdictional issues, as well as establishment of a national level mobilization management policy and plan. NSTAC also recommends Government action regarding energy, and endorses continuing NSTAC work on TSP and CSS.
- September** NCC responds to Hurricane Hugo.
- October** NCC responds to Loma Prieta Earthquake.
- December** FCC approves the NCS TSP implementation procedures.

1990

- January** By the early 1990s, the NCC is coordinating the restoration and provisioning of NS/EP telecommunications services in natural disasters and armed conflicts, including Hurricane Hugo in 1988, the Loma Prieta earthquake in California in 1989, Hurricanes Andrew and Iniki in 1992, and Operations Desert Shield and Desert Storm in 1990-1991.

January	Manager, NCS, the COP, and senior members of the OMNCS hold an offsite meeting to launch NCS Vision 21. Vision 21 is a total quality management program, which seeks to identify and define a range of problems and opportunities before the NCS. Vision, purpose, mission, and goals of the NCS studied and revised, with a target date for achieving these objectives set for January 1, 2001.
March	Special COP Subcommittee formed to review the NLP, particularly NETS. Examines threat, user requirements, program risks, technology alternatives, and costs.
March	NSTAC XI meeting held in Washington, D.C. Recommends that the conclusions of the CSS Task Force be approved for action, and that the Government develop a program to assign electric power restoration priorities and to fund studies to determine feasibility of developing cost-effective back-up power systems.
April	Chairman, Policy Coordinating Committee for National Security Telecommunications and Information System directs Manager, NCS, to ensure coordination of Government and industry efforts regarding protecting the PSN from computer intruders. OMNCS designated as Government focal point. Manager, NCS prepares action plan. Government Network Security Subgroup and NSTAC Network Security Task Force formed to study network security.
May	Second offsite NCS Vision 21 meeting.
June	LTG Thurman D. Rodgers, USA, succeeds General Myers as Director, DCA, and Manager, NCS.
July	White House tasks Manager, NCS, to implement the recommendations of the Joint TIM Group. In response, the Manager developed an implementation plan.
September	TSP System reached IOC. Replaces existing restoration priority (RP) system. Called into use for Operation Desert Shield.
October	First NTMS Operating Center becomes operational.
December	NSTAC XII held in Washington, D.C. Committee briefed on NCC support of Operation Desert Shield, noting that IOC had been achieved for the TSP System. NSTAC recommends Government continue to support the TSP System. In addition, NSTAC continues work on intelligent networks and network security

1991

May	NSTAC Network Security Information Exchange (NSIE) established.
March	NETS IOC date delayed for two years. Panel of experts appointed to again review the NETS Program.
June	Name of DCA officially changed to Defense Information Systems Agency (DISA).
July	LTG Alonzo E. Short, Jr., USA, succeeds General Rodgers as Director, DISA, and Manager, NCS.

August	Security of the Public Switched Network: A status Report to the Chairman, Policy Coordinating Committee, National Security Telecommunications and Information System.
September	First NSTAC Research and Development (R&D) Exchange.
September	Third offsite Vision 21 meeting held to reevaluate and consider the future direction of the Vision 21 process.
September	Advanced Intelligent Network (AIN) Program Office established in OMNCS to study and influence the direction of intelligent networks technology research. Among the topics of interest were AIN and Personal Communications Services technologies, AIN and multimedia communications, and international AIN technology developments.
October	Panel of experts recommends that NETS be replaced by a PSN-based technical approach that would take maximum advantage of commercial off-the-shelf capabilities at substantial cost savings.
October	White House memorandum identifies six basic functional requirements for NS/EP telecommunications; voice-band service in support of Presidential communications; interoperability with selected Government and commercial systems; survivability in order to provide interconnection with surviving users; international interface; nationwide coverage; and intra/interagency emergency operations.
October	NSTAC XIII held in Washington, D.C. NSTAC heard reports from four investigations: Network Security Enhanced Call Completion, Wireless Digital Services, and Intelligent Networks. NSTAC recommends that the Government establish a focal point to monitor wireless digital interface issues and that Government establish an Intelligent Networks Program Office. NSTAC also directed establishment of new energy task force.
November	Government wireless services focal point established in the OMNCS.
1992	
January	A modified technical and acquisition approach developed and incorporated into a new NLP program called Government Emergency Telecommunications Service (GETS), replacing NETS. Objective of GETS to provide authorized Government users with a nationwide NS/EP switched-voice and low-speed data communications service by utilizing surviving PSN resources.
February	In the wake of several major telephone outages, the Network Reliability Council is established.
March	TSP reached full operational capability.
April	Federal Emergency Management Agency (FEMA) publishes the Federal Response Plan, which provides for a coordinated disaster response effort.
May	E.O.P. approves NCS Directive 3-1, "Establishment of the National Telecommunications Management Structure."

