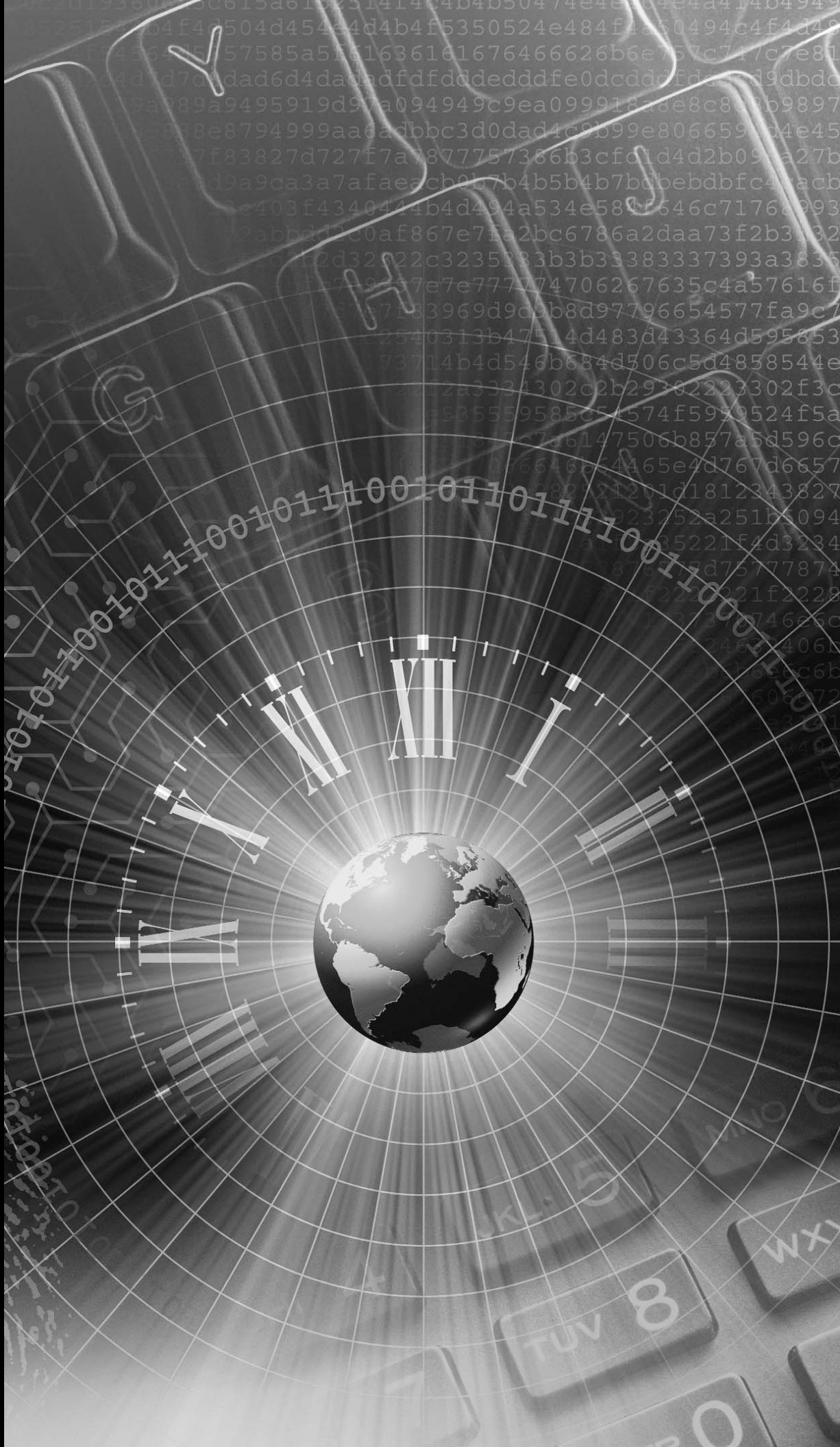
NATIONAL COMMUNICATIONS SYSTEM

EXPLORING SOLUTIONS FOR COMMUNICATIONS RELIABILITY

FY2001

The mission of the National Communications System (NCS) seeks to ensure that the Federal Government can adapt to new telecommunications technologies to meet its national security and emergency preparedness responsibilities under any circumstances. As telecommunications and information systems continue to evolve rapidly, the NCS will focus on identifying new technologies and solutions to meet the Nation's critical infrastructure needs. Building on its successful history of interagency cooperation and industry/Government partnership, the NCS will help guide the Nation through this fast-paced, ever-changing technological environment.



FISCAL YEAR 2001

NATIONAL COMMUNICATIONS SYSTEM

EXPLORING SOLUTIONS FOR COMMUNICATIONS RELIABILITY

Prepared by the Office of the Manager,
National Communications System

FOREWORD

The events of September 11, 2001, have had a profound effect on our Nation. They remind us of the critical roles that telecommunications and information technology play in all aspects of responding to and recovering from such events. In the aftermath of these events, the value of the emergency response programs put into place by the NCS over the past 18 years was clearly highlighted. In particular, the Government Emergency Telecommunications Service (GETS) ensured that national security and emergency preparedness (NS/EP) responders could effectively coordinate recovery efforts. Likewise, the Telecommunications Service Priority (TSP) program played a vital role in reestablishing essential communications capabilities and bringing Wall Street and others back online.

Under the experienced guidance of Mr. Brenton C. Greene, Deputy Manager, the NCS focused its resources on telecommunications critical infrastructure protection (CIP) activities and operations. The NCS continues to modify and develop new strategies to meet the evolving requirements of its role in telecommunications infrastructure protection.

One of our evolving requirements expanded our information-sharing capabilities. The National Coordinating Center for Telecommunications (NCC) established a watch desk in the Defense Information Systems Agency's Global Network Operations and Security Center (GNOSC). This watch desk facilitates a process of information sharing among the GNOSC, Joint Task Force-Computer Network Operations, Department of Defense Computer Emergency Response Team (CERT), and NCC.

On January 18, 2001, Mr. Richard A. Clarke, now Special Advisor to the President for Cyberspace Security, tasked the NCS to address several information-sharing, operational, and technical CIP activities aimed at enhancing industry and Government coordination. The NCS responded on May 15, outlining NCS CIP actions under way to address each of Mr. Clarke's taskings.

In response to direction from the National Security Council (NSC), the NCS is developing a Cyber Warning Information Network to provide dissemination of time-sensitive warnings of threats or attacks against our Nation's critical infrastructures.

Two Executive Orders signed by the President also expanded the mission focus of the NCS. Executive Order (E.O.) 13231, "Critical Infrastructure Protection in the Information Age," provides a framework for coordination and oversight of Government CIP efforts and programs, including some key NCS activities, such as information-sharing efforts, incident coordination and response, and outreach. This E.O. also impacts NCS-member departments and agencies as it changed the name of our Committee of Principals and expands our

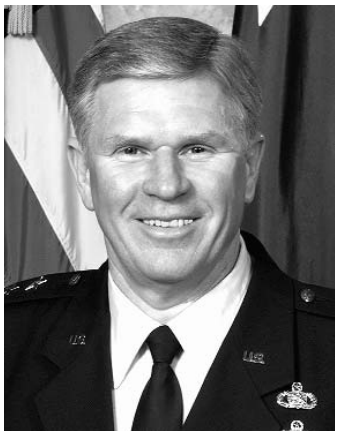
scope into critical infrastructure protection and convergence issues.

In response to the September 11th attacks, the President also signed E.O. 13228, establishing the Office of Homeland Security and the Homeland Security Council. This E.O. provided guidance for developing, coordinating, and implementing a national strategy to secure the United States from terrorist threats. The NCS is involved in the Homeland Security mission as it relates to the national strategy of detection, preparation, prevention, protection, response, and recovery of telecommunications assets from terrorist actions within our Homeland.

The NCS continued to address the impact of the convergence of telecommunications networks. In coordination with the NSC and Office of Science and Technology Policy, the NCS is currently analyzing the NS/EP implications of the convergence of the public switched network and next-generation packet networks. Similarly, the NCS continues to support efforts of the National Security Telecommunications Advisory Committee's Convergence Task Force, which is also examining network convergence security and reliability issues.

The GETS program reached full operational capability on September 30, marking a major milestone for the NCS. NS/EP users now receive priority treatment for GETS calls from more than 85 percent of access lines in the United States, as well as enhanced processing of calls to and from international locations. The effectiveness of this system was validated following the tragic events of September 11th when over 10,000 GETS calls were made in New York City and Washington, DC, with over a 95-percent success of completion rate over wireline networks. We are now focused on implementing a similar wireless capability.

Although the NCS expanded its responsibilities related to CIP in FY 2001 and will be leveraging those capabilities to address homeland security, its core mission remains the same. For nearly 40 years, the NCS has ensured that the national telecommunications infrastructure is responsive to the NS/EP needs of the President, Federal departments and agencies, and the NS/EP community as a whole. By continuing to serve as the focal point for industry-Government planning and coordination related to NS/EP telecommunications activities, the NCS is prepared to face the many challenges that lie ahead.



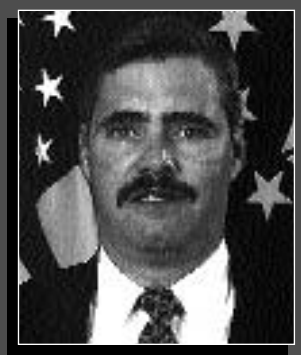
HARRY D. RADUEGE, JR.
Lieutenant General, USAF
Manager

Fire and rescue workers joined U.S. service members in unfurling a U.S. flag from the roof of the Pentagon in honor of those killed in Arlington and at the World Trade Center attack in New York on September 11, 2001.

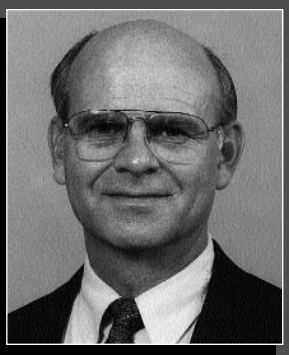
Defense Department photo

Mr. Brenton C. Greene
Deputy Manager

CAPT. J. Katharine Burton
Assistant Deputy Manager



Dr. Peter A. Fonash
Chief
Technology and
Programs Division



Frederick W. Herr
Acting Chief
Operations Division

Mr. Larry E. Wheeler
Chief
Plans and Resources Division

Col. Wilson D. Crafton
Chief
Customer Service Division

NCS Committee for National Security and Emergency Preparedness Communications

Department of State (DOS)
Mr. Fernando Burbano

Department of the Treasury (TREAS)
Mr. Thomas C. Weisner

Department of Defense (DOD)
Radm. Robert M. Nutwell, USN

Department of Justice (DOJ)
Mr. Michael Duffy

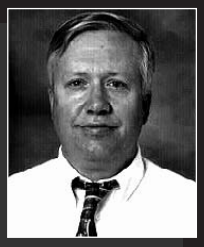
Department of the Interior (DOI)
Mr. Daryl W. White

United States Department of Agriculture (USDA)
Mr. Ira L. Hobbs

Department of Commerce (DOC)
Ms. Karen F. Hogan

Department of Health and Human Services (DHHS)
Dr. Robert F. Knouss

Department of Transportation (DOT)
Mr. Eugene K. Taylor, Jr.



Department of Energy (DOE)
Mr. Howard Landon

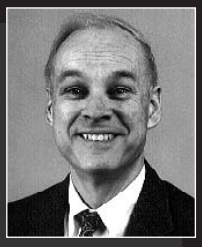
Department of Veterans Affairs (VA)
Mr. Howard Boyd

Federal Emergency Management Agency (FEMA)
Mr. G. Clay Hollister

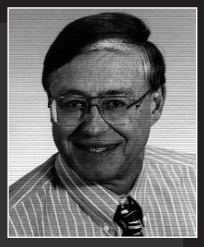
The Joint Staff (JS)
Ltg Joseph K. Kellogg USA

General Services Administration (GSA)
Ms. Sandra Bates

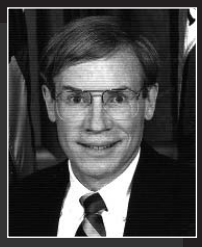
National Aeronautics and Space Administration (NASA)
Mr. Robert E. Spearing



Nuclear Regulatory Commission (NRC)
Mr. Richard Wessman



National Telecommunications and Information Administration (NTIA)
Mr. William T. Hatch



National Security Agency (NSA)
Mr. Michael G. Fleming

United States Postal Service (USPS)
Mr. Timothy J. Patterson

Federal Reserve Board (FRB)
Mr. Kenneth D. Buckley

Federal Communications Commission (FCC)
Mr. Arlan K. van Doorn

NCS Council of Representatives

Department of State (DOS)
Ms. Kimberly A. Godwin

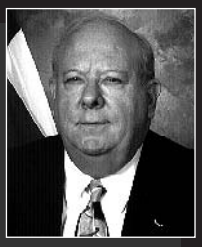
Department of the Treasury (TREAS)
Mr. Edd Barnes

Department of Defense (DOD)
Capt. Lynne Hicks

Department of Justice (DOJ)
Mr. Gary Laws

Department of the Interior (DOI)
Mr. James E. Dolezal

United States Department of Agriculture (USDA)
Ms. Brenda F. Boger



Department of Commerce (DOC)
Mr. Charles Cape

Department of Health and Human Services (DHHS)
Capt. Michael B. Anderson, USPHS

Department of Transportation (DOT)
Mr. James A. Harrell

Department of Energy (DOE)
Mr. Gordon Errington

Department of Veterans Affairs (VA)
Mr. Howard D. Boyd

Federal Emergency Management Agency (FEMA)
Dr. Joseph H. Massa

The Joint Staff (JS)
Col. John Reidt

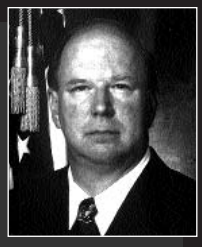
General Services Administration (GSA)
Mr. Thomas E. Sellers

National Aeronautics and Space Administration (NASA)
Mr. John C. Rodgers

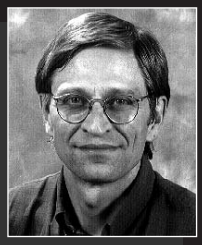
Nuclear Regulatory Commission (NRC)
Mr. Nadir Mamish

National Telecommunications and Information Administration (NTIA)
Mr. William A. Belote

National Security Agency (NSA)
Mr. R. Michael Green



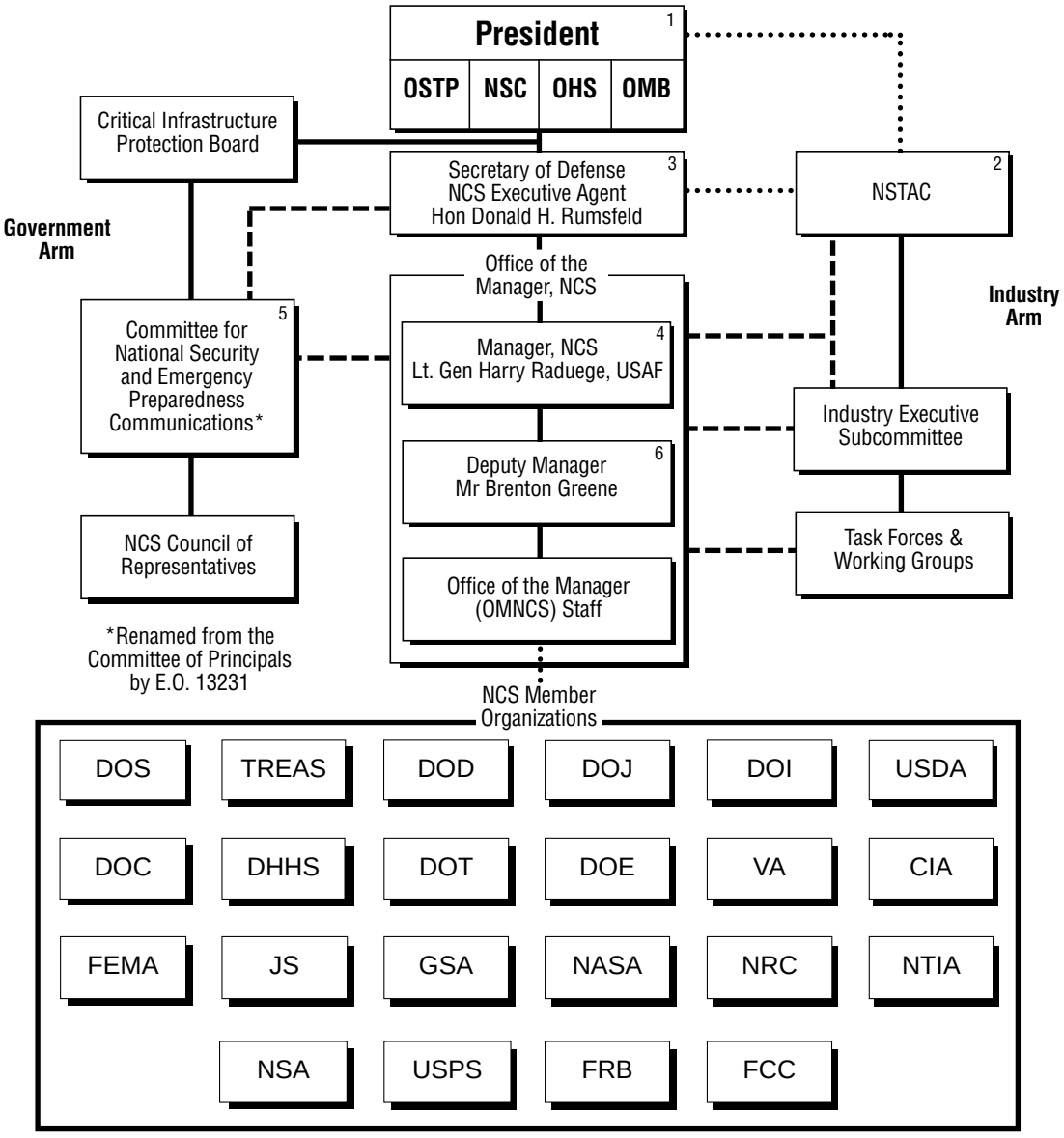
United States Postal Service (USPS)
Mr. Timothy J. Patterson



Federal Reserve Board (FRB)
Mr. Paul Grabow

Federal Communications Commission (FCC)
Mr. Douglas Kyle

THE NCS ORGANIZATION



1. Policy Direction and Direct Execution of War Powers Functions
2. National Security Telecommunications Advisory Committee
3. Executive Agent, NCS responsibilities assigned to Secretary of Defense by E.O. 12472, April 3, 1984
4. Director, DISA, serves as Manager, NCS
5. The Key Telecommunications Officers of the NCS Member Organizations who form one of 11 standing committees under the President Critical Infrastructure Protection Board, created by E.O. 13231, October 11, 2001
6. First line management position that is exclusively NCS

LEGEND

Direction ——————

Coordination ....

Advice – – – – – –

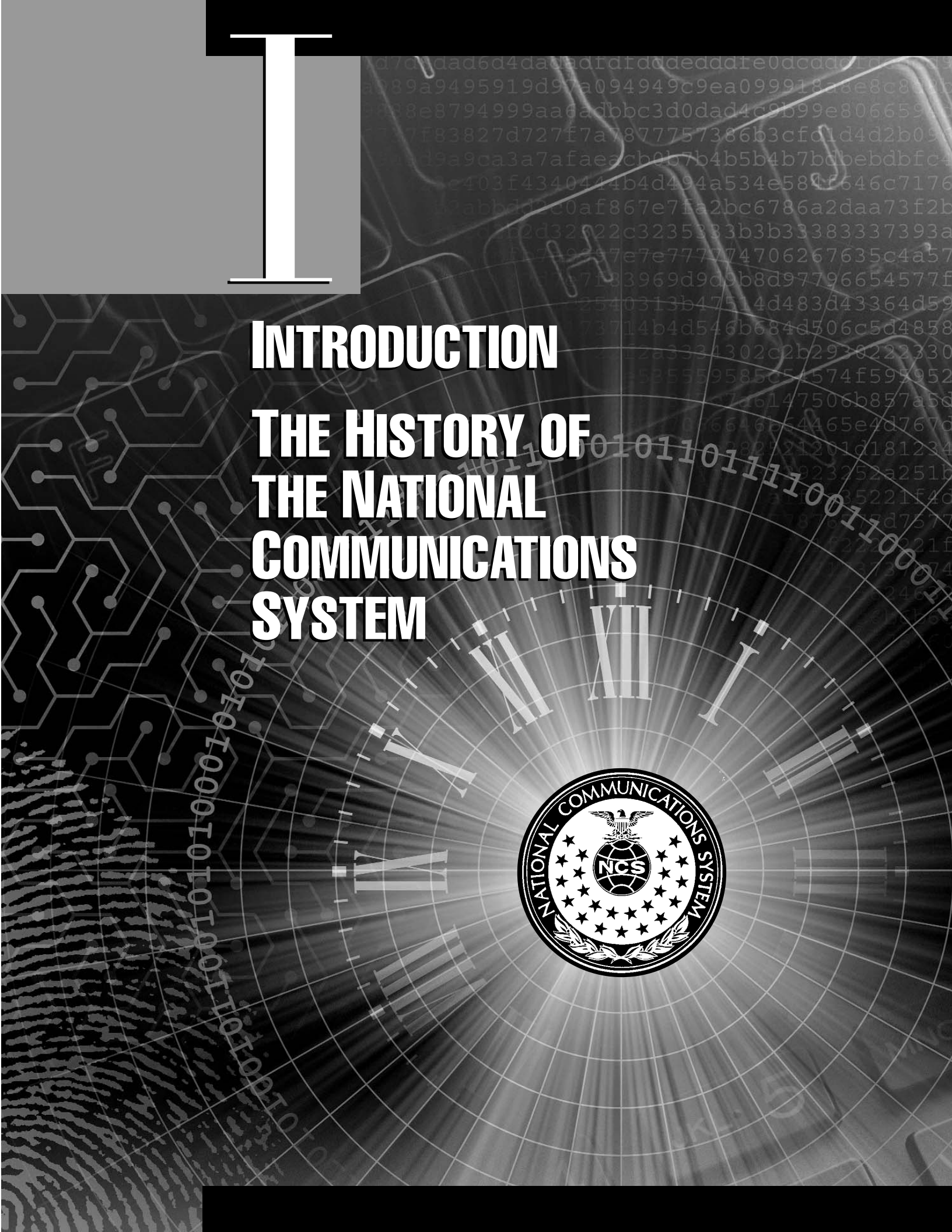
TABLE OF CONTENTS

LIST OF EXHIBITS

I

INTRODUCTION

THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM



I

INTRODUCTION

THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

The Office of the Manager, National Communications System, in coordination with the National Communications System (NCS) Committee of Principals (COP), publishes the *Fiscal Year (FY) 2001 National Communications System Report*. This report highlights significant national security and emergency preparedness (NS/EP) telecommunications events and major NCS initiatives, activities, and accomplishments during FY 2001.