July	President approves NSTAC XIII recommendations on intelligent networks and digital wireless communications.
July	NSTAC XIV held in Washington, D.C. NSTAC celebrates its tenth anniversary, receiving commendation from the President, the National Security Advisor, and the Manager, NCS, for its continuing contributions to the Nation's NS/EP telecommunications policies and programs.
August	NCC responds to Hurricane Andrew.
September	NCC responds to Hurricane Iniki.

CLINTON ADMINISTRATION (1993-2001)

1993

January	COP approves the NCS Vision 21 charter.
April	The President approved NSTAC XIV recommendations regarding network security and enhanced call completion, asking the telecommunications industry to continue its efforts to identify and implement network security standards initiatives. In regard to enhanced call completion, the Manager, NCS, was directed to take steps to improve call completion rates during periods of stress and congestion.
April	All six NTMS teams activated.
April/May	NSTAC/NSIE report on deficiencies in Federal laws on computer crime.
April/May	NCC responds to Tulsa Flooding.
May	NSTAC XV held in Washington, D.C. NSTAC recommended continued Government support of DOE's Telecommunications Electric Service Priority initiative and increased emphasis on survivability of electric power through the President's National Energy Strategy. NSTAC also recommended changes in computer crime legislation that could directly enhance the security of the Nation's telecommunications infrastructure.
June	The Director, OSTP, issues a memorandum instructing the Manager, NCS, to take steps necessary to ensure a flexible, integrated response capability to manage the Nation's telecommunications assets "across the full spectrum of domestic and national security emergencies." This effectively paved the way for an expansion of the NCS mission to encompass emergency telecommunications response following natural and manmade disasters and emergencies.
July	The Administration established the National Information Infrastructure (NII) Task Force.
September	NII: Agenda for Action issued.

September	E.O. 12864, United States Advisory Council on the NII is signed. The Council was created to provide a coordinating mechanism to advise the Federal Government on a national strategy to foster further development of NII capabilities and applications.
November	NCC responds to California Wildfires.
1994	
January	NCC responds to Northridge Earthquake, providing the largest “no-notice” disaster response to date.
February	NCS and NSTAC NSIEs sponsored a Network Security Symposium attended by 240 individuals representing a broad range of Government and private organizations. The purpose of the symposium was to alert and sensitize the audience to the security problem presented to the PSN by computer intruders and to provide information on the NSIE’s experience and lessons learned over the first two years of the NSIE process.
March	NCC responds to Ice Storms.
April	NCC responds to the Miami Floods.
April	The Manager, NCS, established the Office of Strategic Planning to assist in developing strategies that focus NCS efforts on projects that contribute to the successful accomplishment of the NCS mission. The Office of Strategic Planning also supports NII initiative task forces and working groups.
June	NSIE Firewall Workshop to provide up-to-date information on firewalls.
July	Lt. Gen. Albert J. Edmonds, USAF, succeeds General Short as Director, DISA, and Manager, NCS.
August	NCC responds to the Georgia Floods.
September	The Manager, NCS, approves an information resources security plan to encourage sharing of compatible security solutions and to reduce the total security costs to the Federal Government.
October	President Clinton signs the Communications Assistance for Law Enforcement Act (Public Law 103-414, 47 U.S.C. 1001-1010), which seeks to ensure that telecommunications carriers will have the necessary technical ability to fulfill their statutory obligation to accommodate law enforcement requests for assistance.
October	NCC responds to the Houston Floods.
October	The NCS COP endorses a vision statement for the NCS, stating that it should “lead the planning, coordination, and integration of government telecommunications capabilities to ensure access to, and use of critical information services required for effective response in an all-hazards environment.”