BACKGROUND

On August 21, 1963, President John F. Kennedy signed a Presidential Memorandum ordering the formation of the NCS in the wake of shortfalls in communications supporting national security decision making during the 1962 Cuban Missile Crisis. The NCS's original mission was to "provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack." Today, the NCS continues to address NS/EP communications challenges, many of which have evolved with changes in technology, the marketplace, and national security threats.

Over the years, the role of telecommunications in supporting the Nation's NS/EP functions expanded. By the late 1970s, Government policy formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and recovery in the face of nuclear attack from the former Soviet Union. The expanded role of telecommunications was also evident in light of the growing complexity of Government, the rapid growth in telecommunications technologies and services, and the importance of telecommunications in responding to manmade and natural disasters.

Simultaneously, the impending divestiture of AT&T and the proliferation of telecommunications service providers complicated the means for satisfying NS/EP telecommunications requirements. In anticipation of losing a single point of contact within the industry for NS/EP telecommunications planning and service provisioning, President Ronald Reagan established the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order (E.O.) 12382 in 1982.

Composed of chief executives from major telecommunications and information technology companies, NSTAC would provide the President with a unified source of national security telecommunications policy expertise unobtainable solely within the Federal Government.

On April 3, 1984, President Reagan signed E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* which revitalized and expanded the NCS and created the National Coordinating Center for Telecommunications. This Executive Order formally reestablished the NCS structure to include the Secretary of Defense as the Executive Agent; the Manager, NCS, and staff; and an NCS Committee of Principals (COP) to represent Federal member organizations. The NCS's mission, as defined by E.O. 12472, is to assist the Executive Office of the President in the exercise of wartime and nonwartime emergency telecommunications responsibilities, and to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

An important dimension of the rechartered NCS is its mandate to serve as a focal point for industry and Government NS/EP telecommunications planning. Although the NCS COP is the mechanism for Federal interagency coordination, NSTAC and its working group structure are the means through which the NCS works with industry to address the range of NS/EP telecommunications issues.

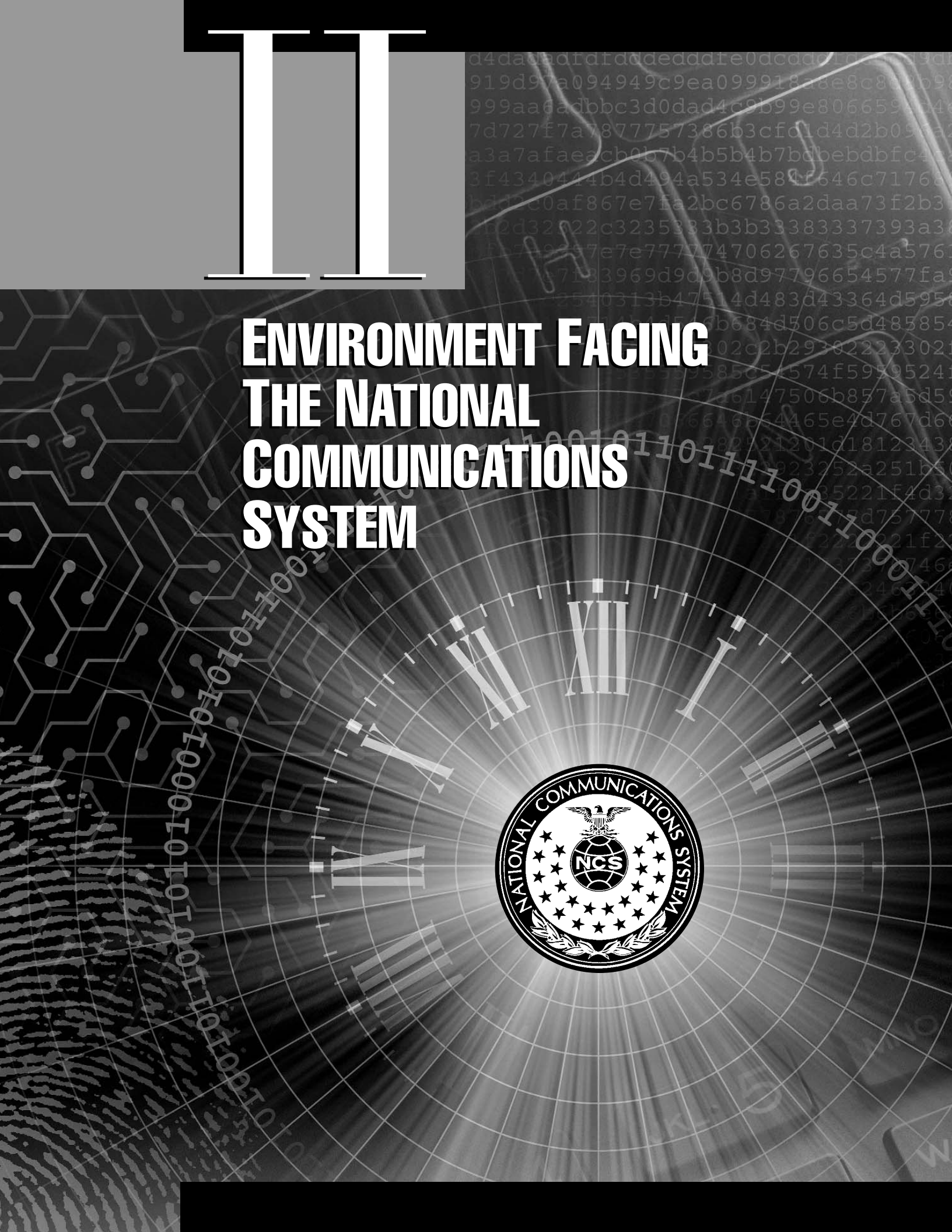
The information age makes the NCS mission of protecting and enhancing the national telecommunications infrastructure even more critical to national security. Today, the telecommunications infrastructure is critical not only because it provides traditional telephony service, but more importantly, because national information networks serve as an enabling infrastructure for most other national infrastructure services on which the Nation's economic, security, and societal functions depend.

Through the collective resources of its members and in partnership with industry, the NCS continues to meet the full range of NS/EP telecommunications challenges, from supporting military operations and responding to natural disasters, to protecting the telecommunications infrastructure from electronic intrusion. As it has for nearly 40 years, the NCS continues to respond to emerging challenges by leveraging its experience, working relationships, and capabilities to improve the security, reliability, and interoperability of the national telecommunications infrastructure.

Today, the NCS continues to address NS/EP communications challenges, many of which have evolved with changes in technology, the marketplace, and national security threats.

II

ENVIRONMENT FACING THE NATIONAL COMMUNICATIONS SYSTEM



II

Environment Facing The National Communications System

Attacks on the World Trade Center and Pentagon

At 8:46 a.m. on September 11, 2001, a hijacked plane, American Airlines Flight 11, crashed into the north tower of the World Trade Center (WTC). Subsequently, another hijacked plane, United Airlines Flight 175, crashed into the south tower of the WTC. Almost simultaneously, American Airlines Flight 77 crashed into the west side of the Pentagon. Both WTC towers collapsed later that morning, killing several thousand people. Nearly 200 people died in the Pentagon attack.

The events of September 11 redefined the need for the U.S. Government to better protect its citizens from terrorist attacks. In his speech to Congress on September 20, 2001, President George W. Bush declared his intention to create a new, Cabinet-level Office of Homeland Security and appointed Pennsylvania Governor Tom Ridge to lead the new office. Ridge will coordinate the activities of more than 40 Federal departments and agencies and forge domestic policy to defend the public against terrorism. The emergence of homeland security as a national priority is causing all Federal departments and agencies to reevaluate their physical and cyber security responsibilities. For the National Communications System (NCS), the national security and emergency preparedness (NS/EP) telecommunications mission and its evolving role in critical infrastructure protection (CIP) have taken on new national importance.

Critical Infrastructure Protection

Ensuring the viability of the telecommunications infrastructure, especially in the face of national security concerns associated with cyber attack, has become a focus of national policy recently. The

Clinton Administration carried out several policy initiatives to enhance CIP, including issuing Presidential Decision Directive 63, *Protecting America's Critical Infrastructures,* and publishing the first version of the *National Plan for Information Systems Protection*, which focused largely on Federal efforts to protect the Nation's critical, cyber-based infrastructures.

The George W. Bush Administration, early in its tenure, has also encouraged CIP initiatives, especially those relating to cyber defense in the telecommunications sector. The administration has stated that in an environment becoming increasingly technologically interconnected and therefore more vulnerable to threats that can disrupt key communication systems, immediate steps are necessary to ensure the Nation's communications infrastructures. In that context, the administration plans to solicit input from industry and Government to issue the second version of the *National Plan*, which will implement a national strategy for infrastructure assurance. The Bush Administration has also encouraged Government to work with the private sector to help pinpoint vulnerabilities, assess risk, and mitigate threats to the Nation's critical infrastructures. To facilitate information sharing between public and private sectors, the administration and Congress have expressed the need for legislation that exempts shared CIP information from the Freedom of Information Act (FOIA). In addition, the White House tasked the NCS to plan, fund, and execute a Cyber Warning Information Network (CWIN) to facilitate the dissemination of time-sensitive warnings regarding threats or attacks against the Nation's critical infrastructures. In October, the President plans to release Executive Order

Verizon Communications technicians splice severed wire pairs in their efforts to restore communications in Lower Manhattan following the September 11 terrorist attack on the World Trade Center. (Photo courtesy of the Federal Communications Commission.)

(E.O.) 13231, *Critical Infrastructure Protection in the Information Age*. Once enacted, E.O. 13231 will provide a framework for coordination and oversight of Government CIP efforts and programs, including some of the NCS's key CIP activities, such as information sharing efforts, incident coordination and response, and outreach.

On February 6, 2001, the House of Representatives reintroduced Concurrent Resolution 22, originally issued as H.Con.Res.285 in the 106th Congress, designating "cyberterrorism as an emerging threat to the national security of the United States which has the potentiality to cause great harm to the Nation's critical electronic infrastructure." The bill calls for an industry-Government partnership in combating cyberterrorism, a revision of the legal framework for the prosecution of hackers and cyberterrorists, and a new interagency study to assess the threat posed by cyberterrorists.

Amid the growing importance of CIP issues in Congress and the Bush Administration, the NCS directed more of its focus and resources in fiscal year (FY) 2001 toward telecommunications CIP-related activities and operations. Commonalities between NS/EP and CIP enable the NCS to anticipate and perform significant activities within the CIP arena.

To aid in developing a CIP strategy and to realign resources appropriately, the NCS created an Integrated Product Team (IPT). The IPT successfully defined the CIP landscape and the NCS's role in telecommunications infrastructure protection issues. On the basis of these findings, the IPT recommended reorganizing the OMNCS to include creating a CIP Division. The restructuring of the Office of the Manager, NCS (OMNCS) directly reflects the IPT's recommendations.

The NCS's focus on CIP is evident in other areas. For example, the National Coordinating Center for Telecommunications (NCC) established a watch desk in the Global Network Operations and Security Center (GNOSC) to facilitate information sharing among the GNOSC, Joint Task Force-Computer Network Operations, and the NCC. The NCC seeks to establish around-the-clock coverage at the GNOSC. In addition, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism tasked the NCS with addressing several operational and technical CIP information sharing activities aimed at enhancing industry-Government coordination. The NCS developed a response outlining the NCS CIP actions now under way and will address each of the National Coordinator's taskings.

As the NS/EP community faces emerging threats to the communications systems, the NCS continues to form key relationships with industry and Government agencies, to facilitate information sharing through its Telecommunications Information Sharing Analysis Center, and to generate solutions for fulfilling its NS/EP communications mission and meeting national objectives.

NETWORK CONVERGENCE

The growing reliance of industry and Government on packet-based networks continued to redefine the landscape for communications capabilities and services

To aid in developing a CIP strategy and to realign resources appropriately, the NCS created an Integrated Product Team (IPT).

during FY 2001. Traditional and nontraditional telecommunications carriers continued implementing packet-network infrastructure to satisfy increasing demand for diverse broadband services and to enable concurrent voice and data transport. Telecommunications service providers continued refining technologies, such as optical networks and third-generation wireless data networks, that promise to offer enhanced broadband capabilities in support of next generation network (NGN) services. Concurrently, because of their vast investments in traditional legacy infrastructure, service providers have relied on gateways to facilitate the interoperability of packet and circuit networks to provide seamless end-to-end services.

Although the evolution of telecommunications infrastructure promises enhanced services, it also presents challenges in meeting NS/EP requirements. Ensuring network security, reliability, and availability in support of NS/EP services and operations within this complex environment is ever more complicated. For instance, convergence of the control space of the public switched telephone network (PSTN) with packet networks via signaling gateways could increase PSTN vulnerabilities and impact traditional NS/EP services, such as the Government Emergency Telecommunications Service (GETS). Moreover, as the telecommunications infrastructure evolves toward the NGN, the NS/EP community may need additional packet network-based capabilities to continue fulfillment of NS/EP requirements.

The NCS is working to ensure that the national telecommunications infrastructure remains responsive to the NS/EP community's requirements in the new technological environment. The OMNCS is vigorously participating in industry and Government analyses related to the possible NS/EP impacts of network convergence and the NGN. In conjunction with the Office of Science and Technology Policy, Richard A. Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, established an interagency convergence subgroup under the Counter-Terrorism and National Preparedness Information Infrastructure Protection Assurance Group. The OMNCS is a key participant in this subgroup, which is called the Convergence Working Group (CWG). The CWG addresses issues associated with the convergence of the voice and data networks and the implications thereof for NS/EP telecommunications services. The OMNCS supports a broad range of activities, including providing subject-matter expertise via technical briefings, leading analyses of technical and security issues, and supporting development of CWG documentation and reports.

Similarly, the NCS has supported the efforts of the National Security Telecommunications Advisory Committee's (NSTAC) Convergence Task Force, which is also examining network convergence security and reliability issues. The outcomes of these analyses will help guide future OMNCS actions. In the meantime, the OMNCS is actively participating in standards organizations, such as the Internet Engineering Task Force and International Telecommunication Union, to ensure that NS/EP priority, security, and reliability requirements are considered during this period of network convergence and NGN emergence.

NETWORK SECURITY

In FY 2001, numerous cyber-related incidents continued to reveal the vulnerabilities of the evolving packet network infrastructure. Web site defacements, hacking attempts into industry and Government networks, and denial of service attacks remained prevalent. New viruses, such as "Anna Kournikova" and "NakedWife," emerged and proliferated throughout networks to cause widespread

disruptions. Additionally, cyber-based attacks brought real-world conflicts to the Internet arena. In February, Israel and the Palestinian Authority waged a series of parallel cyber attacks. In early May 2001, the tension between the United States and China extended to the cyber world, where U.S. industry and Government remained on heightened alert for possible hacking activity originating from China.

The cyber events of 2001 again demonstrated the speed and potentially far-reaching implications of cyber attacks. Furthermore, the events reconfirmed that emerging network vulnerabilities are heightened by the extremely interconnected nature of networks and by industry and Government interdependence on these networks.

The increased frequency and impact of cyber incidents in FY 2001 can be attributed to a variety of factors. First, hacking tools, long available on the Internet, have become more user-friendly and sophisticated. Their enhanced user-friendliness lowers the bar in terms of user skill, allowing unskilled individuals to use them with relative ease, while their sophistication heightens the potency of attacks. Second, the number of home users has grown, particularly those with "always on" broadband connections; and they are generally not very good at keeping up with patches, virus definitions, and similar enhancements. Previously separate categories of techniques and tools (e.g., sniffing, cracking, virus/worm creation) are being combined to multiply the effectiveness of any given attack. This compounding is due in part to the fact that operating systems and applications are becoming increasingly interlinked, allowing vulnerabilities in one to be leveraged against the other. Their growing complexity and sometimes-questionable development practices also make these software products more likely to have defects in the first place. Lastly, the vastly elevated pace of the vulnerability discovery/exploit creation/patch release cycle has significantly burdened those who must administer and maintain the systems being targeted; but the system administration function is frequently understaffed and those staff inadequately trained.

In FY 2001, many local and State governments took steps to battle cyber crimes, promote CIP, and increase awareness of the cyber threat. This heightened awareness should continue and lead to more industry-Government coordination to protect the Nation's critical infrastructures. The NCS has a long history of facilitating industry-Government coordination through mechanisms such as the President's NSTAC, the NCC, the Government and NSTAC Network Security Information Exchanges, and the Telecommunications Information Sharing and Analysis Center. The NCS will continue to use these forums to facilitate information sharing to alleviate the cyber threat.

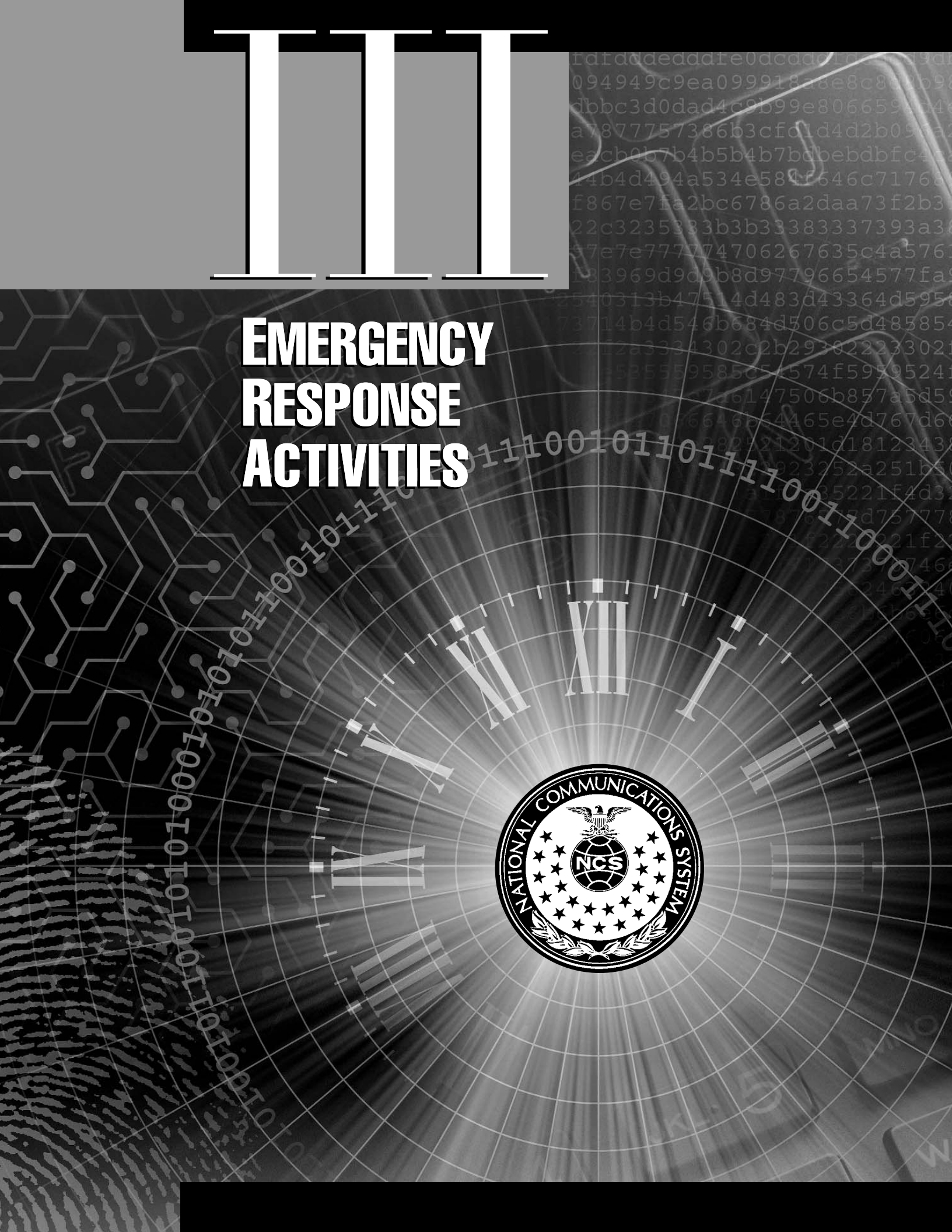
REPORT ORGANIZATION

The subsequent sections of this report detail the NCS FY 2001 activities and accomplishments undertaken to fulfill the NCS mission. Section III describes the emergency response activities of the OMNCS. Section IV contains a description of OMNCS NS/EP telecommunications support, activities, programs, and major interagency initiatives. Finally, Section V reviews the NS/EP telecommunications support and activities of the NCS member organizations.

The *FY 2001 National Communications System Report* reflects the NCS's commitment to meeting the full range of NS/EP telecommunications needs for the Nation under all circumstances.

III

EMERGENCY RESPONSE ACTIVITIES



III

EMERGENCY RESPONSE ACTIVITIES

On September 11, 2001, at 8:46 a.m., American Airlines Flight 11 from Boston to Los Angeles crashed into the north tower of the World Trade Center (WTC) in New York City. Subsequently, two other hijacked planes, United Airlines Flight 175 and American Airlines Flight 77, crashed into the south tower of the WTC and the west side of the Pentagon, respectively. The attacks caused both WTC towers to collapse, killing several thousand people. Nearly 200 people died in the Pentagon crash. Later that day, President George W. Bush declared the New York and Virginia areas to be Federal disaster sites.

Within minutes of the attacks, traditional telecommunications capabilities were taxed and overloaded. In New York, the collapse of the WTC towers destroyed a large telephone switch and nearly a dozen cellular antenna sites in lower Manhattan. Furthermore, telecommunications traffic flooded the networks in the New York and Washington, DC, areas into uselessness.[1]

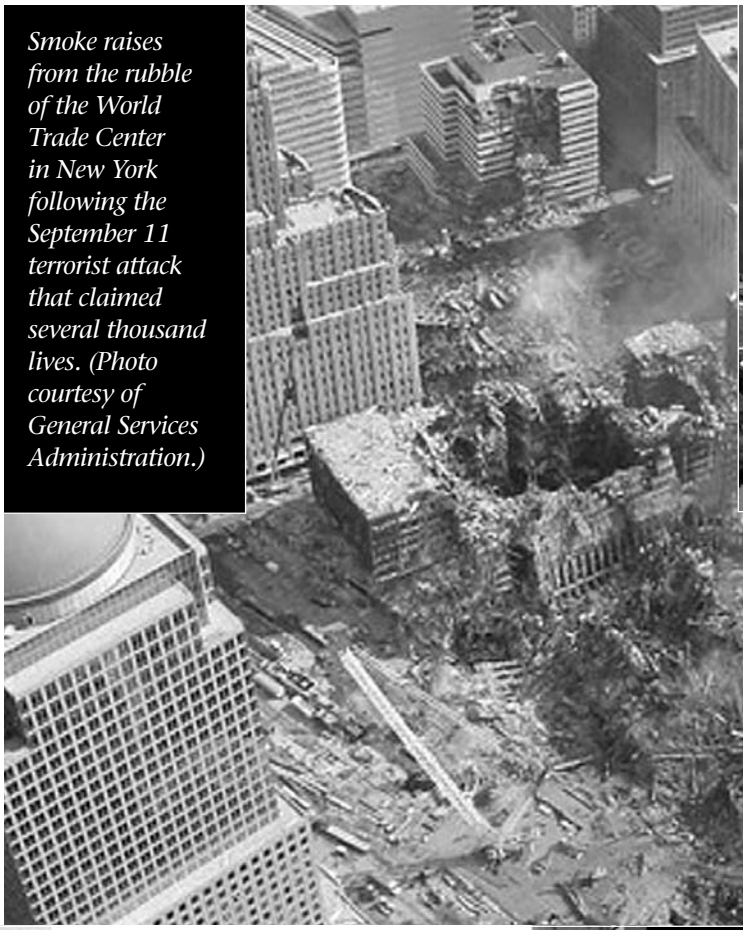
During these disasters, the National Communications System's (NCS) National Coordinating Center for Telecommunications (NCC) ensured that Federal, State, and local responders received national security and emergency preparedness (NS/EP) communications. In the immediate aftermath of the September 11 attacks, the NCS maintained 24-hour operations at four sites: the NCC, Federal Emergency Management Agency (FEMA) headquarters, the Department of Defense's Global Network Operations Support Center, and one remote continuity of operations site. Additionally, the NCS deployed Individual Mobilization Augmentees (IMA) to three FEMA Regional Operations Centers.