1995

- March** Bellcore's *Local Exchange Carrier Mutual Aid Agreement* delineates procedures for requesting and providing supplies, equipment, vehicles, network capacity, personnel, and billing.
- April** NCC responds to Oklahoma City Bombing.
- May** NCC responds to Louisiana Floods.
- June** President Clinton signs Presidential Decision Directive-39, U.S. Policy on Counter-terrorism. NCS assists FEMA in identifying key assets and shortfalls in telecommunications and information technology for emergency response activities.
- September** NCC responds to Hurricane Marilyn.
- October** NCC responds to Hurricane Opal.
- October** GETS reaches IOC.
- October** The Manager NCS restructures the OMNCS, realigning offices into functional divisions based on complementary programs, services, and activities to improve response to the ever-changing threat to NS/EP telecommunications.
- December** Government and NSTAC NSIEs published their report, *An Assessment of the Risk to the Security of the Public Switched Network*. Overall risk to the PN from electronic intrusions considered greater than in previous years. Threats are outpacing deterrents while vulnerabilities outpacing the implementation of protection measures.
- December** NCC coordinates cross-border assistance from Canada during response efforts following flooding in the Pacific northwest.

1996

- January** The NCS Strategic Plan is created and adopted, ensuring the Government has the telecommunications capabilities to gain access to and use critical information services in an all-hazards environment. The Strategic Plan defines seven goals that are accompanied by 28 objectives and strategies for the development of the NCS into the next millennium.
- January** Deputy Manager, NCS, initiates the National Communications Awareness Partnership to revalidate NS/EP telecommunications requirements, promote the OMNCS programs and services available to NCS member organizations, and increase interagency awareness and coordination among NCS members.
- February** NCC responds to the Oregon Floods.
- February** The Telecommunications Act of 1996 dramatically changes the ground rules for competition and regulation in virtually all sectors of the communications industry, from local and long-distance telephone services, to cable television, broadcasting, and equipment manufacturing.

February	NSTAC XVIII Meeting focuses on information assurance, and presentations describe threats to information systems, infrastructure vulnerabilities, and potential consequences of an electronic attack against the Nation's most critical infrastructures. To further discuss and better understand the threats to information systems, a special session of the NSTAC is scheduled for May.
February	Communications Resource Information Sharing (CRIS) initiative begins. The CRIS Directory lists agency contact numbers and the types of equipment, services, and capabilities that are available. It contains more than 30 different systems from more than 20 resource contributors.
March	The Emergency Response Fly-Away Kit (ERFAK) enables emergency response personnel to coordinate disaster relief from remote locations.
April	Deputy Manager, NCS, chaired the NII Reliability and Vulnerability Working Group (RVWG) of the Government's Information Infrastructure Task Force. The RVWG produced a risk assessment of the NII, <i>The NII: A Nation's Information at Risk.</i> "
May	The NCS and NIST co-sponsor a Federal Wireless Users Forum workshop, to provide an opportunity for potential and current Government wireless users to obtain information on evolving wireless technology, define Government wireless requirements, and interface with industry and Government representatives.
July	The President issues E.O. 13010, Critical Infrastructure Protection, establishing the President's Commission on Critical Infrastructure Protection (PCCIP) and the Infrastructure Protection Task Force (IPTF). The NCS becomes an active participant because of its vast experience within the telecommunications and information assurance arenas.
September	NCC responds to Hurricane Fran.
September	The pilot test of the Emergency Response Link (ERLink) begins, with Federal Response Plan departments and agencies and several States participating.
September	The NSTAC's Network Security Group sponsors the second joint industry and Government R&D Exchange. The exchange focused on issues of authentication, intrusion detection, and access control. Industry representatives from AT&T, Bellcore, CSC, EDS, ITT, Mitre, UNISYS, and Government representatives from DOE, Defense Advanced Research Projects Agency, National Security Agency (NSA), and NIST shared the latest R&D concepts with an extensive industry and Government audience.
October	National Information Infrastructure Protection Act of 1996, P.L. 104-294, addressed deficiencies in Federal laws on computer crime identified by the NSTAC/NSIE in 1993.
October	Officials approve the Telecommunications Industry Association, Electronics Industry Association Interim Standard 136, and the air interface standard that includes Priority Access and Channel Assignment in Time Division Multiple Access systems.