Between September 11 and September 30, the NCS received 552 Telecommunications Service Priority (TSP) provisioning requests from 46 organizations, including 74 from the Federal Bureau of Investigation (FBI), 53 from the Port Authority of New York, and 83 from the Federal Reserve Board. Within that same time frame, the Office of the Manager, National Communications System issued

[1] Noam, Eli M. "Testing the Communications Network," *New York Times*, September 24, 2001.

more than 1,000 Government Emergency Telecommunications Service (GETS) emergency personal identification numbers (PIN) to several agencies, including the National Security Council; FBI; the National Military Command Center; the Joint Chiefs of Staff; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Director of the National Security Agency and his immediate staff. The number cited does not include PINs issued from stockpiles at user sites.

In addition to responding to the attacks on the WTC and the Pentagon, the NCS ensured that Federal, State, and local responders received NS/EP communications support during other Presidentially declared disasters in fiscal year (FY) 2001. For example, the NCS provided communications support to disaster relief efforts in the aftermath of Tropical Storm Allison and the Seattle earthquakes. The NCS deployed three IMAs to assist in the storm recovery efforts and one IMA to assist in the earthquake recovery efforts.



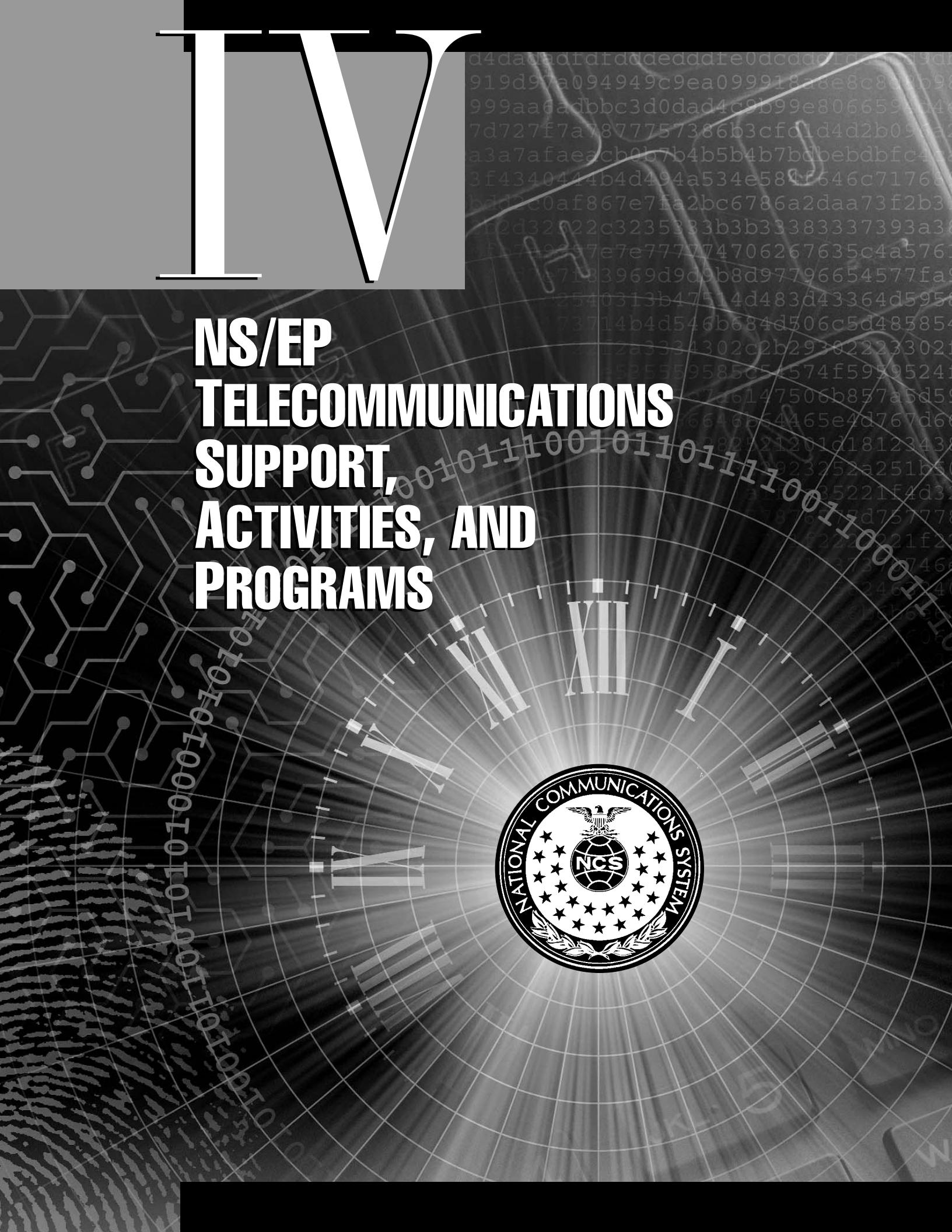
Smoke raises from the rubble of the World Trade Center in New York following the September 11 terrorist attack that claimed several thousand lives. (Photo courtesy of General Services Administration.)

Smoke and flames rise over the Pentagon following a terrorist crash of a commercial airliner into the side of the building on September 11, 2001. The attack killed 125 people at the Pentagon, in addition to the 64 passengers on the aircraft. (Photo by Gerry Gilmore, American Forces Information Service.).

New York fire fighters battle fires burning in the rubble of World Trade Center Building #7. (Photo courtesy of the Federal Communications Commission.)

IV

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS



IV

NS/EP Telecommunications Support, Activities, and Programs

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS), the National Communications System (NCS), and the national security and emergency preparedness (NS/EP) community during fiscal year (FY) 2001.

LEADERSHIP CHANGES

On April 2, 2001, Brenton C. Greene became the 10th Deputy Manager of the NCS, replacing Diann L. McCoy. Mr. Greene was formerly the manager for critical infrastructure protection programs for Sandia National Laboratories. Ms. McCoy assumed duties as the Defense Information Systems Agency's (DISA) Deputy Director for Information Engineering (D6) and Commander, Joint Information Engineering Organization.

Captain J. Katharine Burton, U.S. Navy, became the Assistant Deputy Manager of the NCS on September 4, 2001. CAPT Burton had previously served as the staff director, Defense-Wide Information Assurance Program, in the Information and Infrastructure Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I).

Frederick W. Herr, formerly Chief, Customer Service Division, became the Acting Chief, Operations Division, in May 2001. He replaced Navy Captain Lynne Hicks, now assigned to the OASD/C3I. In June 2001, Air Force Colonel Wilson D. Crafton, formerly a staff analyst at OASD/C3I, became Chief, Customer Service Division.

CRITICAL INFRASTRUCTURE PROTECTION INTEGRATED PRODUCT TEAM

In January 2001, the NCS established a critical infrastructure protection (CIP) integrated product team (IPT) to develop a comprehensive CIP strategy for the NCS.

The Manager, NCS, formed the IPT as a result of growing concerns about the NCS's role in CIP in a rapidly changing environment. The IPT's report, issued in April 2001, identifies a CIP strategy in telecommunications and provides implementing recommendations to ensure that activities are properly coordinated within the NCS, fully integrated with other NCS programs and activities, and coordinated with related initiatives in DISA, in the Department of Defense (DOD), and throughout the Federal Government. The IPT defined telecommunications CIP (T-CIP) as "risk management actions that are intended to prevent a threat from attempting to, or succeeding at, destroying or incapacitating the telecommunications infrastructure." To ensure that views from across the NCS were heard, the IPT members represented each OMNCS division. Working as a cohesive unit, the group—

- Conducted extensive research and analysis into the NCS's T-CIP mission, roles, and activities
- Interviewed numerous internal and external stakeholders
- Examined operational and political challenges
- Identified current and future threats in the changing T-CIP environment
- Explored internal organizational resources and structures affecting the NCS's T-CIP programs.

The IPT's report recommended specific external and internal strategies, roles, and activities for the NCS to undertake in the T-CIP arena, and the OMNCS is now implementing those recommendations.

TECHNOLOGY AND PROGRAMS DIVISION

The Technology and Programs Division implements evolutionary NS/EP communications capabilities for an enduring and effective telecommunications infrastructure. The division develops technical studies, analyses, and standards that promote the reliability, security, and interoperability of NS/EP telecommunications.

The division's objectives emphasize incorporating advanced, cost-effective technology into NS/EP communications programs. To fulfill this mission, division personnel evaluate emerging technologies to mitigate technical interoperability impediments and to satisfy NS/EP requirements. They use this information as they participate in industry and international standards organization meetings to ensure that NS/EP requirements are incorporated into the standards and recommendations developed.

The following paragraphs highlight the major projects undertaken by the Technology and Programs Division during FY 2001.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

BACKGROUND

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. GETS satisfies these requirements by providing specialized processing in local and long distance telephone networks. The program ensures GETS users of a high rate of successful call

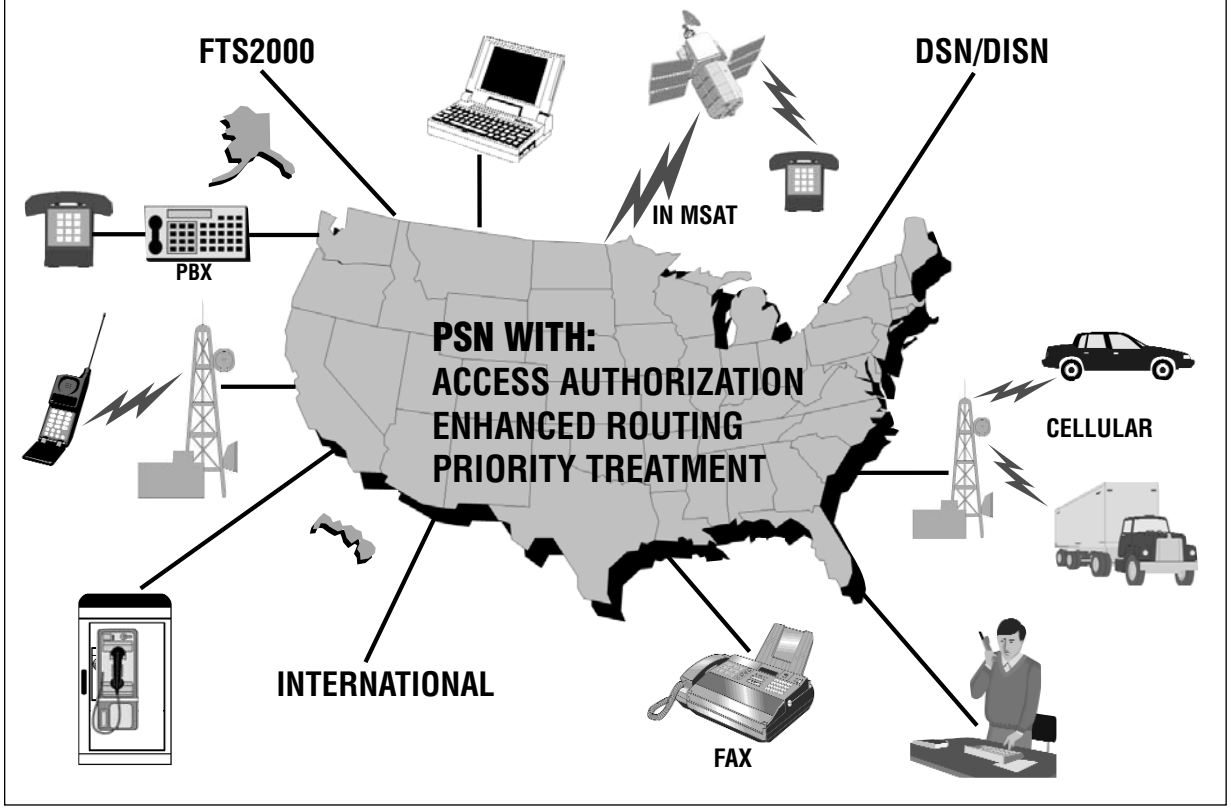
completion during network congestion or outages arising from natural or manmade disasters. GETS reached full operational capability on September 30, 2001.

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient and reliable technology for supporting a service that would meet NS/EP mission requirements. GETS leverages the PSN's vast resources—a $300 billion infrastructure with more than 190 million access lines, 26,000 switches, and 2,200 mobile switching centers. The ubiquitous, robust, and flexible PSN supports more than 90 percent of the Government's telecommunications needs. Despite its enormous size and complexity, it averages 99.999 percent availability. Exhibit 3-1 shows the various means of communication through which GETS users can access the service.

The initial objective of GETS planners was to expeditiously field a service that would provide priority call treatment. They would then incrementally improve the service with specialized calling features. The strategy of developing GETS by using existing assets of the PSN enabled early implementation and provided technical currency by leveraging the continual improvements made by the industry. Embedding GETS primarily within the software resources of the PSN also made it unnecessary for the Government to purchase, install, maintain, and eventually update network equipment.

The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This approach resulted in separate GETS contracts with AT&T, MCI WorldCom (now WorldCom), and Sprint, the three largest IXCs. They are,

Exhibit 3-1 **GETS Operational Concept**



therefore, the only IXCs that can authorize GETS calls. As such, access to these carriers must be available at all PSN end offices and mobile switching centers (MSC). Although the IXCs began with the same basic set of functional requirements, the implementation approach pursued by each IXC and the inherent differences in the structure of the IXCs' respective networks caused the operational features and capabilities to differ slightly among the providers.

The primary focus of feature implementation has now shifted to the local exchange carrier (LEC) networks. DynCorp (formerly GTE Government Systems Division) was awarded a separate integration contract (IC) for assimilating LEC implementation of GETS and for overall GETS operation, administration, and maintenance services. Advanced intelligent network (AIN) technology provided the basis for the first phase of GETS LEC feature deployment, which is alternate carrier routing (ACR). ACR enhances access by automatically attempting all three GETS IXCs.

The GETS IC entered into contracts with four primary switch manufacturers—Lucent Technologies, Nortel Networks, AG Communications Systems (AGCS), and Siemens—for the implementation of priority treatment and enhanced routing features on their products. The GETS IC also contracted with LECs to deploy and operate these features. During FY 2001, feature deployment continued in the LECs on Nortel, Lucent, AGCS, and Siemens switches. As of September 30, 2001, all switches running software supporting GETS features in LECs under contract had GETS features in place. GETS features will be deployed on additional switches as they are upgraded to required software releases or as additional LECs are brought under contract.

The OMNCS also is investigating potential enhancements in other PSN areas. The GETS IC, through a contract with Lucent, is investigating MSCs that provide end-office functionality to wireless networks. Features under consideration include not only the extension of features currently deployed in wireline switches but also enhanced capabilities to obtain priority access to air channels from the user handset to the wireless network.

Based on proposals submitted by the switch vendors that leverage recently completed LEC feature development, the GETS Program is now deploying enhancements that would help GETS calls terminate from the PSN to customer premises (such as private branch exchanges [PBX]). These enhancements also simplify carrier provisioning of GETS features.

As the PN evolves into packet-based technology to support voice traffic, the GETS Program Management Office (PMO) is working with industry to maximize and protect the NS/EP community's substantial investment in circuit-switched network enhancements. This work includes one-on-one meetings with carriers and vendors to gain understanding of their network evolution plans, participation in standards bodies influencing how NS/EP calls may be processed in packet networks, and development of requirements related to packet-based call processing in acquisition packages for the IC and IXC follow-on contracts scheduled for 2003.

OPERATIONS AND FEATURES

Access to GETS is quick and simple: users dial a universal access number (1-710-NCS-GETS) using common telephone equipment, such as a standard desk set, secure telephone (such as Secure Telephone Unit-Third Generation [STU-III]), facsimile, modem, or wireless telephone. Telephones on the Federal Telecommunications System 2001 (FTS2001) Network, the Diplomatic Telecommunications Service, and the Defense Information Systems Network (DISN) can also access GETS.

When a user dials a GETS access number, a tone prompts the user to enter a personal identification number (PIN); a voice prompt then asks for a destination telephone number. Even if the access control system fails, a fail open feature will allow authorized users to complete their GETS calls. The utility of this feature was demonstrated during the September 11 attacks on America.

PRIORITY TREATMENT AVAILABILITY

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS has worked to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks. In 1993, the American National Standards Institute (ANSI) approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993, which provides a classmark for NS/EP-related signaling messages and a high-priority level for those messages within the SS7 message priority scheme. ANSI reaffirmed this standard in December 1999. The classmark allows NS/EP calls to be recognized in any network, facilitating the application of available GETS features. The high-priority level for the signaling message makes it likely that GETS calls will continue to be processed if congestion occurs within the SS7 network itself.

In 1996, ANSI modified the SS7 standards so that NS/EP traffic would have a higher signaling priority level than plain old telephone service (POTS) traffic would. The GETS Program worked closely with the Network Interconnection Interoperability Forum (NIIF) to facilitate industry migration to the standard related to SS7 message priority. GETS representatives worked with the GETS Team Forum members to reach consensus on a migration plan and schedule. Their work resulted in the adoption of the Initial Address Message (IAM) Implementation Plan, which was brought to the NIIF.

In December 1997, NIIF accepted Issue No. 0095, *Implementing POTS IAM Priority Level 0*. On the basis of the resolution, all members submitted plans, providing specific dates indicating when they will comply with the standard. NIIF members should transition noncompliant switches during 2001. The switches that either comply or will soon comply with the standard will serve more than 90 percent of the access lines in the Nation.

INTEROPERABILITY

Many of the significant challenges facing GETS stem from interoperation with other networks and service providers. The GETS PMO is working with industry to ensure consistent, toll-free treatment for service users at privately owned user-to-network access devices. The GETS PMO also is working in concert with the General Services Administration (GSA) to provide FTS2001 users with improved priority for on-net GETS calls and priority access to the PSN for GETS off-net calls.

Like other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the *Telecommunications Act of 1996*. Resulting industry deregulation has led to a significant increase in the number of service providers. This environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin telephones and PBXs, in some service areas. Previous testing shows these problems to be particularly prevalent for coin telephones owned and operated by small businesses and PBXs operated by the hospitality industry (hotels and motels). Commonly encountered problems include the need to

deposit coins at a coin telephone before dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

Critical to solving the problem of toll-free access at privately owned devices is industry recognition of the 710 Numbering Plan Area (NPA) as nongeographic, emergency, and toll-free. To this end, the OMNCS is working with the North American Numbering Plan Administrator (NANPA) and the Federal Communications Commission (FCC) to issue guidance to industry regarding publicizing the 710 NPA. Publicity will give it stature as an emergency toll-free service per sections 228(c) and 276(b) of the Communications Act of 1934, as amended.

On the basis of this work, the NANPA issued a planning letter (PL-NANP-172, April 12, 1999) advising industry of the Government's use of the 710 NPA. This letter also notified owners and managers responsible for user-to-network access (including cellular and personal communications services networks, PBXs, and payphones) of the need to ensure that their equipment does not block 710 calls. In addition, Telcordia Technologies (formerly Bellcore) added a new section on Special Code 710 in the Local Exchange Routing Guide to include routing procedures for 710 calls.

In addition, the OMNCS is working with coin telephone industry groups, such as the American Public Communications Council and hospitality industry organizations and associations, to raise awareness of GETS as an emergency, toll-free service to be given treatment similar to that provided for 911 emergency, toll-free calls.

SUCCESSES

As a result of GETS reaching full operational capability, GETS users now receive end-to-end priority treatment from about 85 percent of access lines in the United States, priority treatment of 100 percent of GETS calls while transiting the three primary IXCs, and enhanced processing of calls to and from international locations. The GETS Program continues to work with industry to add enhancements and carriers to GETS and to ensure that the program evolves in step with the PSN.

GETS successfully supported response to natural disasters, particularly the Nisqually, Washington, earthquake on February 28, 2001, and the terrorist attacks on September 11, 2001. Responders completed a high percentage of GETS calls immediately after these events occurred.

In the past year, the GETS Program has continued to make significant progress in its outreach efforts to all levels of government (Federal, State, and local) and NS/EP qualifying industry organizations. The following increases in GETS PIN holdings have been realized during this period: Federal (33,920 to 39,639), State (3,950 to 5,927), Local (3,920 to 4,780), and industry (2,120 to 2,308). Total holdings rose from 43,910 to 52,654. More than 4,000 new GETS PINs were issued in the month following the September 11, 2001, attacks on the Pentagon and World Trade Center.

NS/EP COMMUNICATIONS OVER THE INTERNET

The OMNCS is assessing the impact of Internet technologies on NS/EP communications. Although the public Internet presently carries few critical NS/EP communications, NS/EP communications use is likely to increase as carriers implement Internet Protocol (IP) networks to support voice and data communications. Consequently, the OMNCS is assessing how IP network-PSN convergence might affect current NS/EP services (such as GETS and the Telecommunications Service Priority [TSP] Program). The OMNCS is also

spearheading the definition of NS/EP requirements for network convergence and for the unified, packet-based Next Generation Network (NGN). The NCS is actively participating in various Internet-related standards bodies, including the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU), to increase awareness of NS/EP requirements, including methods of obtaining priority services over the Internet.

FEDERAL WIRELESS USERS FORUM

The 14th and 15th workshops of the Federal Wireless Users' Forum (FWUF) were conducted in December 2000 and May 2001, respectively. The FWUF, NCS, and the Federal Wireless Policy Committee sponsored the workshops. FWUF objectives encompass the following:

- Educating Federal Government users about wireless telecommunications and associated issues
- Identifying wireless telecommunication needs of Federal Government users
- Facilitating information exchange with other user groups, standards organizations, manufacturers, and service providers to ensure that Government user wireless needs are met
- Supporting the interoperability of emerging wireless services and equipment by increasing participation in the formulation of Federal policy, wireless standards development, and other appropriate activities
- Requirements and issues identified at workshops are provided to the Federal Wireless Policy Committee, the Federal CIO Council, other Government decision-makers, wireless industry, and standards organizations.

WORKSHOP HIGHLIGHTS

A total of 137 individuals from Federal, State, and local government; equipment manufacturers; wireless service providers; and wireless industry representative organizations attended the workshops to discuss and address wireless issues. The workshops reviewed recent Government wireless activities, commercial wireless services with a particular emphasis on mobile Internet and wireless data, user wireless pilots, and wireless security. Dialogue sessions focusing on user requirements for commercial wireless services and user wireless pilots were held to further refine Government requirements and issues, as well as share lessons learned.

Dr. Peter Fonash, Chief, Technology and Programs Division, NCS, gave the keynote address at the 14th FWUF. He described NCS programs for NS/EP communications and the NCS's leadership role in the Information Sharing and Analysis Center (ISAC) for Critical Infrastructure Protection. Dr. Fonash recommended closer partnerships between industry and

The NCS is actively participating in various Internet-related standards bodies, including the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) . . .

Government to realize wireless priority access service (PAS) and to meet the challenges for seamless, secure, and reliable communications.

ADVANCED TECHNOLOGY GROUP

The NCS Advanced Technology Group (ATG) investigates new and emerging technologies that may prove beneficial to NS/EP users. Over the past year, the ATG researched a range of topics, from new ground-based wireless data communications systems to observations on the future of satellite communications. These technologies have the potential to revolutionize the way that NS/EP responders communicate during periods of NS/EP need.

TERRESTRIAL NETWORKS

Recent advances in terrestrial telecommunications networks include the testing of ultra-wideband wireless technology and new products available for high frequency (HF) electronic mail (e-mail). Both technologies hold the promise of becoming new alternatives for data transfer for NS/EP personnel. The ATG is investigating these technologies to better advise NS/EP personnel preparing for disaster responses.

Wireless Data Networks

An increasingly mobile workforce, both in the private sector and in the Government, is demanding access to remote data via e-mail, Internet, or intranets. This demand is fueling the development of wireless networks that can provide data to users on the go. The ATG is investigating the "Implementation of Priority Schemes in Mobile Ad-Hoc Networks over the 802.11 Medium Access Control Layer" and other wireless networks that may prove beneficial to NS/EP responders who need to set up temporary networks, such as those located in disaster field offices.

Ultra-Wideband Wireless

The NCS published a technical note in February 2001 on *Ultra-Wideband (UWB) Technology*. UWB is a revolutionary wireless technology used to transmit large amounts of digital data short distances (up to 230 feet) over a very wide bandwidth (from 1 gigahertz [GHz] up to 10 GHz), and at very low power levels (less than 0.5 milliwatt). Unlike typical radio frequency broadcasts that use continuous sine waves to transmit data, UWB uses precisely positioned pulses at specific time intervals to transmit the signals across a wide spectrum. This effort is accomplished by coordinating a transmitter and receiver to send and receive pulses with an accuracy of within trillionths of a second. Because of its unique characteristics, UWB technology is attractive not only for commercial applications but also for use in the Federal emergency response community.

Future UWB applications could include low-power wireless networks linking phones, computers, and televisions without the need for hard wiring, and also cell phones that could help determine a user's location for a 911 emergency operator. This technology could radically change how NS/EP personnel operate in search and rescue efforts and other crisis events.

HF Radio and E-Mail

A natural or manmade disaster can quickly overload local area communications systems, causing widespread interruption of essential telephone and Internet services. At times like these, HF radio can provide a communications path to the Internet for sending and receiving e-mail messages. Heightened interest in sending e-mail messages over HF radio has led the NCS and DISA to investigate this technology.

The NCS published a technical note in November 2000 entitled, *E-mail Over High Frequency Radio: Filling the Communications Gap During Unexpected Telephone Outages*. DISA

is writing a technical information bulletin and a Federal Telecommunications Recommendation addressing HF e-mail systems. In addition, the NCS sponsors monthly Shared Resources High Frequency Radio Program (SHARES) meetings that attract a large group of potential HF e-mail users.

SATELLITE NETWORKS

Satellite and stratospheric telecommunications systems offer the potential for alternative routing of NS/EP calls when natural or manmade events damage or stress the PSN. The NCS is continually investigating the utility of purchasing voice and data services from nonterrestrial service providers.

The Future of Satellite Communications

Changes in the satellite communications (SATCOM) marketplace continue to have an impact on NS/EP telecommunications. Several low Earth orbit satellite systems, such as Iridium, ICO, and Globalstar, experienced well-publicized setbacks in the past few years; but these systems represent only a small fraction of the SATCOM market. Recent projections indicate that the SATCOM market will continue to grow through the 2003 to 2005 time frame, with revenues predicted in the billions of dollars.

Two new classes of satellites being prototyped are the picosats and nanosats. These miniature satellites work together in a constellation that could someday replace large, expensive satellites. Picosats weigh 10 ounces each and are the smallest operational satellites ever sent into orbit. ATG is studying the development and deployment of these new satellites to understand how they will impact the future of NS/EP communications.

ADVANCED INTELLIGENT NETWORK

The AIN is a rapidly evolving telecommunications technology identified by the President's National Security Telecommunications Advisory Committee (NSTAC) and the OMNCS as potentially able to meet the NS/EP telecommunications needs of NCS member organizations.

AIN technology supports the telecommunications architecture consisting of signaling systems, switches, computer processors, databases, and transmission media. The convergence of these elements allows for customized software-defined network services that can be flexibly, rapidly, and cost-effectively configured to meet changing customer needs. Among other capabilities, AIN provides priority recognition, user authentication, enhanced routing, and network management alternatives in support of NS/EP contingency operations.

In the competitive market environment created by the *Telecommunications Act of 1996*, PN carriers are becoming increasingly dependent on AIN capabilities to deliver services to their customers. Carriers are using AIN to deploy local number portability (LNP), as mandated by the FCC, to open networks to competitive service providers and to meet customer demand for new service capabilities (such as mobility, data, Internet access).

The AIN efforts in the OMNCS address AIN-based technology applications for NS/EP with the following mission objectives:

- Assess AIN architectures, standards, and implementations
- Define, develop, and demonstrate AIN NS/EP applications
- Ensure NS/EP requirements influence the evolving AIN technology
- Facilitate integration into Government initiatives (such as GETS, DISN)
- Evaluate AIN security, survivability, reliability, and interoperability.

The OMNCS coordinates with industry and NCS member organizations to fulfill mission objectives and identify preliminary services that the OMNCS can introduce into NS/EP initiatives (such as GETS) through successful proof-of-concept demonstrations. The OMNCS is deploying AIN-based alternate carrier routing to support LEC-enhanced routing. In conjunction with AIN efforts, the GETS Program Office is pursuing use of the SS7-based HPC ANSI standard for further enhancements.

Intelligent network capabilities have reached a critical mass in the public telecommunications network. The industry's deployment of LNP service promises to bring near-universal AIN availability. The OMNCS continues to monitor FCC rulemakings that may affect AIN availability and participates in industry forums to communicate NS/EP needs. Currently, the OMNCS is evaluating the role of traditional intelligent network capabilities in emerging multimedia networks, intelligent devices, and future applications of the emerging wireless intelligent network. This applied research enables the AIN program to influence these promising new technologies in the developmental stages and ensure the continued efficacy of existing and future intelligent network applications.

FEDERAL TELECOMMUNICATIONS STANDARDS COMMITTEE

The Federal Telecommunications Standards Committee (FTSC), chaired by the Chief, Technology and Programs Division, OMNCS, continued to develop Federal telecommunications standards to meet specific Government and NS/EP requirements. Federal telecommunications standards development was based not only on evolving commercial standards but also on comments from industry, Government, and the public. The committee coordinated proposed Federal telecommunications standards with manufacturers, State and local governments, and the public. The committee forwards all proposed standards through the Manager, NCS, to the GSA or the National Institute for Standards and Technology, as applicable, for approval and publication.

PRIORITY SERVICES TEAM

The Priority Services Team addresses a prime NS/EP requirement: priority communications for governmental, civil, and other essential users of public telecommunications services in crisis situations. Recognizing that Internet and wireless communications have become increasingly vital to national security during crisis situations, the Priority Services Team focuses on these two telecommunications media by working proactively with industry in the following organizations of new telecommunications service development: Telecommunications Committee T1, Telecommunications Industry Association (TIA), ITU, IETF, TeleManagement Forum, and Project Telecommunication and Internet Protocol Harmonization over Networks (TIPHON).

The basic requirements for future NS/EP service definition and development in these organizations are priority establishment, priority access, dynamic restoration, authentication, security integrity, user location, resource management, multiprecedence levels, and optional preemption for the telecommunications evolution. The first area of focus is network convergence, such as where the public switched telephone network (PSTN) (a voice-based network infrastructure) interworks with the packet switched (data) PN. The second area is the transition to the fully integrated service structure of an NGN packet-based infrastructure.

The high-level technical areas under study to achieve fulfillment of NS/EP service requirements in these environments take into account the following: ingress/egress,

call control, gateway signaling, performance, routing restoration, management controls, authentication, security, and service level agreements (SLA). Technical approaches include the following:

▶ Firmly establishing NS/EP requirements in work programs of telecommunications industry standards organizations

▶ Developing and providing detailed technical proposals (such as NS/EP contributions) within industry standards programs and encouraging industry participants in these programs to make technical proposals to augment NCS proposals

▶ Integrating NS/EP technical service agreements into operational systems as an *inherent part of the underlying packet-based infrastructure* rather than a retrofitted fix in deployed systems, and investigating new features emerging in packet-based networks to enhance NS/EP operations (such as e-mail, instant messaging, multicast video, Web access, and tunneling).

NETWORK MODELING AND ANALYSIS

The OMNCS uses several network analysis tools and databases to conduct impact and vulnerability analyses on the commercial telecommunications infrastructure and the PN. The impact analyses determine characteristics such as surviving network connectivity following natural and manmade disruptions. Vulnerability analyses identify critical assets whose impairment could significantly degrade the network ability to fulfill NS/EP telecommunications objectives.

Maintaining and improving a valid telecommunications assets database for network modeling and simulation efforts is an ongoing challenge. In the past year, the physical network architecture of major

Exhibit 3-2 Priority Services Team's Significant Accomplishments

The following table reflects summaries of successful accomplishments stemming from the Priority Services Team's initiatives:

Telecommunications Committee T1

▶ Introduced NS/EP PAS wireless requirements and championed an ad hoc committee to draft a PAS technical report

▶ Introduced PAS requirements to Global Mobile Services North America and gained support from the global mobile services industry chief telecommunications officers

▶ Championed establishing an ad hoc committee to produce a PAS NS/EP implementation plan

▶ Introduced NS/EP "end-to-end" priority service wireless requirements

▶ Introduced requirements to support NS/EP in two backbone signaling systems, SS7 and Bearer Independent Call Control (BICC).

Telecommunications Industry Association

▶ Established a working group to pursue development of service standards to support wireless access to GETS

▶ Introduced a standards requirement document for development of an NS/EP wireless intelligent network (WIN) service control point

▶ Received acceptance for a WIN queuing standards requirements document

▶ Introduced an NS/EP wireless requirements document for end-to-end priority service in hybrid networks.

International Telecommunication Union

▶ Introduced NS/EP emergency communications requirements into several ITU-T study groups

▶ Developed and received approval for new ITU Recommendation F.106, International Emergency Multimedia Services, which specifies

functional requirements and service definition for NS/EP emergency communications

▶ Initiated development of an NS/EP priority mechanism and a special quality-of-service class in the H.323 (Packet-based Multimedia Communications Systems) family of ITU-T Recommendations

▶ Introduced end-to-end priority services to Special Study Group "IMT 2000 and Beyond"

▶ Introduced requirements to support international NS/EP in two backbone signaling systems, SS7 and BICC

▶ Introduced requirements to develop an interface for interchange of critical service management data among service providers, and for interchange of this data among service provider(s) and operational customers of telecommunications services.

Internet Engineering Task Force

▶ Introduced and published two Internet Drafts (with NS/EP specifications) to establish a framework to support an International Emergency Preference Scheme (IEPS) and the securing of prioritized emergency traffic in IP telephony.

TeleManagement Forum

▶ Received approval to include NS/EP service markers in the new version of an industry handbook on SLAs.

Project TIPHON

▶ Received approval for NS/EP IP-telephony applications in two draft technical requirements documents and one draft technical specification

▶ Initiated development of a new specification for security protection of NS/EP emergency communications.

Note: Additional detailed information on IEPS may be obtained from http://www.iepscheme.net.

Internet service providers, and their assets that directly support Government facilities were identified. Additionally, the models themselves have been reconfigured to address modified routing schemes resulting from the evolving public network architecture and emerging telecommunications technologies. The OMNCS provides its network modeling and analysis capabilities to its NCS member organizations and other Government organizations.

INFORMATION SHARING AND ANALYSIS SYSTEM DEVELOPMENT

The Infrastructure Integrity, Analysis, and Modeling (IIAM) branch of the Technology and Programs Division delivered an automated information sharing capability to the National Coordinating Center for Telecommunications-Information Sharing and Analysis Center (NCC-ISAC) in April. The newly accredited Information Sharing and Analysis System (ISAS) Version 1.6 provides NCC-ISAC participants with a virtual means for sharing information about network outages and cyber incidents.

Based on a system that was developed to abet the Y2K rollover, the ISAS supports a variety of functions, each with a distinct access control policy associated with its operation. Supported functions include—

▶ *Ticketing System:* Tickets are created on any issue; information related to ongoing resolution is recorded and tracked

▶ *Sharing Groups:* Multiple "sharing groups" support special interest groups, guest groups, or any other subgroup whose data should be segregated and protected from disclosure to the larger user community

▶ *Advisories:* General warnings distributed on impending or ongoing issues; may be associated with an existing ticket to provide supporting information

▶ *Message Forum:* Bulletin board-like service in which users create specific topic groups, post inquiries, or discuss related issues

▶ *Alerting Mechanisms*: Nonsensitive information instructing the recipient to check the ISAS because a specific condition was triggered, e.g., a ticket was changed, a new advisory was issued, or a new message or message forum was posted

▶ *Report Generation*: A canned report is preformatted based on predefined search criteria; an ad hoc report provides query flexibility by allowing the user to specify the search criteria

▶ *Document Library:* Contains electronic files intended for general distribution; serves as a repository for document sharing among participants

▶ *Point-of-Contact Directory:* Automatically includes ISAS users and may also include contact information for non-ISAS users.

Painstaking efforts have been made to protect the ISAS from both internal and external threats, given its objective of sharing sensitive corporate and cyber-incident data. Security features such as firewalls, intrusion detection devices, and public key infrastructure technologies were implemented to ensure the ISAS is as secure as possible.

Future NCC-ISAC support efforts of the IIAM branch will concentrate on exploring data correlation and analysis tools, information assurance tools, an information portal to access and disseminate open-source products, and the assessment of possible network enhancements.

OPERATIONS DIVISION

The Operations Division ensures the availability of critical NS/EP telecommunications services across the entire spectrum of emergencies. During FY 2001, two milestone events occurred that are likely to change the Operations Division significantly. The first was a focusing of the NCS on CIP. This began in January 2001 when the Manager directed that a study be initiated to identify a CIP strategy for the NCS. The initiative gained momentum with a series of taskings from the National Security Council for the NCS to undertake significant new CIP initiatives. The second event was the September 11 terrorist attacks on the World Trade Center and the Pentagon. While the response and recovery activities were still under way at the close of the fiscal year, the attacks have already and will undoubtedly continue to have significant impacts on what we do and how we do it. The following paragraphs describe activities of the Operations Division during FY 2001.

FOCUS ON CRITICAL INFRASTRUCTURE PROTECTION

In January 2001, the Manager established a team to recommend a CIP strategy for the OMNCS. The team's final report, entitled "Critical Infrastructure Protection Integrated Product Team Report: Recommendations for the Future" was issued on April 2, 2001. The report recommends six mission-related strategies for the OMNCS to pursue and one enabling strategy necessary for the OMNCS to focus its internal resources and processes. The report also recommends six roles the OMNCS should perform to implement the strategies and many specific activities to fulfill the roles. The OMNCS already carries out many of the identified roles and activities, but the challenge will be to expand

and improve the performance of them to a level sufficient to make substantial progress toward implementing the identified strategies. The Manager and Deputy Manager approved the report's recommendations, and the OMNCS was implementing them at the end of the fiscal year.

TERRORIST ATTACKS ON THE UNITED STATES

On September 11, 2001, the United States was stunned by terrorist attacks on the World Trade Center and the Pentagon and the crash of a terrorist-hijacked jet in Pennsylvania. The NCC immediately went into 24-hour, 7-days-per-week operation to assist in restoring damaged communications and provisioning new communications capability to aid in the recovery and subsequent investigation. The destruction of the World Trade Center and damage and destruction of a number of surrounding buildings presented a significant challenge for the telecommunications industry. Some telecommunications switches in the area were destroyed, while many others were damaged. In addition, telecommunications cables were cut, cable vaults were flooded, and electricity to the area was cut off, requiring use of backup generators that needed to be fueled regularly. Following is a list of some of the more significant activities within the NCC following the attacks:

▶ Coordinated access for telecommunications service providers into the "Red Zone" in Manhattan, ensuring restoration of NS/EP communications, and continued operation and viability of facilities, e.g., refueling of emergency generators.

▶ Issued more than 500 TSP orders, assisting the response/recovery effort and ensuring that the telecommunications services necessary for a successful opening of Wall Street were in place. TSP's continue to be issued to expedite provisioning of telecommunications services in support of Operation Enduring Freedom.

▶ Hosted daily conference calls among resident and nonresident members of the NCC to coordinate efforts, identify problems, and share information on progress.

▶ Coordinated access of the Wireless Emergency Response Team in the "Red Zone," to triangulate on emissions from cell phones and pagers, to aid in the search for victims.

▶ The NCC continued on 24X7 operations as the fiscal year ended.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS

The NCC continues to serve as the operations focal point for the initiation, coordination, restoration, and reconstitution of NS/EP communications services and facilities under all conditions of crises or emergency. The NCC efforts in FY 2001 focused on CIP

Paul Lacouture, President of Verizon Network Services Group, explains Verizon restoration efforts to Federal Communications Commission Chairman Michael Powell and others during Powell's visit to the World Trade Center area on September 19. (Photo courtesy of the Federal Communications Commission.)

activities, Telecom-ISAC, and international support activities.

CIP Activities: On January 18, 2001, the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, the National Security Council (NSC) sent a memorandum to the Assistant Secretary of Defense for Command, Control and Communications, and the Manager, NCS, requesting the NCS to take a number of actions relating to the protection of the telecommunications infrastructure. In response to that memorandum, the following actions were initiated:

- The NCC broadened its membership to include additional nontraditional service providers and equipment manufacturers. Development and implementation of additional strategies to further encourage new membership to the NCC and Telecom-ISAC were initiated and continue.

- In June 2001, the NCC established an NCS Watch Desk in the DOD's JTF-CNO to foster the sharing of classified DOD information with industry and coordinate information sharing among Government network operating centers.

- The Operations Division initiated the development of a conceptual framework and management plan for a "real-time synoptic view" to track abnormalities in traffic flow of major networks. In addition, extensive research into existing market capabilities advancing the "synoptic view" functionality was conducted.

- To facilitate the establishment of an Aerospace/Defense ISAC, members of the OMNCS met on numerous occasions with representatives of the Aerospace Industry Association to discuss experiences and lessons learned from establishing a Telecommunications ISAC.

Telecom-ISAC: The Telecom-ISAC serves as a central hub for sharing critical telecommunications information on vulnerabilities, threats, intrusions, and anomalies among participating companies and between industry and the Government. In April 2001, the NCC assumed full operational responsibility of the ISAS. The ISAS is designed to provide a virtual means for industry and Government to share and analyze information relating to the security of the telecommunications infrastructure.

International Support: The NCS has established an effective working relationship regarding telecommunications issues with both the Canadian Government and the telecommunications industry in Canada. In December 2000, the Manager, NCC, briefed the Canadian Telecommunications Planning Association on the role of the Telecom-ISAC. In addition, the NCC Manager presented a U.S. CIP overview to the Canadian National Emergency Telecommunications Committee.

ALERTING AND COORDINATION NETWORK

Prior to January 1, 2001, the National Telecommunications Alliance (NTA) managed and operated the Alerting and Coordinating

"In April 2001, the NCC assumed full operational responsibility of the ISAS."

Network (ACN) a switched, private line network to provide emergency communications among the Regional Bell Operating Companies, their suppliers, and certain Government agencies. The ACN is not dependent on the PSN, so it provides continued communications during disruptions, congestion, and outages affecting the PSN. When NTA went out of existence on January 1, 2001, the ACN was in jeopardy of being disbanded. Because the ACN provides emergency backup communications capability that could help coordinate response to and recovery from a widespread network outage, the Director, Office of Science and Technology Policy (OSTP), directed the NCS to take over the ACN.

Operational responsibility for the ACN has been incorporated into the NCC operations to serve as a vital coordination resource in the event of severe congestion or catastrophic damage to the PN. The OMNCS is working with industry to establish procedures for maintaining and utilizing the ACN and expanding its availability within the telecommunications infrastructure. The ACN can also provide for cross-infrastructure coordination in the event of outages in the telecommunications infrastructure affecting other infrastructures or outages in other infrastructures affecting telecommunications. The OMNCS will be seeking participants from other infrastructures to allow this capability to be realized.

CYBER WARNING INFORMATION NETWORK

By memorandum, dated May 30, 2001, the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, NSC, tasked the NCS with planning and executing the deployment and operational management of the Cyber Warning Information Network (CWIN). This is a three-phased development effort designed to facilitate the immediate sharing of critical cyber information within Government and, ultimately, with industry. Phase I, initiated during FY 2001, supports the development and implementation of operational capabilities and procedures beyond existing network capabilities in seven Federal watch centers in five geographically dispersed locations. Phase II, targeted for FY 2002, consists of deploying a dedicated network to support CWIN operations at the initial seven Federal centers. Phase III, targeted for FY 2003 and beyond, is designed to expand the CWIN to include other Federal Government locations and possibly locations in the private sector at the rate of about five per year.

NATIONAL TELECOMMUNICATIONS COORDINATING NETWORK-HIGH FREQUENCY

The National Telecommunications Coordinating Network-High Frequency (NTCN-HF) is managed by the NCS and comprises 22 industry and 34 Government HF radio stations located nationwide. Industry participation includes all of the major telephone service providers. During FY 2001, on-air operations throughout the NTCN-HF network increased. New NTCN-HF stations were established in Gettysburg, Pennsylvania (FCC); Honolulu, Hawaii (Verizon); and Lena Point, Alaska (AT&T).