1997

- January** NCC responds to the Northwest Floods.
- February** OMNCS conducts its first ERLink exercise with the NCC Blue Emergency Operations Team, focusing on use of ERLink as a new information resource.
- March** NSTAC XIX approves four recommendations to the President: three address the growing concern for the information-based vulnerabilities of the Nation's electric power infrastructure and its NS/EP implications, and the fourth advises the President to endorse the establishment of an industry-based Information Systems Security Board as a potential mechanism for enhancing the reliability and trustworthiness of the Nation's information products and services.
- March** The NCS-N5 Information Assurance Branch co-sponsors the Prosperity Game for Infrastructure Surety with DOE, the PCCIP, and Sandia National Laboratories, to examine threats and vulnerabilities to critical infrastructures and identify possible solutions.
- April** NCC responds to the Red River Floods.
- May** The NCS and NSA co-sponsor a Federal Wireless Users Forum workshop to address mobile satellite systems, wide area data services, and commercial dispatch services.
- June** LTG David J. Kelley succeeds General Edmonds as Director, DISA, and Manager, NCS.
- July** NSIE examined Local Number Portability and its implications for the PSN.
- August** An NCS study, *The Electronic Intrusion Threat to NS/EP Telecommunications*, concludes that electronic intrusions can have serious ramifications for both the public network and NS/EP activities that rely on that network.
- October** The PCCIP submits its final report.
- December** NSTAC XX Meeting in Washington, D.C., marks the 15th anniversary of its founding.

1998

- February** NCC responds to the Solar Sunrise computer attack.
- May** President Clinton issues PDD-63, *Protecting America's Critical Infrastructures*.
- June** NSIE holds Insider Threat Workshop, providing a framework for understanding and managing the insider threat in the business environment.
- September** NSTAC XXI Meeting held in Washington, D.C.
- September** NSTAC issues *Year 2000 Problem Status Report*.
- October** The NSTAC sponsors the third R&D Exchange at Purdue University in West Lafayette, Indiana.

1999

- September** NCC conducted the first operational test of its Year 2000 (Y2K) response capabilities.
- April** Government and NSTAC NSIEs publish an assessment of the Risk to the Security of the Public Network. Findings concluded that old vulnerabilities are still being exploited, even though fixes are readily available. Importance of the PN and the value of the information flowing over it are increasingly making it a more valuable target.
- June** NSTAC XXII Meeting held in Washington, D.C.
- June** NSTAC Network Group published *Internet Report: An Examination of NS/EP Implications of Internet Technologies*.

2000

- February** A series of Distributed Denial of Service (DDoS) attacks occur within a span of 44 hours. The attacks demonstrated to the Nation how profoundly cyber attacks could affect users worldwide.
- March** The NCC designated as the Telecommunications Information Sharing and Analysis Center.
- May** NSTAC XXIII Meeting held in Colorado Springs, CO.
- May** NCC responds to the Love Letter Worm computer attack.
- July** The FCC released a Second Report and Order, FCC 00-242, on wireless Priority Access Service.
- September** The NSTAC sponsors the fourth R&D Exchange in Tulsa, Oklahoma.

BUSH ADMINISTRATION (2001-PRESENT)

2001

- January** Special Advisor to the President for Cyberspace Security forwards two Memoranda to the NCS directing it to complete several Critical Infrastructure Protection (CIP) activities.
- February** The NSTAC establishes the Legislative and Regulatory Task Force as a standing task force.
- April** The NCS CIP Integrated Product Team issues a report recommending specific external and internal strategies, roles, and activities for the NCS to undertake in the telecommunications CIP arena.
- May** OMNCS establishes the CIP Division.
- May** The National Coordinator for Security Infrastructure Protection and Counter-terrorism, NSC, tasks the NCS with planning and executing the deployment and operational management of the Cyber Warning Information Network.
- June** NSTAC XXIV Meeting held in Washington, D.C.

- September** Terrorists attack the World Trade Center and the Pentagon, taxing and overloading traditional telecommunications capabilities. The collapse of the World Trade Center towers destroys a large telephone switch and nearly a dozen cellular antenna sites in lower Manhattan.
- September** GETS reaches full operational capability.
- September** TSP and GETS capabilities are used to restore vital switches in New York's financial district and to give priority routing to 7,000 critical calls in Manhattan and Washington, D.C., after September 11, 2001.
- October** The United State Congress passes the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, also known as the USA PATRIOT Act.
- October** President Bush issues E.O. 13228, *Office of Homeland Security and the Homeland Security Council*, creating the Office of Homeland Security within the Executive Office of the President.
- October** President Bush issues E.O. 13231, *Critical Infrastructure Protection in the Information Age*.