NORTH ATLANTIC TREATY ORGANIZATION CIVIL COMMUNICATIONS PLANNING COMMITTEE

The OMNCS represents the United States on the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), its telecommunications working group, and other subsidiary bodies. The Department of State (DOS) detailee to the OMNCS is the head of delegation. CCPC purview extends to telecommunications and

postal services. The OMNCS accordingly consults closely with U.S. commercial telecommunications service providers and affected U.S. Government agencies and organizations. During FY 2001, the CCPC met twice in plenary session: once at NATO headquarters in Brussels, Belgium; and the other time in Sofia, Bulgaria. The CCPC's telecommunications working group met four times, and the postal working group met once.

Major CCPC FY 2001 activities and accomplishments were as follows:

▶ Approved the 2001-2002 CCPC work program based on NATO's new Strategic Concept and Ministerial Guidance. The work program includes civil support for alliance military operations, support for civil emergency planning, protection of the population against weapons of mass destruction, and cooperation with partner nations.

▶ Expanded the United States/United Kingdom effort to identify and test NATO-authorized secure voice equipment.

▶ Completed a paper on the Internet from a NATO civil emergency planning (CEP) point of view (led by the United States).

▶ Began implementing the new CCPC tasks and proceedings identified and approved in FY 2000.

▶ Began a series of visits to partner nations to brief their authorities on NATO CEP and develop help-effort programs. Trips were made to Azerbaijan, Armenia, and Georgia.

▶ Continued working with ITU national representatives in defining an international emergency preference schemes standard.

▶ Conducted a 2-day seminar with the three newest NATO nations, Czech Republic, Hungary, and Poland (host), which included briefings by three U.S. participants.

▶ Elected the U.S. Postal Representative to the chairmanship of the CCPC Postal Working Group, effective September 2001.

▶ The Alliance completed a major review of the role of the Senior Civil Emergency Planning Committee and will conclude with a thorough study of its subordinate boards and committees, including the CCPC.

▶ The U.S. Industry Advisor attended a 1-week NATO training course in Oberammergau, Germany.

TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM

The TSP Program, established by an FCC Report and Order dated November 17, 1988, provides a regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications services. FCC authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments. TSP efforts in FY 2001 focused on operations, information technology (IT) solutions, and outreach strategy.

TSP OPERATIONS

The OMNCS continued to facilitate coordination between industry and Government to ensure adherence to TSP responsibilities within the evolving telecommunications marketplace. Working closely with the TSP Oversight Committee, the OMNCS examined the rapidly changing telecommunications environment and assessed potential effects on the TSP Program. For example, a considerable number of new entrants into the telecommunications marketplace, specifically, competitive local exchange carriers, required information on the capabilities of the TSP Program. Subsequently, the OMNCS initiated an

aggressive outreach effort identifying new telecommunications vendors and informing them of their FCC-mandated TSP Program responsibilities.

The OMNCS facilitated meetings of the newly formed TSP Working Group, which provides a forum in which TSP Program users and vendors can discuss day-to-day TSP procedures. The working group focused its efforts on resolving technical TSP Program issues, such as the transfer of crucial TSP Program data among telecommunications vendors, subcontractors, TSP users, and the OMNCS.

A revalidation effort was initiated to ensure the accuracy of TSP codes designating critical NS/EP telecommunications circuits. To confirm that the TSP database contained valid and up-to-date information, organizations with expired TSP codes were contacted and informed of the urgent need to revalidate their data. More than 80 organizations were contacted during the initial phase of the revalidation effort.

As part of the emergency response activities following the September 11, 2001, terrorist attacks against the World Trade Center and the Pentagon, the OMNCS issued in excess of 600 new TSP provisioning assignments.

TSP INFORMATION TECHNOLOGY SOLUTIONS

The OMNCS continues to recognize the importance of IT solutions for improving TSP processing. During FY 2001, IT efforts focused on three areas: the Priority Telecommunications System (PTS) client/server, the TSP Web site, and the electronic forms (e-forms) application.

IT upgrades to the PTS client/server included replacing hardware and software and implementing a new computer platform. The new system enables faster processing of specific TSP requests and priority level assignments. The OMNCS continued to maintain a functional backup client/server database with valid data, ensuring continuity of TSP operations under any circumstances. Finally, the OMNCS instituted robust network security measures, enabling the PTS to complete its System Security Authorization Agreement and remain accredited through the DOD Information Technology Security Certification and Accreditation Process.

Throughout FY 2001, the TSP Web site http://tsp.ncs.gov was regularly enhanced and revised to distribute TSP Program information to existing and potential TSP clients. The site includes instructions for using the PTS and e-forms applications, which offer an easy, secure, and universal mechanism for performing various TSP processes.

TSP OUTREACH STRATEGY

In addition to outreach efforts to new telecommunications service providers, educating and training emergency responders about the TSP Program remained a priority. To that end, the OMNCS provided comprehensive training to potential vendors; Federal, State, and local users; and emergency response coordinators. Briefings were provided to the NCS Emergency Response Training (ERT) seminars and national trade association conferences, such as the National Emergency Number Association annual conference and trade show, as well as the Association of Public-Safety Communications Officials' annual conference and exposition. In addition, the OMNCS provided one-on-one training on the PTS client/server and the e-forms application and held classroom-style revalidation and reconciliation training sessions.

TELECOMMUNICATIONS ELECTRIC SERVICE PRIORITY

In 1987, the Department of Energy (DOE), in coordination with the NCS, developed the Telecommunications Electric Service Priority

(TESP) Program to enable essential national defense and civilian requirements to be met if an event, natural or manmade, disrupted electric supplies to critical telecommunications facilities. Management and administration of the TESP Program are the responsibility of OMNCS with assistance from DOE, State governments, and electric power utilities.

The OMNCS implemented an outreach strategy plan to increase the awareness of the TESP Program within the NS/EP community, focusing on large States that may encounter power supply problems resulting from energy deregulation. The outreach strategy included development of a TESP brochure and other information materials and establishment of a TESP Web site http://tesp.ncs.gov. These outreach tools provide an overview of the TESP Program and related processes and outline eligible critical facilities.

During FY 2001, the outreach effort included presenting TESP information at various NS/EP forums around the country, including NCS ERT seminars and national trade association conferences. The OMNCS plans to continue promoting the program and utilizing information technology initiatives to enhance the TESP process. The OMNCS also plans to implement remote access capabilities, providing an efficient means for participants to access and update the TESP database.

PRIORITY ACCESS SERVICE (PAS)

Over the past few years, wireless technology has become increasingly vital to the ability to coordinate and respond to crises, natural disasters, and incidents that threaten national security. Yet emergency situations often increase wireless communication usage, leading to network congestion and call blocking precisely when NS/EP personnel and disaster relief officials most need mobile communications. The events of September 11, 2001, highlighted how critical wireless communications capabilities are in times of crisis.

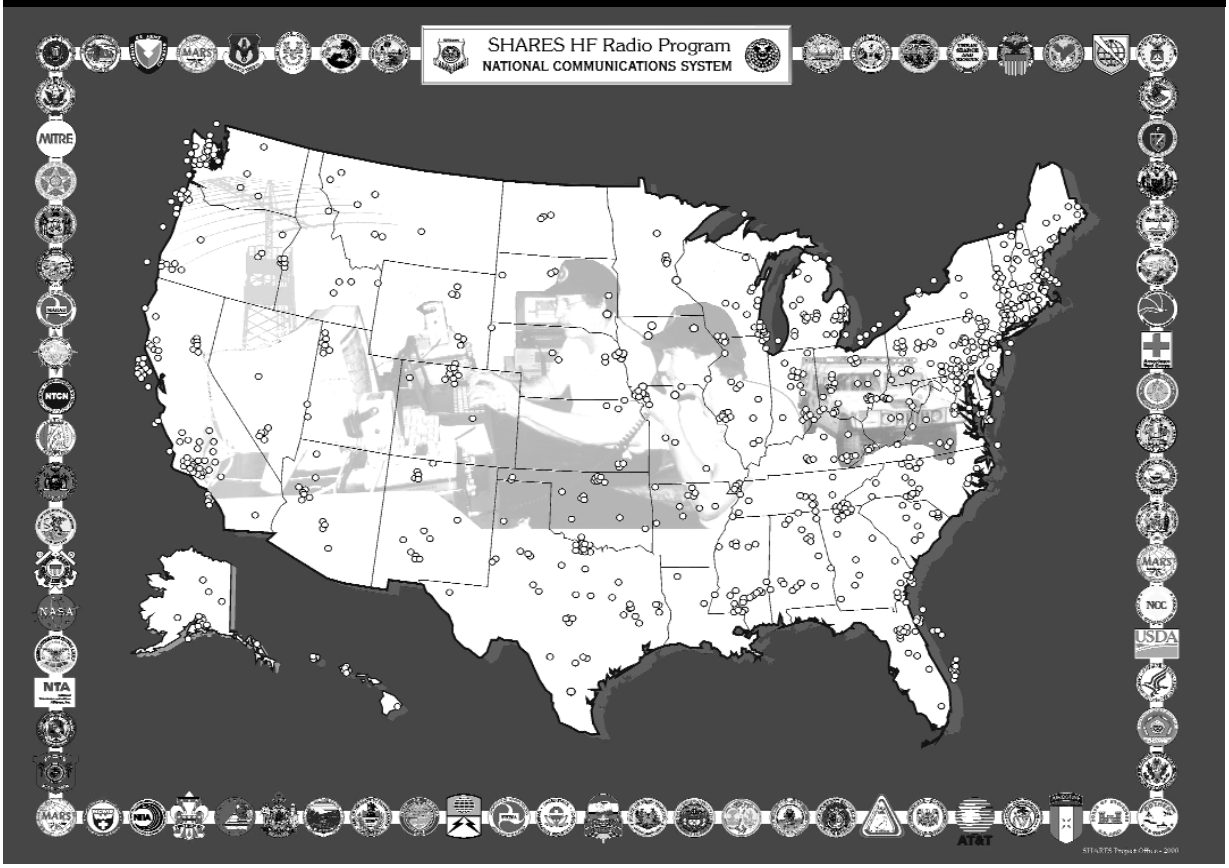
After studying this issue, in 1995 the President's NSTAC recommended establishing a wireless priority service for NS/EP users. In response, the NCS petitioned the FCC to allow wireless telecommunications service providers to provide priority cellular services for NS/EP. The FCC acted on this recommendation in FCC Report and Order No. 00-242, which became effective on October 10, 2000. The Report and Order allows commercial mobile radio service (CMRS) providers to offer PAS to public safety personnel at Federal, State, and local levels. CMRS providers offering PAS will provide authorized NS/EP personnel priority access to available wireless channels during emergency situations ahead of any other wireless users.

The OMNCS, working with industry leaders, industry associations, State representatives, and standards bodies, developed the framework for the PAS Program in its efforts to facilitate and coordinate the development of a cost-effective, uniform, nationwide wireless priority capability that enhances NS/EP user access to the PN. The OMNCS is working with the FCC to address the regulatory issues related to implementing a priority access service. In the interim, the OMNCS completed several studies investigating the feasibility and technical aspects of PAS implementation.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARES HF Radio Program continues to provide emergency communications in support of all-hazard's situations and special operations. SHARES incorporates the resources of 1,074 HF radio stations contributed by 86 industry, Federal, and State organizations into a nationwide emergency message-handling network.

Exhibit 3-3 **SHARES Coordination Network**



During FY 2001, SHARES conducted 22 on-air operations. Three SHARES Coordination Network Operational Level Change Notices were issued in response to Hurricane Debby, the Seattle earthquake, and the 2001 Presidential inauguration. The number of SHARES stations participating in readiness exercises continued to increase. During the weekly SHARES network tests, 6,984 Station Availability Reports were received. A total of 632 stations participated in the three SHARES nationwide readiness exercises conducted during the year.

The NCS expanded the number of NTCN-HF and NCS Regional Managers HF Radio Network (RM-HF) radio stations participating in SHARES. Forty-four NTCN-HF sites and 13 NCS RM-HF sites now participate in SHARES. With this expansion, all major telephone service providers and NCS Regional Managers are members of SHARES.

The SHARES HF Interoperability Working Group, a permanent body established under the Committee of Principals (COP) and the Council of Representatives (COR), continued to meet monthly to coordinate SHARES network activities and to address issues affecting interoperability of Federal HF radio systems. The working group, composed of 142 members representing 96 organizations, published the 10th edition of NCS Handbook 3-3-1, SHARES Directory; expanded the digital and Automatic Link Establishment (ALE) structure of the nationwide SHARES Coordination Network (see Exhibit 3-3), and supported technologies in HF e-mail and automatic HF interconnection into the PSN.

The working group also continued to expand awareness of SHARES throughout the Federal emergency preparedness community through the SHARES Outreach Program.

TRAINING, PLANNING, AND OPERATIONAL SUPPORT

The Operations Division is responsible for ensuring that a cadre of skilled civilian and military reservist personnel are qualified and ready to provide emergency response support during crises and emergencies. In an effort to meet this goal, the Operations Division sponsors a nationwide training program through:

- Telecommunications ERT seminars
- Internal and external exercises
- Regional planning support
- OMNCS Augmentee Program.

TRAINING

The Operations Division trains telecommunications industry personnel, OMNCS staff, NCS Regional Managers, Emergency Support Function (ESF) 2 support personnel, military reservists, and regional and State emergency responders to effectively execute their responsibilities during the various phases of response and recovery operations. During FY 2001, the Operations Division successfully coordinated and performed the following activities.

ERT Seminars

ERT seminars are 2-day seminars designed to provide industry, Federal, regional, State, and local personnel with the background and information required to successfully respond to a crisis. In the third phase of the ERT Program, more than 500 attendees have participated in seven sessions, and five more training seminars are scheduled. Since the ERT training program started in 1993, more than 2,000 participants have attended 30 sessions. During FY 2001, the OMNCS held seminars in—

- Oakton, Virginia (National Capital Region)
- Kansas City, Missouri (Federal Region VII)
- Philadelphia, Pennsylvania (Federal Regions II and III).

Relocation Facility Training

In November 2000, members of the NCC Emergency Operations Teams (EOT) trained at the NCS relocation facility. Team members toured and familiarized themselves with the facility's equipment and operations. In addition, team members were briefed on the operations and functions of other agencies that coordinate with the NCS during an emergency relocation. EOT members also received a demonstration and hands-on training with the LEC Mapping (LECMap) tool, an automated tool used to identify telecommunications assets.

Exercises

The OMNCS conducts internal and external exercises to maintain expert knowledge of, and proficiency in, the management, integration, and employment of NS/EP telecommunications resources. In FY 2001, the Operations Division successfully coordinated and conducted the following event.

Telecommunications Tabletop Exercise

On March 19, 2001, industry and Government representatives of the NCC and the NSTAC Convergence Task Force (CTF) participated in a tabletop exercise to examine the impact and response measures associated with structural damage that potentially can cause widespread disruptions across the PN.

The event gave participants and observers from across the telecommunications industry and Government an opportunity to discuss the intra- and inter-organizational coordination processes required in responding to telecommunications outages.

CONTINUITY OF OPERATIONS

The OMNCS maintains an active Continuity of Operations (COOP) Program that ensures that its essential functions can be sustained throughout an emergency. As directed by E.O. 12656, *Assignment of Emergency Preparedness Responsibilities,* the NCS developed a COOP Program in 1990 to identify NS/EP telecommunications functions that key OMNCS staff must perform in any emergency, developed plans to perform these functions, and implemented the capability to execute those plans.

During FY 2001, the OMNCS revised the COOP Program to reflect enhanced operational requirements and new Federal emergency preparedness guidance. This guidance includes Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, and Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*. The NCS is an active member of the interagency COOP Working Group, chaired by the Federal Emergency Management Agency. This forum coordinates and develops Federal COOP policies and initiatives. Through its involvement in the COOP Working Group during FY 2001, the NCS has continued to play an important role in developing emerging Federal emergency preparedness requirements associated with alternative operating facilities and tests, training, and exercises.

Additional enhancements to the OMNCS COOP Program included development of a vital records plan that addresses the identification, inventory, protection, and recovery of critical OMNCS electronic and nonelectronic records. The plan also outlines training requirements associated with preserving and securing OMNCS vital records.

During FY 2001, the OMNCS further enhanced its COOP Program capability by acquiring a second emergency relocation site. An integral element of a viable COOP capability, this site will provide an effective operating environment to support short-term OMNCS critical operations if NCS headquarters becomes temporarily unavailable.

Following the September terrorist attacks, the NCS provided around-the-clock telecommunications support to Federal emergency response operations from the NCS's primary relocation site. Lessons learned from these alternative site operations are being developed and will be incorporated into the OMNCS COOP Program.

PLANS AND RESOURCES DIVISION

The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial

Following the September terrorist attacks, the NCS provided around-the-clock telecommunications support to Federal emergency response operations from the NCS's primary relocation site.

matters, strategic and performance management planning activities, manpower allocations, and other personnel-related matters. The division exercises authority and ensures accountability over all resources allocated to NCS programs.

The division serves as the interface with the DISA directorates on financial and acquisition matters; DOD Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The division also conducts analyses and makes recommendations to the OMNCS and the DISA directorates on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

PLANNING

The Planning Team documents the OMNCS leadership's near-, mid-, and long-term strategic direction, vision, and priorities through the development of the Strategic Plan, Performance Plan, Future Years Corporate Plan, and Advanced Acquisition Plan.

The Planning Team, through the implementation of the Strategic and Performance Plans, comprehensively evaluates organizational performance and effectiveness. The OMNCS developed the NCS Strategic and Performance Plans in response to the requirements of the Government Performance and Results Act (GPRA) of 1993. These plans embrace the GPRA concept of engaging in a cycle of strategic planning, performance planning, and evaluation of an organization's effectiveness.

After collecting performance metric data during 1999, the OMNCS reviewed and reassessed its performance measurements based on changes to the external environment and its own reorganization. The Plans and Resources Division revised the Performance Plan and the Strategic Plan in FY 1999. These documents defined the new strategic goals and performance measures of the NCS, which reflected an increase in emphasis on customer service.

FINANCIAL MANAGEMENT

The Financial Team provides the overall fiscal direction to the OMNCS for day-to-day operations. It develops and produces all PPBS-related documentation for the OMNCS, including documentation for program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits. The team ensures that exhibits reflect decisions and directions from the Manager, NCS, and DOD.

The Financial Team also leads in developing, coordinating, and implementing of funding procedures as directed and provides guidance and assistance to non-DOD agencies involved in the NCS to ensure that their requirements are met. In addition, the team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

ACQUISITION MANAGEMENT

The Acquisition Team provides OMNCS offices with support throughout all aspects of the agency-level acquisition process. This support includes preparing acquisition strategy documentation, statements of work, contract solicitations, proposal evaluations, and other acquisition support documentation for OMNCS programs and projects. The Acquisition Team also monitors contractual compliance, identifies contractor deficiencies, recommends contractual remedies, tracks contract expenditures, monitors all contractor reporting for accuracy, and recommends adjustments.

CUSTOMER SERVICE DIVISION

The Customer Service Division provides support to the NCS COP (now the Committee for National Security and Emergency Preparedness Communications) and COR and the President's NSTAC. The division also identifies and validates NS/EP telecommunications requirements to ensure that the NCS is responsive to customer needs, develops assessment of threat to NS/EP telecommunications, and manages the Government and NSTAC Network Security Information Exchange (NSIE) process. The following paragraphs describe the Customer Service Division's FY 2001 activities.

NCS COMMITTEE OF PRINCIPALS/COUNCIL OF REPRESENTATIVES

The NCS COP met twice and the COR met three times during FY 2001. At these meetings, the COP and COR were provided with information on the NCC ISAC, NSTAC, the NCS 500-day plan development, the White House Convergence Task Force activities and report, the Cyber Warning Information Network, Last Mile Bandwidth Availability, the ACN, and various other OMNCS programs. The COP concurred with the NCS Comments to the NSTAC XXIII Executive Report. The COP approved the formation of a National Wireless Communications Infrastructure Concept Working Group to address the feasibility of a national wireless communications capability.
(Editor's Note: The Committee of Principals became the Committee for National Security and Emergency Preparedness Communications on Oct. 11, 2001, as ordered by Executive Order 13231).

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

The President's NSTAC held its 24th meeting on June 6, 2001, in Washington, DC, at the U.S. Department of State. The central theme of the meeting was *America's Security and Next Generation Information Networks*. Major topics addressed included industry and Government information sharing for CIP; network convergence and existing vulnerabilities of U.S. computer systems, including denial-of-service attacks; and the *National Plan to Defense Cyber Space*. During the Business and Executive Sessions of the meeting, the NSTAC Principals and senior administration officials discussed these and other topics developed by NSTAC's Industry Executive Subcommittee (IES) during FY 2001.

NSTAC'S INDUSTRY EXECUTIVE SUBCOMMITTEE ACTIVITIES

In FY 2001, the NSTAC's IES continued to develop issues for consideration and to direct the activities of its subgroups. The five key issue sets that the IES and its subgroups addressed during FY 2001 were information sharing for CIP, network convergence, last mile bandwidth availability, research and development exchange, and legislative and regulatory matters. Exhibit 3-4 depicts the NSTAC organizational structure. Specific subgroup activities and the results of their work are discussed in the subsequent sections.

NSTAC'S INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION TASK FORCE

The IES formed the Information Sharing for Critical Infrastructure Protection Task Force (ISCIPTF) to address IA- and CIP-related issues. The task force examined potential barriers to information sharing, developed input for Version 2.0 of the *National Plan for*

Information Systems Protection, and continued dialogue with U.S. Space Command (USSPACECOM).

The ISCIPTF addressed pertinent provisions of the *Freedom of Information Act* (FOIA) and recommended that the President support legislation similar to the Year 2000 Information and *Readiness Disclosure Act* to protect CIP information shared voluntarily by industry with the Government from disclosure under FOIA. Subsequently, the NSTAC Chair sent a letter to the President emphasizing the importance of the FOIA issue. After examining the issue, the ISCIPTF requested that the NSTAC's Legislative and Regulatory Working Group (LRWG) investigate what would be potentially effective FOIA legislation and related policy considerations as a part of its activities in FY 2001.

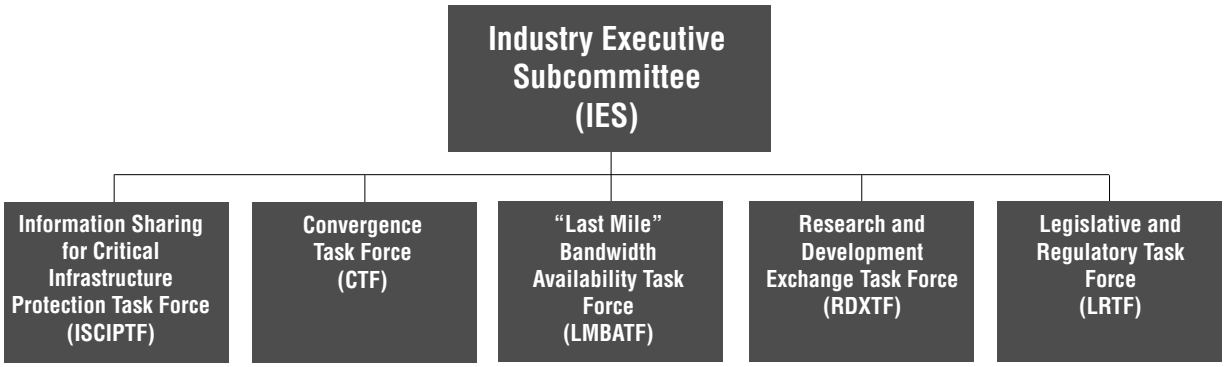
The ISCIPTF examined whether law enforcement prohibits victims of cyber crimes, such as electronic intrusions into network systems and databases, from reporting the intrusions to ISACs or similar information sharing forums. The ISCIPTF concluded that the NSTAC and Government NSIEs should consider the issue because of the NSIEs' experience in this area. In coordinating with the Department of Justice (DOJ), it was found that, although common practice discourages victims from sharing information, no laws or policies actually prohibit victims from discussing crimes against them even after they report crimes to law enforcement.

The private sector will have to ensure that its personnel who interact with law enforcement on such cases are aware that they are permitted and encouraged to share this information for network security purposes, using appropriate mechanisms. At the same time, the Chief, Computer Crime and Intellectual Property Section, DOJ, will work with the law enforcement community to develop and implement policies that encourage victims to share such information, and to educate victims on those policies.

In response to an NSC request, the ISCIPTF developed *The NSTAC's Response to the National Plan*, which serves as input to Version 2.0 of the *National Plan for Information Systems Protection*. The task force isolated key points from the NSTAC's work to be considered as the Nation develops a CIP strategy. The task force documented NSTAC findings related to the three broad objectives of Version 1.0 of the National Plan, prepare and prevent, detect and respond, and build strong foundations, that should be reflected in Version 2.0 of the plan.

In addition, the task force proposed that a new broad objective, international considerations, be included in the next iteration of the plan. The task force concluded that the NSTAC's cumulative work

Exhibit 3-4 The President's National Security Telecommunications Advisory Committee Organization (for the NSTAC XXIV Cycle)



Daniel P. Burnham (left), Chairman, President, and Chief Executive Officer of Raytheon Company and Chair of the President's National Security Telecommunications Advisory Committee (NSTAC), addresses NSTAC Principals and senior Government and telecommunications industry officials during the NSTAC Business Session, held June 6 in the State Department's Loy Henderson Auditorium. Beside Burnham is Lieutenant General Harry D. Raduege, Jr., Manager of the National Communications System. (Photo by Robert Flores, Defense Information Systems Agency.)

Dr. Condoleezza Rice, National Security Advisor to President George W. Bush, addresses the Principals of the President's National Security Telecommunications Advisory Committee, during an Executive Session held June 6 in Washington. Seated next to Dr. Rice is Richard Clarke, the National Security Council's National Coordinator for Security, Infrastructure Protection and Counter-terrorism. (Photo by Robert Flores, Defense Information Systems Agency.)

in the areas of CIP and IA can serve as a baseline for intensifying the dialogue between industry and Government regarding the best means of protecting the Nation's critical infrastructures. Key to this future discussion are the differing perspectives that industry and Government hold regarding the threat to these infrastructures. Bridging the gap in perspectives can create a foundation for future collaboration.

The IES also tasked the ISCIPTF with establishing a dialogue with USSPACECOM. The task force invited command representatives to attend all task force meetings—an invitation USSPACECOM accepted on numerous occasions during ISCIPTF meetings and IES working sessions. ISCIPTF representatives visited command facilities in Colorado to discuss the evolving relationship between the NSTAC and USSPACECOM. The task force agreed that information sharing is a cornerstone of national infrastructure protection and concluded that efforts to share information between the NSTAC and USSPACECOM should continue.

NSTAC'S CONVERGENCE TASK FORCE

The IES established the CTF to examine the converged network's ability to securely and reliably support NS/EP communications requirements. The CTF analyzed issues related to the potential security and reliability vulnerabilities of converged networks, including network control space issues, based on briefings received from industry and Government representatives.

The CTF concluded that the PSTN is becoming increasingly vulnerable as a result of its convergence with open packet networks. The converged network provides ample opportunities for individuals to gain access to, manipulate, and steal sensitive information transmitted via the PSTN. In addition, the interoperation of the PSTN's intelligent network with the IP networks via existing unreliable gateways presents vulnerabilities. Malicious attacks on these gateways could degrade overall network availability and reliability. Furthermore, the IP does not accord higher priority to in-band signaling messages. Therefore, using conventional NS/EP priority access and

transport mechanisms may not allow priority IP packets to bypass congestion within the converged network.

The CTF suggested that possible remedies for these vulnerabilities include implementation of signaling firewalls at network gateways and embedded security capabilities defined through standards. The task force recommended additional analysis of converged network security vulnerabilities to gain further understanding of the possible consequences of the evolving NGN.

The CTF agreed that the NGN must offer the NS/EP community quality of service, reliability, protection, and restoration features analogous to those of the PSTN. Government must develop an understanding of evolving network technologies and applications to determine security and reliability vulnerabilities affecting the converged network. To achieve this, the CTF suggested that Government foster cordial working relationships with NGN carriers and work to specify security requirements in packet network-related procurements in an effort to attain network reliability commensurate with that of the PSTN.

In response to concerns expressed by prominent Government officials, the CTF also examined the reliability and availability issues of single points of failure and possible widespread outages as they relate to the converged networks. The CTF analyzed pertinent previous NSTAC reports and participated in the NCC Single Point of Failure exercise. CTF members determined that a scenario could not be envisioned, even in the converged network environment, in which a single point of failure could cause widespread network disruption. Furthermore, the CTF found that converged network vulnerabilities and possible points of failure were more likely to diminish service availability and reliability essential to NS/EP operations than cause network component failures. Members suggested that detailed network data sharing among industry, Government, and academia should be undertaken to gain further understanding of the converging networks and achieve more accurate network modeling and simulation techniques to analyze vulnerabilities and their impacts.

The CTF also examined the ongoing standards development efforts in support of NS/EP priority requirements in the converged network. Group members concluded that, as the NGN evolves to offer more advanced broadband services, the Government must remain actively involved in the relevant standards bodies' activities to help define and ensure the consideration of NS/EP requirements in the IP environment. The CTF further encouraged the Government to remain actively involved in working group activities related to NS/EP issues, including the IETF and the ITU.

NSTAC'S "LAST MILE" BANDWIDTH AVAILABILITY TASK FORCE

The IES formed the "Last Mile" Bandwidth Availability Task Force (LMBATF) based on the recommendations of the "Last Mile" Bandwidth Availability Scoping Group and the request in October 2000 from Air Force Lt Gen Harry D. Raduege, Jr., Manager, NCS, for NSTAC's assistance. Lt Gen Raduege asked the NSTAC to recommend what the Government

The [CTF] recommended additional analysis of converged network security to gain further understanding of the possible consequences of the evolving NGN.

could do to expedite the provisioning of last mile bandwidth or to mitigate the provisioning periods for such services.

The IES tasked the scoping group with examining the NS/EP implications related to the provisioning of bandwidth at the local level and to determine next steps for the NSTAC's examination of the issue. Based on its research, the scoping group found that the complex technological, legal, and regulatory environment, along with the rapidly growing industry and Government requirements for bandwidth, had significantly lengthened the time needed to provision services at the local level. Additionally, the scoping group determined that the current environment could potentially harm the Nation's NS/EP readiness. In light of those findings, the group recommended that the IES form a task force to examine the root causes of the lengthened provisioning periods, how the Government might work with industry to reduce provisioning times or mitigate their effects, and what policy-based solutions could be applied to the provisioning of high-bandwidth circuits for NS/EP services.

The LMBATF included widespread representation of NSTAC member companies and NCS departments and agencies. LMBATF members gathered data from both industry organizations and Federal Government departments and agencies regarding their experiences with provisioning at the local level. Similarly, the task force solicited input from telecommunications service providers concerning the processes for provisioning at the local level and the factors affecting provisioning periods. On the basis of that input, the LMBATF agreed that the scope of the study should apply to all services that are not provisioned universally in the United States, including fiber optics, T1 and T3 lines, and integrated services digital network and digital subscriber line technologies. The task force continued to receive briefings from industry and Government organizations and affirmed the scoping group's initial analysis of the issue. The LMBATF planned to complete its report in September 2001.

NSTAC'S RESEARCH AND DEVELOPMENT EXCHANGE TASK FORCE

The IES established the Research and Development Exchange Task Force (RDXTF) to help coordinate the 2000 Research and Development (R&D) Exchange. On September 28-29, 2000, the President's NSTAC cosponsored its fourth R&D Exchange with the OSTP. The NSTAC conducted the event in conjunction with the Telecommunications and Information Security Workshop 2000 held at the University of Tulsa in Tulsa, Oklahoma. The purpose was to stimulate an exchange of ideas among representatives from industry, Government, and academia on the challenges posed by network convergence.

From these discussions, the RDXTF concluded that:

- There is a shortage of qualified IT professionals, particularly those with expertise in IA and/or computer security

- Developing a business case for security poses difficult challenges in the commercial sector, and there is a need to offset the high costs and high risks associated with R&D in security technology

- Given the complexity and interdependence introduced to networks by convergence and the proliferation of network providers and vendors, best practices, standards, and protection profiles that help to ensure secure interoperable solutions must be evenly applied across the NGN

- There is a need to enhance R&D efforts to develop better testing and evaluation programs to reduce the vulnerabilities introduced by malicious software.

Participants at the R&D Exchange recommended that the Government and NSTAC work to improve the security of networks in a converged and distributed environment. To support the Government, the NSTAC should—

- Consider the issues of best practices and standards in its report to NSTAC XXIV

- Consider the evolving standards of due care legal issues discussed at the R&D Exchange, including linked or third-party liability and new privacy legislation and regulations, such as the *Health Insurance Portability and Accountability Act*

- Conduct another R&D Exchange in fall 2001 in partnership with one or more of the IA Centers of Excellence to discuss the difficulties in, and strategies for, increasing the number of qualified IT security professionals and enhancing the academic curricula to meet the security challenges of the NGN.

NSTAC'S LEGISLATIVE AND REGULATORY TASK FORCE

The Legislative and Regulatory Task Force (LRTF) began the fiscal year as the LRWG, but became an autonomous standing body, the LRTF on February 15, 2001.

In FY 2001, the LRTF played an active role in addressing the legislative and regulatory implications of two critical issues: convergence and information sharing. As tasked by the IES, the LRTF considers the impact of current legislative and regulatory actions on NS/EP communications. Specifically, the LRTF continues to sustain the LRWG's tasking from the IES, which includes the following:

- Examining whether existing legal and regulatory authority is adequate to ensure that NS/EP requirements will be met in the converged and NGN environment

- Identifying and addressing other legal and regulatory issues related to convergence, as appropriate

- Analyzing information sharing/CIP legal and regulatory issues pending before Congress and the administration and those to be recommended (if any) for NS/EP implications

- Considering the legal issues discussed at the NSTAC R&D Exchanges, including linked or third-party liability and new privacy legislation and regulations

- Addressing legal and regulatory issues affecting the other IES task forces, if they request support.

The third issue, information sharing, follows on the June 1999 NSTAC XXII meeting, where the LRWG/LRTF examined impediments to information exchange, especially critical infrastructure information sharing. The group undertook an in-depth analysis of FOIA, specifically examining FOIA's potential to hinder information exchange between industry and Government. Under FOIA, the public may request and gain access to records maintained by Government departments and agencies.

For various reasons, such potential disclosure of data may deter industry from sharing information with the Government. Although there are a number of exemptions to FOIA's requirement for information disclosure, none of the exemptions clearly cover information pertaining to CIP. To address this issue, the LRWG/LRTF met several times with DOJ officials to exchange views on perceived problems and potential legal solutions.

As a result of their deliberations, the LRWG/LRTF agreed with DOJ representatives on the need for a nondisclosure provision to protect security-related information that is voluntarily

shared with the Government. The LRWG/LRTF shared its analysis with the NSTAC's ISCIPTF, which addressed the issue in its May 2000 report to NSTAC XXIII.

NSTAC XXV ACTIVITIES

The IES met on June 7, 2001, to discuss the preceding day's NSTAC XXIV meeting and begin developing the NSTAC XXV work plan. Later that month, the IES formed its task forces for the NSTAC XXV cycle and reaffirmed its intent to complete studies already under way. In addition to the LMBATF and LRTF, the IES formed the National Plan Task Force, which it chartered to develop input for the National Strategy for Cyberspace Security and work with the Information and Communications sector coordinators on the telecommunications portion of the plan. Moreover, the IES created the Network Security/Vulnerability Assessment Task Force and tasked it with assessing the policy and technical issues related to convergence and the NGN.

The NSTAC immediately began developing its formal reports and analyses on these issues in preparation for delivery to the President during the NSTAC XXV cycle. The NSTAC also recommended that the President support legislation that would ensure that CIP information voluntarily shared by industry received exemptions from disclosure under FOIA. Following the tragic events of September 11, the IES formed an ad hoc group to examine the telecommunications industry's response to service restoration and assess how the industry and Government can best work together to respond to such crises.

NETWORK SECURITY INFORMATION EXCHANGE ACTIVITIES

The joint meetings of the NSTAC and Government NSIEs provide a trusted environment in which industry and Government representatives can exchange information on threats to and vulnerabilities of the PN. The NSIEs' focus on technical issues affecting the security of the PN, such as unauthorized penetration or manipulation of the PN software, databases, and other infrastructures supporting NS/EP telecommunications services.

The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the PN and its supporting infrastructures. In FY 2001, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including intrusion detection systems, honeypots, virtual private networks and remote access vulnerabilities, and incident response and forensic capabilities.

The establishment of ISACs for our Nation's critical infrastructures has increased the demand for effective information sharing within and between industry and Government. During FY 2001, the NSIEs built on the lessons learned over the past 10 years and worked with DOJ to develop a larger model of information sharing to address the complexities of exchanging information within the NS/EP environment. A goal of this model is to protect the interests of industry, law enforcement, and the intelligence and defense communities while protecting the Nation's infrastructure.

During FY 2001, the NSIEs built on lessons learned and worked with DOJ to develop a larger model of information sharing to address the complexities of exchanging information within the NS/EP environment.

The procedures the NSIEs have developed for protecting and sharing information can provide a foundation for this model.

In FY 2001, the NSIEs extended their information sharing efforts to the international arena by inviting British and Canadian industry and Government representatives to participate in the information sharing process and provide an overview of CIP activities within their own countries.

In July 2001, support to the Government and industry NSIEs transferred from the OMNCS Customer Service Division to the Operations Division.

NCS ISSUANCE SYSTEM

The NCS Issuance System is the authority for the internal organization, policy, procedures, practices, and management of the NCS. In FY 2001, NCS Directive 3-10, GETS was staffed for coordination before being forwarded to the Executive Office of the President for approval.

NS/EP TELECOM NEWS

NS/EP Telecom News, published quarterly by the OMNCS, provides NS/EP information for the NCS and NS/EP telecommunications community, helping the NCS member organizations keep abreast of legislative, regulatory, judicial, technological, and policy developments.

NCS HOME PAGE

The NCS home page (http://www.ncs.gov) provides Internet clients and browsers with a chance to learn about the NCS and NSTAC. The home page contains NCS and NSTAC history, information about NCS and NSTAC programs and activities, and online versions of NCS and NSTAC publications.

The OMNCS continues redesigning many of its Web pages, including the NCS home page. The redesigns will give NCS Web site visitors better access to sites concerning NCS programs and activities, as well as updated information about NCS activities. The current redesign is also incorporating format changes to bring the site into compliance with Section 508 of the *Rehabilitation Act*. Section 508 requires Federal agencies to make their electronic and IT resources accessible to people with disabilities.

Among the publications posted to the NCS Web site during FY 2001 were the FY 2000 NCS Report, the NSTAC XXIV Issue Review, and the NSTAC XXIV Reports. The home page holds current and back issues of the *NS/EP Telecom News*, speeches and testimony on NS/EP telecommunications issues, and fact sheets on various NCS programs.

REQUIREMENTS

The Communications Assessment Branch (CAB) is responsible for identifying, evaluating, and validating NS/EP telecommunications requirements for the NCS. CAB works in conjunction with the OMNCS Requirements Forum, which consists of representatives from each OMNCS division. The forum provides an ongoing process for identifying and discussing NCS requirements and applying the maximum agency expertise and experience to addressing identified customer needs. In addition, the forum optimizes OMNCS customer interface and participation in the requirements process. The following paragraphs describe the accomplishments of CAB during FY 2001.

REQUIREMENTS SHORTFALLS ASSESSMENT

In collaboration with representatives of the NCS divisions, CAB updated the original 1999 *NCS Shortfalls Assessment Report*. The report assesses the ability of industry, the OMNCS, and Federal departments and

agencies to meet customer-identified NS/EP communications requirements and other functional requirements. The updated 2001 *NCS Shortfalls Assessment Report* documents several recently satisfied NS/EP communications requirements regarding e-mail reliability, interoperability, and attachments and access to directory service information. These requirements were satisfied by capabilities developed and incorporated into the Defense Message System.

REQUIREMENTS IDENTIFICATION EFFORT

As of July 2001, the requirements identification effort is being reevaluated.

V

NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF MEMBER ORGANIZATIONS

DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

The Department of State (DOS) mission is to support the President in formulating and executing U.S. foreign policy. This mission determines its telecommunications support requirements. Essential DOS telecommunications functions include the following:

- Implementing and managing a reliable, secure, responsive, survivable, cost-effective, global telecommunications network
- Providing communications support (including data, voice, imagery, facsimile, and video) for all U.S. Government agencies at U.S. overseas diplomatic facilities
- Maintaining a rapid response capability via alternative means to ensure the continual availability of effective communications links under all conditions.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOS manages its telecommunications through the Bureau of Information Resource Management and the Diplomatic Telecommunications Service Program Office.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Worldwide Internet Access

OpenNet Plus is one of the Department's highest priority information technology projects, designed to address Secretary Powell's commitment to provide DOS employees with access to the Internet. This program will enable secure Internet browsing and Web transaction services via the Department's existing OpenNet (sensitive but unclassified) worldwide computer network infrastructure. OpenNet Plus will provide access to Internet resources and Web-based transaction services. These resources and services will enable collaboration among foreign affairs agencies, via the Web and provide a strong foundation for modern E-government operations. Additional services will be added to OpenNet Plus as new requirements, technologies, and effective security practices are developed. The OpenNet Plus program will also enhance existing system security by replacing or enhancing current legacy systems within the Department.

Classified Connectivity Program

The Classified Connectivity Program (CCP) will put classified personal computers, e-mail, secret Internet protocol router network (SIPRNET) access, and other office automation tools on overseas desktops where they are needed. CCP addresses a major IT equipment and software deficiency. Existing CCP posts will receive replacements and upgrades of their computer and communications equipment as soon as possible. The major thrust of this program will extend classified services, including e-mail and SIPRNET browsing capabilities, to all posts authorized to have them.

Interagency Collaboration

Following the Overseas Presence Advisory Panel's recommendations, the Department started a program to establish a common information technology infrastructure to improve communication and collaboration among Federal agencies at overseas posts, beginning at the sensitive-but-unclassified level. This program will improve knowledge sharing between organizations at post. It will also allow agencies at post to easily collaborate on interagency projects and to garner the expertise of specialists from other posts or headquarters organizations in a virtual team environment. The Department has approved an IRM-led program to develop and deploy a prototype interoperable IT infrastructure, creating an Overseas Presence Collaboration Zone (OPCZ) at two locations (Mexico and India). In July 2001, three prototype vendors were selected. Following evaluation, testing, and selection, a five-month pilot will be conducted among 2,400 interagency users in Mexico, India, and the United States. The pilot will be evaluated and potentially ready for worldwide deployment beginning in October 2002.

Processing Consolidation

The Department has begun to consolidate disparate IT processing facilities by expanding the mainframe "super server" data centers into one enterprise server operations center, thus providing centralized 7x24 operations and maintenance and standardization while achieving economies of scale.

Communication Security

The DOS created a public key infrastructure (PKI) Program Office to implement PKI, providing users secure Internet and intranet Web application and e-mail services heretofore unavailable. The Department implemented PKI during fiscal year (FY) 2001. The Department will provide this smart access card-based technology to users from all Federal agencies with requirements to access the OPCZ at overseas posts when deployed. This technology will have a profound impact on the overall level of information security for the State Department and the conduct of its business in the future.

DOS continues its successful implementation of over-the-air-rekey (OTAR). The number of posts using OTAR as the primary means of traffic encryption key delivery increased to 135 fully operational as of April 2001. To date, the posts' reaction to OTAR is overwhelmingly positive. The Department continues toward its goal of converting all posts to OTAR operations by the end of FY 2002.

Secure Voice Program

The Department, through interagency collaboration, transitioned its legacy secure voice system to the new National Secure Voice Standard, the Secure Terminal Equipment system. STE units were deployed domestically and at overseas posts. The Department's life cycle support infrastructure for the new secure voice system is in place and operational.

Counter-Narcotics

The Department provided imagery, automated data processing, voice, and high-speed data services to the Department of Defense Counter-Narcotic Command Management System.

Support for the Secretary of State

The Department provided and supported protective communications packages for domestic and overseas protection of the Secretary and designated diplomats.

DEPARTMENT OF THE TREASURY (TREAS)

NS/EP TELECOMMUNICATIONS MISSION

The essential functions of the Department of the Treasury (TREAS) requiring NS/EP telecommunications are summarized as follows:

- Protecting the President, Vice President, their families, and other dignitaries
- Managing the economic activities of the United States, including all monetary, credit, and financial systems
- Administering the laws pertaining to customs, taxes, alcohol, tobacco, and firearms
- Serving as the principal economic advisor to the President
- Accomplishing international economic and monetary control as it pertains to the well-being of the Nation
- Manufacturing currency, coins, and stamps, and establishing methods of exchange.

TELECOMMUNICATIONS STAFF ORGANIZATION

TREAS manages telecommunications through the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO), under the Assistant Secretary of the Treasury for Management. This office oversees NCS liaison and NS/EP support activities, and provides management guidance and financial oversight to improve the Department's use of telecommunications systems. The office is also responsible for ensuring, through the exercise of program management authority, that TREAS bureaus can access a cost-effective, technologically sound telecommunications infrastructure for mission performance. This year, the CIO organization was expanded to include physical security as well as technical security for the Department.

The TREAS CIO also serves as the vice chair of the Federal CIO Council. In this capacity, the TREAS CIO is responsible for guiding, directing and developing information technology (IT) management policies, procedures, and standards. The Federal CIO Council is the lead interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources.

ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Law Enforcement Users Group

TREAS has continued its activities as Co-Chair of the Federal Law Enforcement Wireless Users Group (FLEWUG) to ensure the development of a cost-effective, interoperable, nationwide tactical wireless network for use by Federal, State, and local law enforcement and public safety groups.

Computer Emergency Response Capability

A formal computer emergency response capability working group was formed with members from all the bureaus and departmental operations to determine how best to develop this capability for a variety of areas. Priority was placed on determining incident reporting standards and procedures. TREAS completed the year with no major embarrassing or operational compromises of its electronic data systems and hopes to continue this trend as well as to enhance the intrusion prevention, detection, and remediation capabilities it now has in place.

Support for Public Key Infrastructure Development

TREAS provided technical, budgetary and leadership support for the development and use of an interoperable governmentwide public key infrastructure to permit electronic transactions over the Internet in a trusted environment.

Seat Management

TREAS headquarters (departmental offices) has partnered with Getronics Government Services under the GSA Seat Management contract. This performance-based contract provides TREAS customers with personal computers (desktop and laptop), standard software, and printers, help desk, infrastructure support (network, LAN desktop), information technology learning center services, telephone administration, and Internet/intranet services at a fixed cost. Other services include periodic updates (refresh) to both hardware and software to keep technology current and a variety of custom IT development and administrative services.

International Trade Data System

The International Trade Data System is a single governmentwide system that is under development for the secure electronic collection and distribution of international trade transaction data required by Federal agencies. It is expected to reduce operating costs of the Federal Government by reducing the number of standalone agency systems that collect and process submissions, and improve risk assessment, enforcement, policy formulation and analysis. Though the system is under development by the U.S. Customs Service, but an interagency board of directors is responsible for overseeing the development and implementation of the system.

Treasury Secure Data Network

The Department implemented a new infrastructure for processing and distribution of classified data. This effort is being coordinated with the building renovation team to ensure that the historic integrity of the facility is not compromised and that a state-of-the-art, classified, data processing capability is available for the entire Department.

DEPARTMENT OF DEFENSE (DOD)

NS/EP TELECOMMUNICATIONS MISSION

Under the provisions of Executive Order (E.O.) 12472, the Department of Defense (DOD) is assigned the following NS/EP telecommunications responsibilities:

- Provide, operate, and maintain the telecommunications services and facilities to support the National Command Authorities and execute the responsibilities assigned by E.O. 12333, United States Intelligence Activities, December 4, 1981
- Ensure that the Director, National Security Agency (NSA), provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications
- Execute the functions listed in Section 3(I) of E.O. 12472.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOD includes the Office of Secretary of Defense, the military departments and the services within them, the unified commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency (DISA) is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy and the ASD for C3I. Command, control, and communications requirements are the concern of the Joint Staff J6.

DOD SIGNIFICANT ACCOMPLISHMENTS

The Global Information Grid

The Global Information Grid (GIG) is the vision of the ASD C3I for achieving information superiority (IS). The GIG has a multipart mission: supporting the warfighter's needs for IS; addressing the critical concerns of frequency spectrum allocation; improving management of the information infrastructure investment; and coevolving doctrine, organization, training and education, material, leadership, personnel, and facilities (DOTMLPF).

In 2001 the DOD passed several important GIG milestones: the GIG Version 1.0 architecture was approved, the role of network centric warfare (NCW) was clarified, an update to the GIG definition was signed, and the GIG Capstone Requirements Document (CRD) was signed. A GIG implementation plan is in coordination.

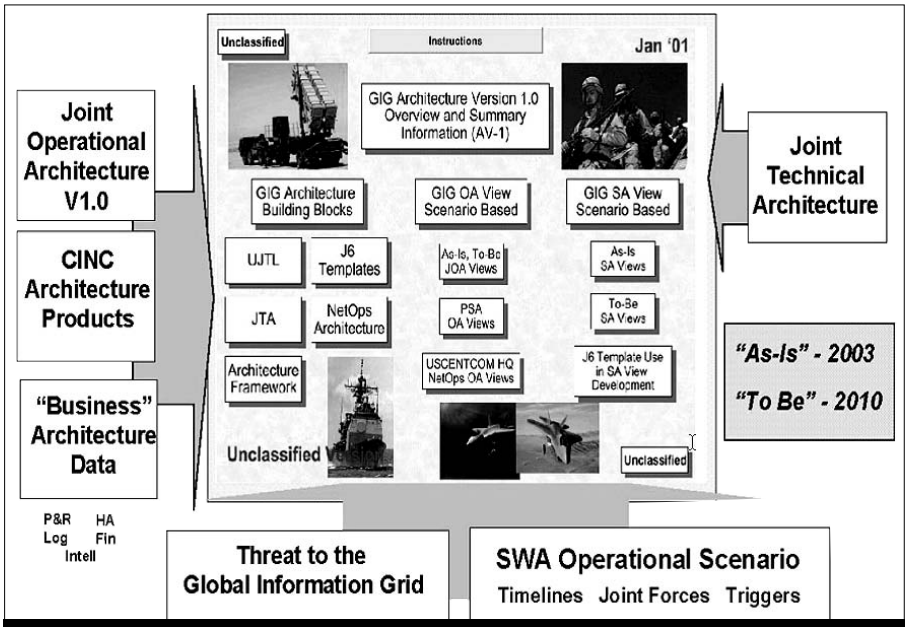


Figure 1: GIG Version 1.0 Contents

GIG Version 1.0 Approved

Version 1.0 of the GIG was approved by the DOD Chief Information Officer (CIO) Executive Board on July 19, 2001. Figure 1 shows the entry screen of the CD ROM of GIG Version 1.0 and the relationships of GIG Version 1 to other products. Figure 2 shows some of the architecture artifacts from GIG Version 1.0.

DOD SIGNIFICANT ACCOMPLISHMENTS *continued*

NCW and the GIG Infosphere

The GIG will provide the joint and coalition warfighter with a single, end-to-end information system capability, which includes a secure network environment. The GIG will allow users to access shared data and applications, regardless of location, and be supported by a robust network/information-centric infosphere.

Moving from concept to reality requires the development of network-centric functional capability packages and a GIG infrastructure that can support them. Bringing network-centric concepts and capabilities to fruition will require a coordinated strategy that is characterized by an unprecedented degree of collaboration among the various communities of interest within DOD.

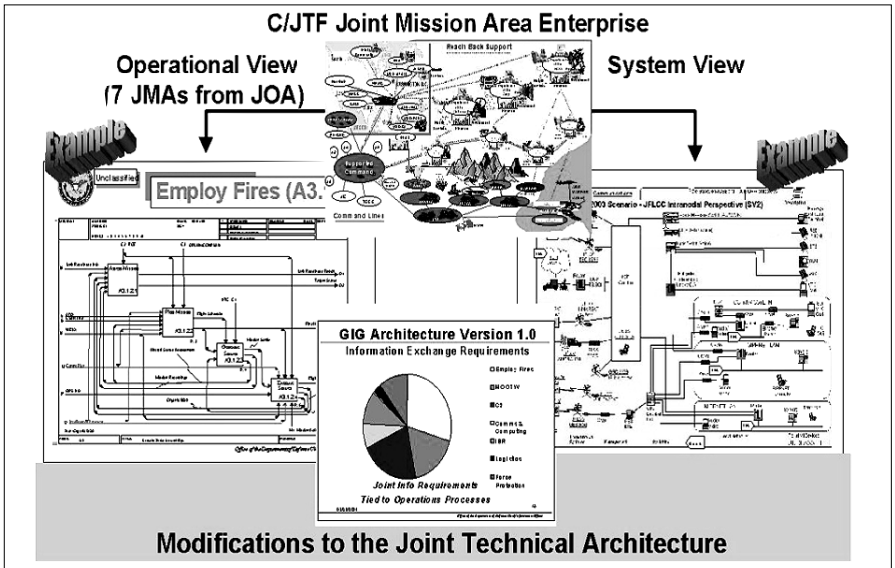


Figure 2: GIG Version 1.0 Architecture

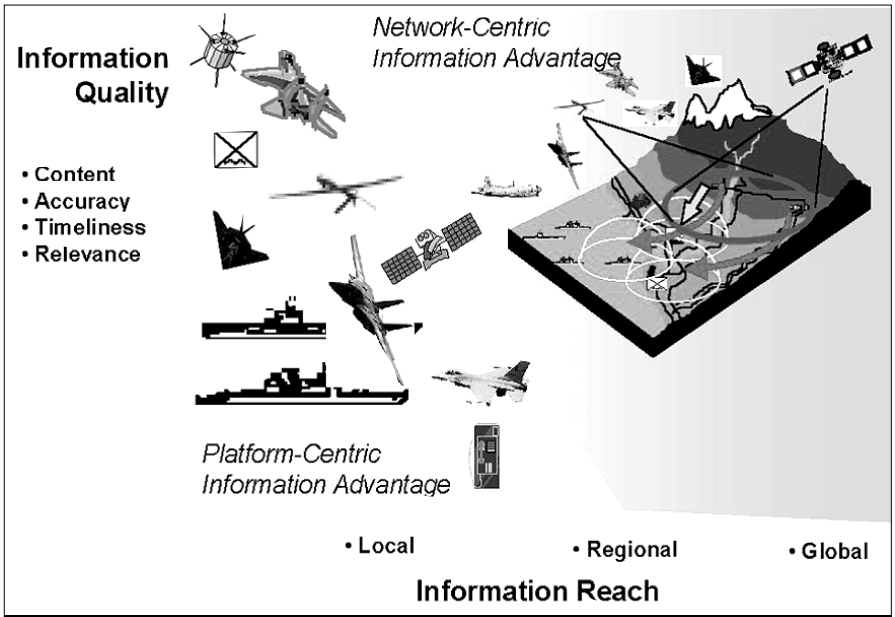


Figure 3: Network Centric Warfare—Way Ahead

The GIG CRD Signed

In August 2001, the GIG CRD was signed.

The GIG Definition

In May 2001 the DOD redefined the role of the GIG in the department's evolving enterprise architecture.

The GIG is defined as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve IS. It also includes national security systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

The GIG also comprises any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software and services

DOD SIGNIFICANT ACCOMPLISHMENTS *continued*

- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services
- Processes data or information for use by other equipment, software and services.
- Non-GIG information technology (IT) refers to stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

GIG Transformation of Command, Control, and Communications
Implementing the GIG will enable the transformation of command and control (C2) and communications to the Joint Vision 2020 goal of the Department.

Implementing the GIG Using Functional Capability Profiles
Functional Capability Packages (FCP) are central to implementing the GIG, in that they provide a construct for describing an operational concept and the integrated collection of DOTMLPF that are required to make each concept a reality. FCPs will be used to field new capabilities, such as the recent Deployable C2 Center initiative, improve situational awareness, and provide for collaborative planning services to all GIG users.

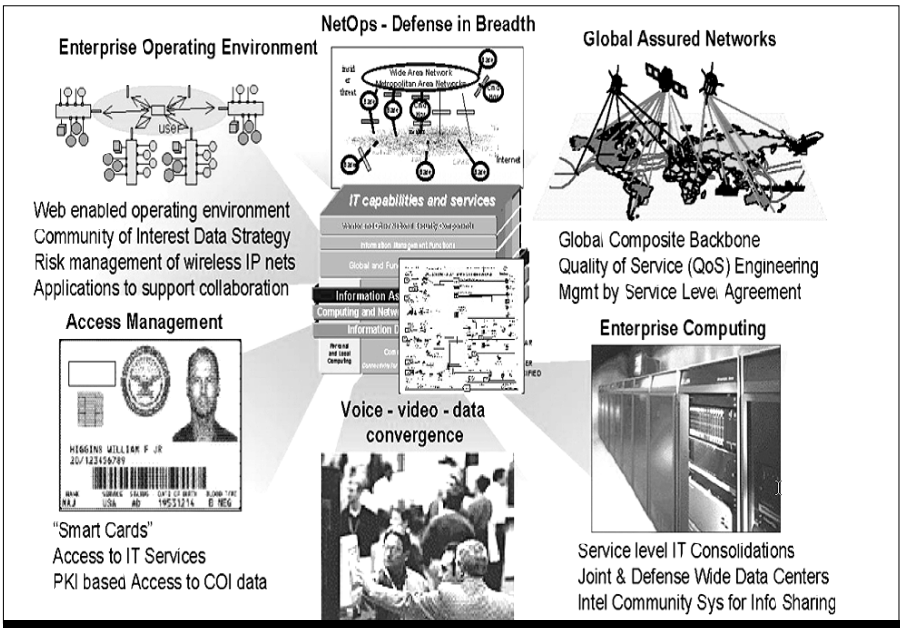


Figure 4: Global Information Grid Infrastructure

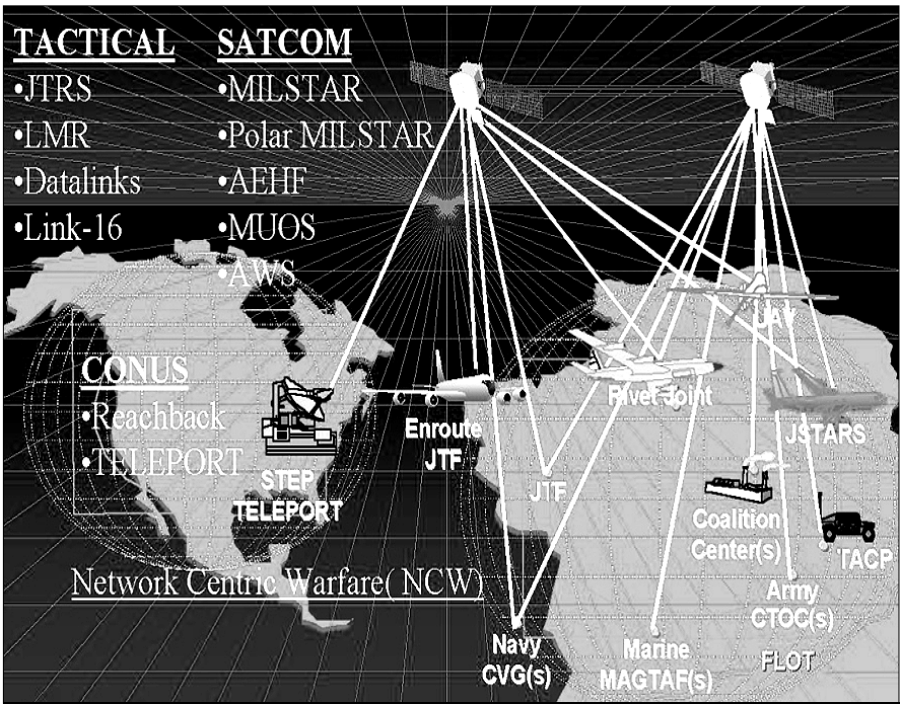


Figure 5: Global Information Grid Transforming Communications

DOD SIGNIFICANT ACCOMPLISHMENTS *continued*

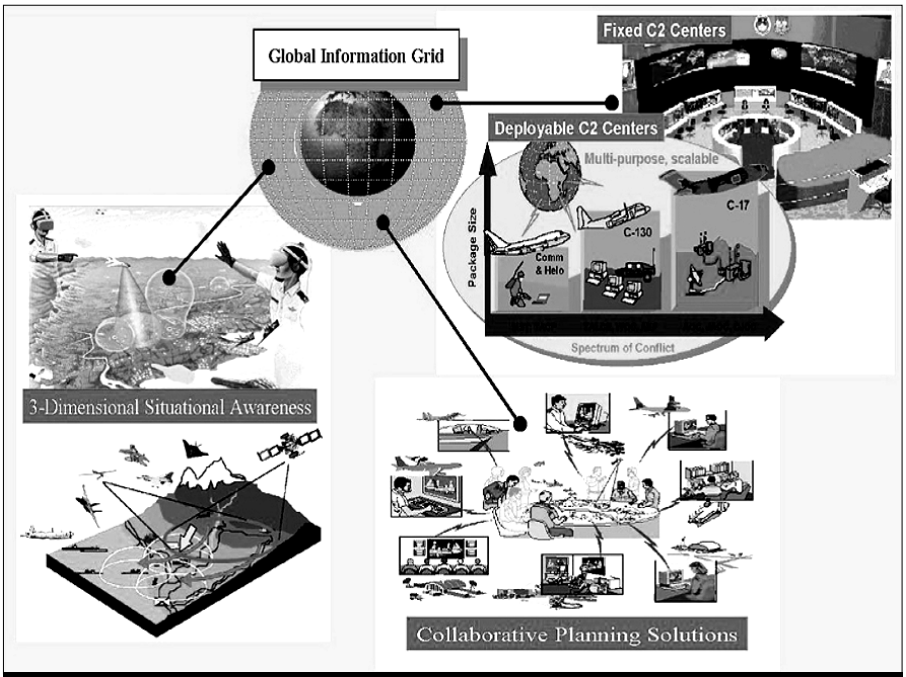


Figure 6: Global Information Grid Transforming Joint, Allied, and Coalition C2

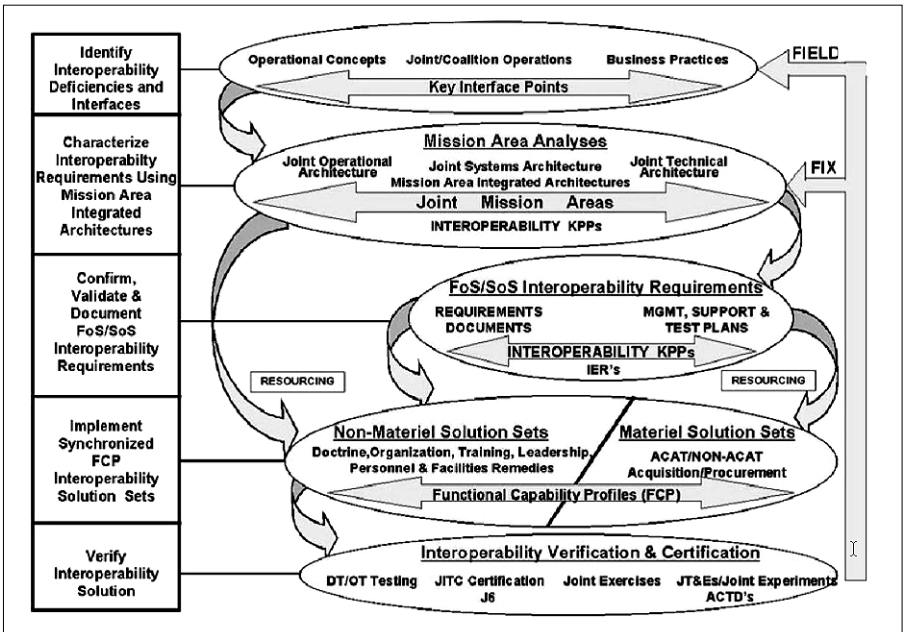


Figure 7: Functional Capability Profile Based GIG Implementation

DEPARTMENT OF JUSTICE (DOJ)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission for the Department of Justice (DOJ) is to provide telecommunications facilities and services in support of DOJ NS/EP essential functions. The Department centralizes its NS/EP responsibilities in the Justice Management Division (JMD) for all Department entities except the Federal Bureau of Investigation (FBI). The Bureau maintains separate secure network facilities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Director, Telecommunications Services Staff (TSS) under the JMD's Deputy Assistant Attorney General for Information Resources Management operates and manages DOJ's consolidated data transport network, law enforcement message processing systems, and Telecommunications Services Center. TSS also provides networking and technical assistance to DOJ's offices, boards, divisions, and bureaus. Secure interagency message transmission is offered through separate facilities (Automatic Digital Information Network, and Justice Automated Message System).

The Information Security Policy Group (ISPG), Security and Emergency Planning Staff is responsible for security oversight of all national security communications systems within the Department. The ISPG is the central office of record for all national security information key material for the Department. The Drug Enforcement Administration (DEA), FBI, the Immigration and Naturalization Service (INS), and United States Marshals Service (USMS) continue to administer their own communications security programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following current/ongoing DOJ activities support NS/EP objectives:

- TSS provides full-time, onsite representation for DOJ as the Deputy Chief, Operations Division, National Communications System (NCS).
- TSS provides representation for DOJ on the Council of Representatives (COR).
- TSS provides the Deputy Chairman, Telecommunications Service Priority (TSP) Oversight Committee.
- DOJ continues its active participation in the NCS activities of the Committee of Principals (COP)/COR, and participated in NCS NS/EP telecommunications support, activities, and programs.
- DOJ continues its vigorous support of the activities of NCS Internet Protocol Implementation Team; Government NS/EP telecommunications activities; NS/EP planning, program, and contingency programs; and emerging NS/EP telecommunications programs. DOJ has sponsored TSP access for three commercial companies that either are departmental component contractors or engaged in national security and emergency preparedness support in their normal duties.
- Additionally, the Department actively participates in the Government Emergency Telecommunications Service Program, the TSP Program, and the Shared Resources High Frequency Radio Program.

DOJ SIGNIFICANT ACCOMPLISHMENTS

In 1998, the Department initiated the Justice Consolidated Network (JCN) program to be the wide-area high-speed data telecommunications network of choice for all DOJ components. Through this program, more than 20 separate DOJ networks were upgraded and modernized into a single JCN, thereby consolidating services, reducing costs, improving security, and boosting network performance.

In fiscal year 2001, the JCN transitioned into a fully operational network as more than 600 DOJ locations for the Executive Office for the U.S. Attorneys, DEA, the U.S. Trustees, INS, the Federal Bureau of Prisons, and a number of smaller components were obtaining service by the end of the fiscal year. More than 1,200 additional DOJ and other agencies' locations are planned to transition to JCN during the next 2 fiscal years. Chief among the DOJ components scheduled to transition are the FBI, the USMS, and the Executive Office for Immigration Review. In addition, several components that have already transitioned are planning to upgrade both the number of locations serviced and their bandwidth requirements for JCN. Over the next few years, JCN will service almost twice as many component locations as originally envisioned, while providing a flexible means to accommodate growth in the Department's telecommunications requirements.

DEPARTMENT OF THE INTERIOR (DOI)

NS/EP TELECOMMUNICATIONS MISSION

The Department of the Interior's (DOI) mission is to efficiently manage the Nation's natural resources. DOI and the United States Department of Agriculture (USDA) co-manage the National Interagency Fire Center in Boise, Idaho. The center is the Nation's primary emergency support facility for forest fire suppression. From multiple radio caches strategically located throughout the United States, emergency mobile radio systems are available for fire fighting and other national emergencies. Forest fire suppression operations are conducted in close cooperation with State and local government emergency support activities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The transition of the Department's voice and data communications services from GSA's Federal Telecommunications System (FTS) 2000/AT&T contract to the FTS2001/MCI contract was a priority effort. Most of the Department's switched voice services were transitioned in fiscal year (FY) 2000, while the transition and redesign of the Department's data network services were accomplished in FY 2001. We have significantly improved services by increasing the bandwidth available to the Department's nationwide data communications network (vDOINET) users by changing from a private network to a virtual network architecture on the MCI WorldCom public network. VDOINET supports departmentwide administrative applications, bureau programs, and other agency needs. High-speed Internet access was also implemented at multiple locations throughout the United States.