2002

- February** Government and NSTAC NSIEs publish "An Assessment to the Risk to the Security of the PN." The document concluded that overall risk to the PN is growing due to new vulnerabilities, rapid technological changes, and the dynamic business environment that have outpaced deterrent and protection capabilities.
- March** NSTAC XXV Meeting held in Washington, DC.
- June** President Bush issues E.O. 13267, establishing the Department of Homeland Security (DHS) Transition Planning Office.
- June** NCS establishes a DHS transition team to manage the transition process internally and coordinate with the DHS Transition Planning Office.
- July** President Bush issues *The National Strategy for Homeland Security* to mobilize and organize the Nation to secure the U.S. from terrorist attacks.
- September** NSTAC celebrates its 20th Anniversary.
- October** First Emergency Notification Service pilot program designed to facilitate interoperability across existing systems, provide for data collection across infrastructures, use multiple communication technologies, 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.
- November** President Bush signed *The Homeland Security Act of 2002*, which established DHS.
- December** The OMNCS begins offering nationwide Wireless Priority Service immediate operating capability.

2003

- January** Governor Tom Ridge sworn in as the first secretary of the newly formed DHS.
- February** President Bush issues *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.
- February** President Bush issues *The National Strategy to Secure Cyberspace* in order to provide a framework for protecting the critical cyberspace infrastructure.
- February** President Bush signs omnibus E.O. 13286, *Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*.
- February** President Bush issues Homeland Security Presidential Directive 5 in an effort to ensure NS/EP telecommunications services are made available to the President, and other Government leaders and the emergency preparedness community, in the event of a crisis.
- March** The NCS officially transfers to DHS along with employees from 21 other agencies.
- March** The NSTAC’s R&D Task Force hosts the fifth R&D Exchange held at the Georgia Institute of Technology in Atlanta, Georgia.
- April** The NSTAC hosts the first quarterly NSTAC Principals’ Conference Call. The calls are initiated in an effort to keep the NSTAC Principals better informed of and more involved in the work of the Industry Executive Subcommittee.
- April** NSTAC XXVI Meeting held in Washington, DC.

GLOSSARY

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS (NCC)

The NCC assists the President, National Security Council (NSC), Director of the Office of Science and Technology Policy (OSTP) and the Director Office of Managements and Budget (OMB) in exercising telecommunications responsibilities and functions and the coordination of the planning for and provisioning of national security and emergency preparedness communications (NS/EP) for the Federal Government under all circumstances including an emergency attack, recovery, or reconstitution.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE (GETS)

GETS is a telecommunications service provided by the Office of the Manager, National Communications System (OMNCS). The program provides emergency access and priority processing in the local and long distance segments of the Public Switched Network (PSN). GETS Priority Identification Numbers (PINs) are issued to priority telecom users during emergency situations.

TELECOMMUNICATIONS SERVICE PRIORITY (TSP)

The TSP system is the regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of NS/EP telecommunications services. The TSP System is the only authorized mechanism for users to receive priority provisioning and restoration of NS/EP telecommunications services in emergency situations.

PRIORITY ACCESS SERVICE (PAS)

PAS provides a means for NS/EP telecommunications users to obtain priority access to available wireless radio channels when necessary to initiate emergency calls.

WIRELESS PRIORITY SERVICE (WPS)

OMNCS is implementing a program to provide a nationwide wireless priority access capability for NS/EP users. This capability was implemented to support the Olympics in Salt Lake City, Utah and is being fielded nationally on an expedited basis. OMNCS has formed several wireless initiatives such as: cellular priority services, enhanced satellite

capabilities, Personal Communications Service (PCS), and wireless data services to ensure NS/EP user requirements are understood and can be supported in their networks.

NETWORK DESIGN AND ANALYSIS CENTER (NDAC)

The OMNCS developed the NDAC, a secure computing facility for the design, modeling, and analysis of telecommunications networks. The NDAC enables the OMNCS to understand the operation and vulnerabilities of the PSN and how it performs under conditions of stress. NDAC software resources include network performance assessment tools, telecommunications modeling and simulation tools, and telecommunications geographic information systems.

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

The NSTAC provides analyses and recommendations from industry to the President regarding policy that affects NS/EP telecommunications. The NSTAC consists of 30 Presidentially appointed industry leaders who assist in identifying legislative and regulatory issues impacting NS/EP telecommunications.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS – INFORMATION SHARING AND ANALYSIS CENTER (ISAC)

The ISAC mission is to facilitate voluntary collaboration and information sharing among Government and industry ISAC participants in support of E.O. 12472 and the Critical Infrastructure Protection (CIP) goals of Presidential Decision Directive 63 (PDD-63). The ISAC gathers and analyzes “all hazards” information on vulnerabilities, threats, intrusions, and anomalies in order to avert or mitigate impact upon the telecommunications infrastructure. Information is sanitized and disseminated in accordance with information sharing agreements established by ISAC Participants.

EXECUTIVE ORDER (E.O.) 10995. “ASSIGNING TELECOMMUNICATIONS MANAGEMENT FUNCTIONS” (1962)

E.O. 10995 established the Office of Director of Telecommunications Management (DTM) within the Executive Office of the President (EOP). While the purpose was to centralize telecommunications

policy leadership and achieve a balanced and well-planned national and international telecommunications program, the communications priorities outlined in E.O. 10995 shifted significantly after the Cuban Missile Crisis.

E.O. 11490. “ASSIGNING EMERGENCY PREPAREDNESS FUNCTIONS TO FEDERAL DEPARTMENTS AND AGENCIES” (1969)

E.O. 11490 assigned emergency preparedness functions to Federal departments and agencies. This order has since been replaced; see E.O. 12656 and E.O. 13228.

E.O. 11556. “ASSIGNING TELECOMMUNICATIONS FUNCTIONS” (1970)

E.O. 11556 abolished both the Office of the DTM and the position of Special Assistant to the President for Telecommunications. Both were replaced by the Office of Telecommunications Policy (OTP) within the EOP to oversee the NCS process and capabilities.

E.O. 12046. “RELATING TO THE TRANSFER OF TELECOMMUNICATIONS FUNCTIONS” (1978)

E.O. 12046 transferred NCS activity to the National Security Council, which assumed responsibility for the development of policy, plans, programs, and standards for mobilization and use of the Nation’s telecommunications resources during emergencies. The Office of Science and Technology Policy was given the task of implementing these functions under policy guidance from the National Security Council.

E.O. 12382. “PRESIDENT’S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE” (1982)

E.O. 12382 established NSTAC, a group composed of 30 industry leaders who provide the President with knowledge, expertise, and insight on problems relating to the implementation of national security telecommunications policy. In 2003, the order was amended to realign the NSTAC’s reporting channel to the President through the Secretary of Homeland Security.

E.O. 12472. “ASSIGNMENT OF NATIONAL SECURITY TELECOMMUNICATIONS AND EMERGENCY PREPAREDNESS FUNCTIONS” (1984)

E.O. 12472 outlined a new organizational structure and technical path for creating an NCS and its

NS/EP telecommunications capabilities. It reaffirmed NCS’ mission to serve the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The Council of Principles (COP), Council of Representatives (COR), and the National Coordinating Center for Telecommunications (NCC) were all formed as a result of this order. In 2003, the order was amended to name the Secretary of Homeland Security as the new Executive Agent for the NCS and realign reporting channels through the Department of Homeland Security.

E.O. 12656. “ASSIGNMENT OF EMERGENCY PREPAREDNESS RESPONSIBILITIES” (1988)

E.O. 12656 provided the primary guidance on the functional NS/EP responsibilities of Federal departments and agencies. This order has been amended twice, most notably by E.O. 13228 (2003) when many of the Federal Emergency Management Agency’s coordinating responsibilities were transferred to the Department of Homeland Security.

E.O. 13228. “ESTABLISHING THE OFFICE OF HOMELAND SECURITY AND THE HOMELAND SECURITY COUNCIL” (2001)

E.O. 13228 represented the first and most important initial organization change in response to the events of September 11, 2001. The order established the new Office of Homeland Security (OHS) to develop a national strategy to secure the United States from terrorist threats or attacks, which was formally issued in July 2002. The order also established the Homeland Security Council as an advisory body to the President.

E.O. 13231. “CRITICAL INFRASTRUCTURE PROTECTION IN THE INFORMATION AGE” (2001)

E.O. 13231 revoked E.O. 13130 (1999) and provided a policy, which supersedes Presidential Directive 63. The order created a number of organizational entities, including the President’s Critical Infrastructure Protection Board and the National Infrastructure Advisory Council (NIAC).

PDD-63.

PDD63 issued in 1998, called for each federal department and agency to develop a plan for protecting its own critical infrastructure, as well as the development of “A National Infrastructure

Assurance Plan” to include information (and milestones) about vulnerabilities, remedial plans, warnings, responses, reconstruction, education and awareness, research and development, intelligence, international cooperation, and legislative and budgetary requirements. In addition to assigning lead agencies for different sectors of the economy, the directive led to the establishment of various warning and information centers.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD) 5. “MANAGEMENT OF DOMESTIC INCIDENTS” (2003).

The directive ensures the availability of NS/EP telecommunications services for the President, other national leaders, and the emergency preparedness and response community during times of crisis by creating a single policy for domestic incident management.

NATIONAL COMMUNICATIONS SYSTEM LEADERSHIP

	US Presidents	Executives Agents, NCS	Managers, NCS	Deputy Managers, NCS
1960	JOHN F. KENNEDY 1961-1963	ROBERT S. MCNAMARA Secretary of Defense 1961-1968	ALFRED D. STARBIRD Lieutenant General, USA 1963-1967	CLIFFORD D. MAY 1966-1969
	LYNDON B. JOHNSON 1963-1969	CLARK M. CLIFFORD Secretary of Defense 1968-1969	RICHARD P. KLOCKO Lieutenant General, USAF 1967-1971	IRVING R. OBENCHAIN Brigadier General, USA 1969-1970
	RICHARD M. NIXON 1969-1974	MELVIN R. LAIRD Secretary of Defense 1969-1973		
1970	GERALD R. FORD 1974-1977	ELLIOT L. RICHARDSON Secretary of Defense 1973	GORDON T. GOULD JR. Lieutenant General, USAF 1971-1974	CLIFFORD D. MAY 1970-1973
	JIMMY CARTER 1977-1981	JAMES R. SCHLESINGER Secretary of Defense 1973-1975	LEE M. PASCHALL Lieutenant General, USAF 1974-1978	JOSEPH ROSE 1973-1981
		DONALD H. RUMSFELD Secretary of Defense 1975-1977	SAMUEL L. GRAVELY, JR Vice Admiral, USN 1978-1980	
		HAROLD BROWN Secretary of Defense 1977-1981		
1980	RONALD W. REAGAN 1981-1989	CASPER W. WEINBERGER Secretary of Defense 1981-1987	WILLIAM J. HILSMAN Lieutenant General, USA 1980-1983	JOHN G. GRIMES 1981-1984
	GEORGE H.W. BUSH 1989-1993	FRANK C. CARLUCCI III Secretary of Defense 1987-1989	WINSTON D. POWERS Lieutenant General, USAF 1983-1987	BENHAM E. MORRIS 1984-1994
		RICHARD B. CHENEY Secretary of Defense 1989-1993	JOHN T. MYERS Lieutenant General, USA 1987-1990	
1990	WILLIAM J. CLINTON 1993-2000	LESTER ASPIN Secretary of Defense 1993-1994	THURMAN D. RODGER Lieutenant General, USA 1990-1991	ROBERT M. MARQUETTE, JR. 1994-1995
		WILLIAM J. PERRY Secretary of Defense 1994-1997	ALONZO E. SHORT, JR. Lieutenant General, USA 1991-1994	D. DIANE FOUNTAINE 1995-1999
		WILLIAM S. COHEN Secretary of Defense 1997-2000	ALBERT J. EDMONDS Lieutenant General, USAF 1994-1997	
			DAVID J. KELLEY Lieutenant General, USA 1997-1999	
2000	GEORGE W. BUSH 2001-	DONALD H. RUMSFELD Secretary of Defense 2001-2002	ROBERT LISCOUSKI Assistant Secretary for Infrastructure Protection, DHS 2003-	DIANN L. MCCOY 2000
		THOMAS RIDGE Secretary of Homeland Security 2003-		BRENTON C. GREENE 2001-

**National Communications System
701 South Courthouse Road
Arlington, Virginia
22204-2198**

www.ncs.gov