The Alaska Regional Telecommunications Network was reconfigured to provide DOI and other Federal agencies in Alaska faster access to the Internet and improved DOI access to departmentwide administrative applications based in Denver, Colorado. Shared use of this network has lowered costs, improved performance, and increased the availability of data and video services. DOI and USDA continue to work together to improve operations by sharing telecommunications services, particularly where facilities are collocated.

DOI has a multivendor, multiyear contract to supply narrowband digital land mobile radios (LMR) and systems in response to the National Telecommunications and Information Administration mandated transition to narrowband LMR operations. This contract, available to all Federal agencies, provides lower cost standardized interoperable digital radios. DOI is implementing a multiyear capital investment plan to ensure that all wideband very high frequency radio systems are replaced by narrowband systems before 2005.

Key officials, emergency coordinators, and telecommunications managers throughout the Department have Government Emergency Telecommunications Service cards for long distance emergency telephone communications. Secure telephone unit-third generation telephones are used to support DOI national security programs, and high frequency radio links are now used to connect DOI emergency relocation sites.

DOI SIGNIFICANT ACCOMPLISHMENTS

During FY 2001, the DOI—

- Successfully tested digital narrowband radios during wildfire operations
- Transitioned FTS2000/AT&T telecommunications services to FTS2001/WorldCom services
- Converted the legacy DOINET data communications network to a virtual network architecture to improve service availability and Internet access speeds
- Restructured the Alaska Regional Telecommunications Network to provide improved Internet access
- Provided Internet access and computers to all Alaskan Indian Tribes through the Alaskan Tribal Technology Access Project.

UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)

NS/EP TELECOMMUNICATIONS MISSION

The United States Department of Agriculture (USDA) has several essential functions requiring NS/EP telecommunications. These functions include providing for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment, along with inspection of livestock, poultry, and other products to ensure the safety and wholesomeness of food. In addition, the USDA manages the protection and use of national forests, national grasslands, wilderness areas, and other public lands and facilities under USDA jurisdiction. This includes managing wildland fire control activities on these lands in coordination with local authorities and co-op forestry activities in support of State and local fire protection.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- USDA continues to actively support the Government Emergency Telecommunications Service (GETS) by working to ensure personal identification number (PIN) cards are provided to key NS/EP personnel within the Department. In this effort, USDA has increased the number of stockpile PIN cards in the Office of Crisis Planning and Management. GETS has been incorporated into the Continuity of Operations Plan for the Department, and PIN cards are used regularly during exercises.
- USDA obtained TSP authorization to accelerate new installation of Digital Signal 3 service for the USDA Kansas City National Information Technology Center (NITC). This acceleration was in response to the Secretary of Agriculture support to the Wildfire Management Program to ensure an adequate telecommunications infrastructure to Federal, State, local, and military personnel combating wildfires throughout the country and to aid in access to personnel deployment applications at the NITC.
- USDA aided in the rescue efforts in New York City and at the Pentagon by mobilizing Forest Service incident management teams skilled in managing large emergency situations through their experience with wildfires. The USDA also provided clear radio frequencies and staff for the firefighting portion of the Federal Response Plan.

USDA also—

- Continues support for the Committee of Principals/Council of Representatives and the President's National Security Telecommunications Advisory Committee
- Participates on Shared Resources High Frequency Radio Program, Communications Resource Information Sharing Initiative, Federal Telecommunications Standards Committee, Federal Wireless Users Forum, and GETS User Council
- Supports the Department of State Diplomatic Telecommunications Service
- Participates in Celluluar Priority Access Service, Federal Law Enforcement Wireless Users Group, and other working groups as necessary
- Maintains secure telephones throughout the Department supporting NS/EP functions and is working to upgrade current analog technology to digital.

NS/EP PARTNERSHIP ACTIVITIES

USDA recently pilot tested a mixed digital/analog land mobile radio system at several locations in the western United States. The intent of these tests was to ensure that any unknown problems were identified and resolved before large-scale implementation of digital equipment was begun. The tests proved that analog and digital land mobile radio equipment could operate within the same systems without degradation of mission operations. With the availability of digital land mobile radio equipment fast becoming a reality, conversion to the new technology is highly important. The USDA is weighing carefully the balance between a swift conversion and the requirements of mission capability, employee safety, and overall cost. The ability to operate with mixed analog/digital systems allows for a gradual transition to digital, spreading the costs over several years. This transition eliminates major budget peaks and allows manufacturers time to work out many of the problems associated with the new technology.

Smokejumpers suiting up.

DEPARTMENT OF COMMERCE (DOC)

CURRENT NS/EP TELECOMMUNICATIONS ACTIVITIES

The Department of Commerce (DOC) continues to support previous activities for NS/EP as outlined in the FY 2000 report.

NEW NS/EP ACTIVITIES

The Office of the Chief Information Officer (OCIO) is the responsible activity for NS/EP issues within the Office of the Secretary for the DOC. During FY 2001, the OCIO has assumed responsibility for two new NS/EP programs through its Office of Special Projects and Programs. These two programs are known as the Digital Network Management System (DNMS) and the National Wireless Communications Infrastructure Program (NWCIP).

FUNCTIONAL DESCRIPTION OF PROGRAMS

- Both the DNMS and NWCIP programs deal with telecommunications interoperability to support NS/EP activities. The DNMS is a digital telecommunications interface device that allows smooth interoperability between disparate land mobile radio (LMR) systems.
- The NWCIP is envisioned as two large interconnected LMR trunk systems within 10 separate regions in the contiguous United States. Each State government will have a single trunk network using National Guard frequencies while allowing other State NS/EP and law enforcement personnel to ride their system.
- The Federal NWCIP will be mirrored within the same regions and overlay the State systems. This separate system will allow total interoperability to exist among Federal, State, and local operations during times of stress for NS/EP activities. It will also allow every Federal activity within the system to be autonomous and still provide capability for interoperability that could be activated at the time of requirement.
- The NWCIP is based on the trunked LMR network system being deployed in Hawaii and Alaska, is an all leased network, and does not involve capital funding.
- The NWCIP concept is under review by the National Communications System to determine whether it should be adopted nationally.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

DHHS SIGNIFICANT ACCOMPLISHMENTS

During fiscal year 2001, the Department of Health and Human Services (DHHS) used the Shared Resources High Frequency (HF) Radio Program (SHARES) in its field-deployable HF radio kits that were developed during the last fiscal year. Civil Air Patrol and Military Affiliate Radio System stations are particularly helpful with on-the-air testing.

SHARES was also used to link the DHHS Office of Emergency Preparedness with the field command post of the National Disaster Medical System during the Federal response to the flooding caused by tropical storm Allison in the Houston, TX, area.

In addition to the Office of Emergency Preparedness/National Disaster Medical System (OEP/NDMS), several other operating divisions of the DHHS are considering adding HF radio systems to their Continuity of Operations plans. Automatic Link Establishment (ALE) technology makes HF radio more practical for offices that do not have access to trained HF radio operators. OEP/NDMS is indebted to the SHARES program for providing the opportunity to gain experience with this valuable mode of communications.

OEP/NDMS is also grateful for the continued leadership demonstrated by FEMA in performance evaluation of certain HF ALE equipment, and for their efforts in evaluating HF e-mail products.

Amateur radio operators continue to provide invaluable assistance to NDMS Disaster Medical Assistance Teams (DMAT). Many of the communications officers and telecommunications specialists on DMATs learned their communications and electronics skills through their amateur radio experience. During exercises and actual deployments, amateur radio provides a versatile pool of operators, technicians, and radio frequencies that help DHHS to serve the American people.

DEPARTMENT OF TRANSPORTATION (DOT)

NS/EP TELECOMMUNICATIONS MISSION

The Mission Statement outlined in the Department of Transportation (DOT) Strategic Plan asserts that the Department will "serve the United States by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people." Towards that end, a DOT strategic goal for national security states that the Department will work to "ensure the security of the transportation system for the movement of people and goods, and advance our national security interests in support of the National Security Strategy." Within this framework, DOT has created what are called "flagship initiatives" in support of the aforementioned goals and plans. The National Emergency Response Flagship deals with improving command and control communications activities (including secure communications) and ensuring continuity of all Government operations. The DOT continues to actively participate in national telecommunications forums, realizing the vital role telecommunications plays in providing for the safety and security of the traveling public and our Nation's transportation systems.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The Department participates in several ongoing NS/EP telecommunications activities, including:

Support of National Communications System activities

The Department continues its active participation on the National Communications System (NCS) Committee of Principals (COP)/Council of Representatives (COR), the President's National Security Telecommunications Advisory Committee, and it actively supports NCS NS/EP activities and programs.

Government Emergency Telecommunications Service

The Department has been involved with the NCS Government Emergency Telecommunications Service (GETS) program since its inception. DOT organizations account for more than 3,500 of the GETS cards issued by the NCS Program Office. GETS cards have been assigned to Regional Emergency Transportation Coordinators and Representatives across the United States and overseas for use during natural disasters and other emergency situations and exercises.

Federal Telecommunications System 2001

The Department is nearing completion of its transition from Federal Telecommunications System (FTS) 2000 to FTS2001 across all DOT operating administrations. WorldCom was selected to provide the range of services being offered under the FTS2001 to the Department. The DOT/WorldCom team will further the Department's "One DOT" corporate management strategy by unifying the entire organization under a common telecommunications vehicle. This One DOT strategy is intended to achieve more effective service solutions that minimize cost and administrative effort departmentwide, while maximizing service capabilities and flexibility for the OAs. Additionally, the Department continues to pursue opportunities to consolidate networks and other telecommunications systems to achieve enhanced capabilities and cost reductions.

OTHER NS/EP PROGRAMS

DOT continues to participate in the Federal Telecommunications Committee Standards Program, the Shared Resources High Frequency Radio Program, the Communications Resource Information Sharing Initiative, and the Telecommunications Service Priority (TSP) program.

DEPARTMENT OF ENERGY (DOE)

THE HEADQUARTERS EMERGENCY COMMUNICATIONS NETWORK

The Emergency Communications Network (ECN) is an integral part of Department of Energy's (DOE) emergency management system that links the DOE headquarters (HQ) Emergency Operations Center and 25 data/25 video nodes DOE-wide, DOE's deployable radiological emergency assets, other Government agencies, and one international unclassified video link with the Russian Ministry of Atomic Energy. The ECN supports emergency responses and meetings at the executive, interagency, and international levels.

DEPARTMENT OF ENERGY CORPORATE NETWORK

The Department of Energy Corporate Network (DOENet) is a private, secure wide area network designed to carry critical business applications and business-sensitive data to users DOE-wide. This essential, centrally managed, "firewalled" network currently connects 40 sites using Asynchronous Transfer Mode (ATM). ATM allows cost efficient convergence of networks and integration of data, voice, and video traffic onto the same network. Upgrades have provided corporate network connectivity at a minimum of 1.544 Megabits per second and routers that enable simultaneous voice, video, and data services. Network traffic is less subject to unauthorized disclosure because it does not pass through public Internet channels.

ALBUQUERQUE OPERATIONS OFFICE

The Albuquerque Operations Office (AL) is transitioning its existing wideband Emergency Response Radio system to the Sandia National Labs (SNL) trunked radio system (TRS). The local ultra high frequency (UHF) radio system expands the AL radio net to a broader communications base covering Kirtland Base, SNL, AL, and the associated ECN Network at the AL emergency operations center (EOC). The transition to the TRS is scheduled for completion by early fall of 2001. Work has also begun on replacing local analog radio systems with new trunked narrowband radio systems. AL has begun the scheduled replacement of the OTS/EOC building 20387-phone system with an integrated private branch exchange communications system, a major change that will significantly enhance communications during emergencies at the AL and the Office of Transportation Safeguards. The new system is expected to be implemented during early fiscal year 2002.

OAK RIDGE OPERATIONS OFFICE

The Oak Ridge Operations Office (OR) continued plans for implementing a wide area radio system. The safety committee determined that implementing the proposed system would resolve known safety, emergency preparedness, and mutual aid issues. A construction design review was completed, and requests for project funding were made to DOE HQ. The new trunked-capable narrowband UHF mobile radio system will replace the existing conventional analog, wideband very high frequency (VHF) mobile radio system, and provide a central OR infrastructure with OR-wide connectivity. OR continued implementing public key infrastructure to support encrypted network traffic, and key personnel training is completed. OR continues to support the National Weather Service as a retransmission site for the Emergency Manager's Weather Information Network. Data distributed as a signal enables a personal computer to become a weather graphics, data, and alarm terminal.

RICHLAND OPERATIONS OFFICE, HANFORD SITE

The automated Hanford Site (HS) Emergency Alerting System integrates site notification systems into a common network for emergency message distribution. The outdoor siren warning system is placed along the Columbia River to provide action messages to personnel working outdoors when an emergency arises. Future upgrades include indoor sirens, computer messaging, site pagers, and radio systems. The Narrowband Migration Implementation Plan converts the current VHF wideband radio communications, pager services, and Global Positioning Systems at HS. A new task team will establish a prioritization plan for telephone communications during an emergency event by identifying priority numbers through the HS telephone and commercial offsite telecommunications switches.

DOE SIGNIFICANT ACCOMPLISHMENTS

Nevada Operations Office
The Nevada Operations Office (NV) has converted from a local, Government-owned paging system to a partnership agreement with a nationwide supplier that provides local (including the NV Test Site) and Departmentwide coverage. NV installed a new digital, narrowband base support trunked radio system for complete two-way radio coverage in Southern Nevada, and a video conference network that provides video communications among locations in Las Vegas, NV; Livermore, CA; Los Alamos, NM; and Santa Barbara, CA.

DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

FTS2001 Transition

AT&T's private Federal Telecommunications System (FTS) 2000 network is scheduled to be discontinued in December. Nearly all FTS2001 replacement services were established before June 2001. Careful planning prevented significant disruptions of service to VA facilities during the transitions. Planning continues to anticipate unforeseen consequences of the termination of AT&T's private network.

Veterans Health Administration Wide Area Networking

Veterans Health Administration (VHA) is establishing wide area communications networks that will independently connect to the national VHA asynchronous transfer mode (ATM) backbone at two diverse sites within each of the 22 Veterans Integrated Service Networks (VISN). The major advantage of this approach is that if one VISN site loses connectivity, the network will retain connectivity among internal VISN facilities and with facilities at other VISNs through the remaining connection to the VHA ATM backbone.

VA Nationwide Teleconferencing System

The VA nationwide teleconferencing system (VANTS) provides audio and video teleconferencing services to the entire VA. VANTS services are used primarily for business meetings, program planning sessions, distance learning, interviews, and hearings. VANTS customers include VA employees, emergency personnel, State officials, hospitals, universities, and other Government agencies, such as DOD.

The video teleconferencing section of VANTS consists of two multipoint conferencing unit bridges capable of providing multipoint videoconferences at baud rates from 112 kilobits per second (Kbps) up to 768 Kbps. Sixty-four ports are available to support the most commonly used bandwidth of 384 Kbps. The video bridging services run over Integrated Services Digital Network and allow connectivity from various networks throughout the VA. The only costs associated with the use of this service are the long distance charges incurred when dialing a video teleconference and will depend on the users' video network configuration and the long distance provider. This technology allows VA employees to conduct "face-to-face" meetings without the time and expense of travel.

The audio section of VANTS currently has 576 ports for voice teleconferencing; however, an expansion/upgrade is way to increase the available ports to 744. Participants are provided toll-free numbers for easy access from any telephone within the continental United States. The estimated completion date for the expansion/upgrade is September 7, 2001.

VANTS audio and video services are available 7 days a week, 24 hours a day.

Offshore Satellite Service

The Office of Telecommunications coordinates offshore satellite telephone service via the International Maritime Satellite Organization (INMARSAT) to provide emergency voice and data telecommunications service to VA facilities operating in United States territories and possessions. Multiple portable terminal platforms are provided to ensure survival of communications facilities under the most severe natural phenomena. The INMARSAT system has been proven successful in emergency and recovery operations resulting from several hurricane events in recent years.

VA Southern California Emergency Communications System

The VA's Southern California Emergency Communications System ultra high frequency radio system was integrated into the Los Angeles Federal Government Wireless Trunking Network. Conversion from the existing analog, shared frequency radio system to the wide-area, digital trunking system provided service to a widely expanded area with a vastly increased capacity for voice, secure voice, and data communications. The Federal Trunking System is linked to all Federal and civil emergency service and law enforcement providers in the Los Angeles Basin.

New Office of the Inspector General Network

The VA Radio Frequency Management Office, working with the IG, has completed implementation of a nationwide, narrowband fixed/mobile radio network.

The new very high frequency network integrates the investigative arm of the Inspector General's (IG) office with Federal and civilian law enforcement services nationwide, and it provides unique narrowband radio frequencies for six VA regions. The new radio system provides the highest degree of security in communications available today for IG field operations.

Frequency Management Automation

As radios proliferate in the VA workplace, and the radio frequency spectrum becomes nearly saturated in every Federal frequency band, engineering a new radio frequency for a hospital or cemetery has become a complex task.

To simplify the process, the Radio Frequency Management Office acquired a new frequency management tool in the form of a Windows NT compliant software package called Spectrum XXI. The new tool allows VA technicians to compartmentalize the gigantic Federal Government Master File of Radio Frequency authorizations into VA regions, which reduces the number of records involved in a search for a new frequency. A search that once took six or more hours now can be completed in about 20 minutes, allowing two to three technicians to do the work that formerly required six to eight highly skilled specialists.

CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission of the Central Intelligence Agency (CIA) is to ensure the secure flow of all-source foreign intelligence information to the President and other selected national policy makers. To this end, CIA provides secure, rapid, and reliable round-the-clock telecommunications and information services that are—

- Modern, efficient, and interoperable to support intelligence collection and distribution requirements
- High-volume and timely for open-source collection
- Quick-reacting in support of crises and special operational requirements wherever needed.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Information Services Infrastructure operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities.

The Agency also provides telecommunications support to other U.S. Government departments, agencies, and the military services as required to support intelligence gathering activities.

CURRENT/ONGOING TELECOMMUNICATIONS ACTIVITIES

The following CIA activities support NS/EP objectives:

- Active participation in the National Communications System activities of the Committee of Principals/Council of Representatives
- Continued support of the Government Emergency Telecommunication Service, the Federal Telecommunications Standards Committee, the Telecommunications Service Priority Program, and the Shared Resources High Frequency Radio Program.

CIA SIGNIFICANT ACCOMPLISHMENTS

Continued to develop a cadre of professional personnel prepared to meet operational, technical, and system management requirements of modern telecommunications and automated information systems
Provided enhanced telecommunications services between the CIA and the U.S. military services
Continued support to Defense Message System objectives and architecture.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP TELECOMMUNICATIONS MISSION

The Federal Emergency Management Agency's (FEMA) mission is to reduce the loss of life and property and protect United States institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

FEMA's Five-Year Strategic Plan has three major goals:

- Protect lives and prevent the loss of property from all hazards
- Reduce human suffering and enhance the recovery of communities after disaster strikes
- Ensure that FEMA serves the public in a timely and cost-effective manner.

PROGRAM ACTIVITIES

In fiscal year (FY) 2001, FEMA continued to develop and coordinate its all-hazards disaster programs among Federal departments and agencies, State and local governments, and other public and private sector organizations. This effort is sustained by a comprehensive national mitigation, preparedness, response, and recovery, all-hazards emergency management capability. Additionally, FEMA functions under the authorities established by the Stafford Act, National Security Decision Directive 97, and Executive Orders 12472 and 12656.

FEMA continued to administer the Federal Response Plan and respond to Presidential disaster declarations. FEMA's Mobile Emergency Response Support detachments deployed in response to 60 Presidential disaster declarations. Additionally, FEMA participated in several emergency management and emergency telecommunications tests and exercises.

In FY 2001, FEMA updated its information technology architecture (ITA) documentation, expanding the information on the Agency's major programs. Also, an executive summary of the ITA was developed and distributed in hard copy to ranking members and chairpersons of Congress, other Federal Department and Agency heads, and national associations associated with emergency management. The ITA was also posted on the Internet at fema.gov. The executive summary of the ITA is nontechnical, and puts into context how FEMA's major programs support the road to e-FEMA. President Bush said that E-government is a priority for his administration. FEMA will take a leadership role and serve as a model agency in fully realizing E-government, which will improve service to the American public.

The National Emergency Management Information System (NEMIS) is an integrated system providing FEMA, States, and other Federal departments and agencies with automation to perform disaster and nondisaster operations. In FY 2001, NEMIS supported 64 disasters and obligated approximately $2 billion for disaster assistance. NEMIS supports all phases of emergency management, from State mitigation planning to situation assessments, providing disaster assistance, command and control, programmatic planning, emergency support, and mitigation operations. In FY 2001, NEMIS supported all disaster declarations. NEMIS supports the Individual Assistance Program, Public Assistance Grant Program, Hazard Mitigation Grant Program, and the Flood Mitigation Assistance Program.

The National Interagency Emergency Operations Center (NIEOC) at FEMA Headquarters was activated on a 24-hours-a-day basis for several Presidential disaster declarations, during which FEMA administered the Federal Response Plan. The NIEOC is the main base of operations for Federal departments and agencies in Washington, DC.

FEMA's Internet home page's popularity continues to grow. In FY 2001, an average of 811,144 pages were viewed weekly, compared with 617,537 weekly in FY 2000. Also, the site now has more than 30,000 pages available. The information published on FEMA's Web site expanded significantly. Information on flood plain hazard mapping and the dam safety section were expanded. Flood code maps can now be purchased online.

THE JOINT STAFF (JS)

NS/EP TELECOMMUNICATIONS MISSION

The Director for Command, Control, Communications, and Computer (C4) Systems (J-6) provides advice and recommendations to the Chairman of the Joint Chiefs of Staff and to the Joint Chiefs of Staff, as directed by the Chairman, on C4 matters. He will develop policy and plans, monitor programs for joint C4 systems, and ensure adequate C4 support to Commander-in-Chiefs, National Command Authority, and all joint warfighters for joint and combined military operations. He leads the C4 community, conceptualizes future C4 systems architectures, and provides direction to improve joint C4 systems. He oversees C4 support for the National Military Command System.

TELECOMMUNICATIONS STAFF ORGANIZATION

The C4 Systems Directorate (J-6) consists of the Director, a Vice Director, and 14 subordinate divisions. The Director is also the Chairman of the Military Communications-Electronics Board. Each military Department has approximately equal representation by rank, number, and importance of billets throughout the directorate. The Director and Vice Director for C4 Systems are general or flag officers from the military departments.

SIGNIFICANT ACCOMPLISHMENTS

(Refer to DOD Section)

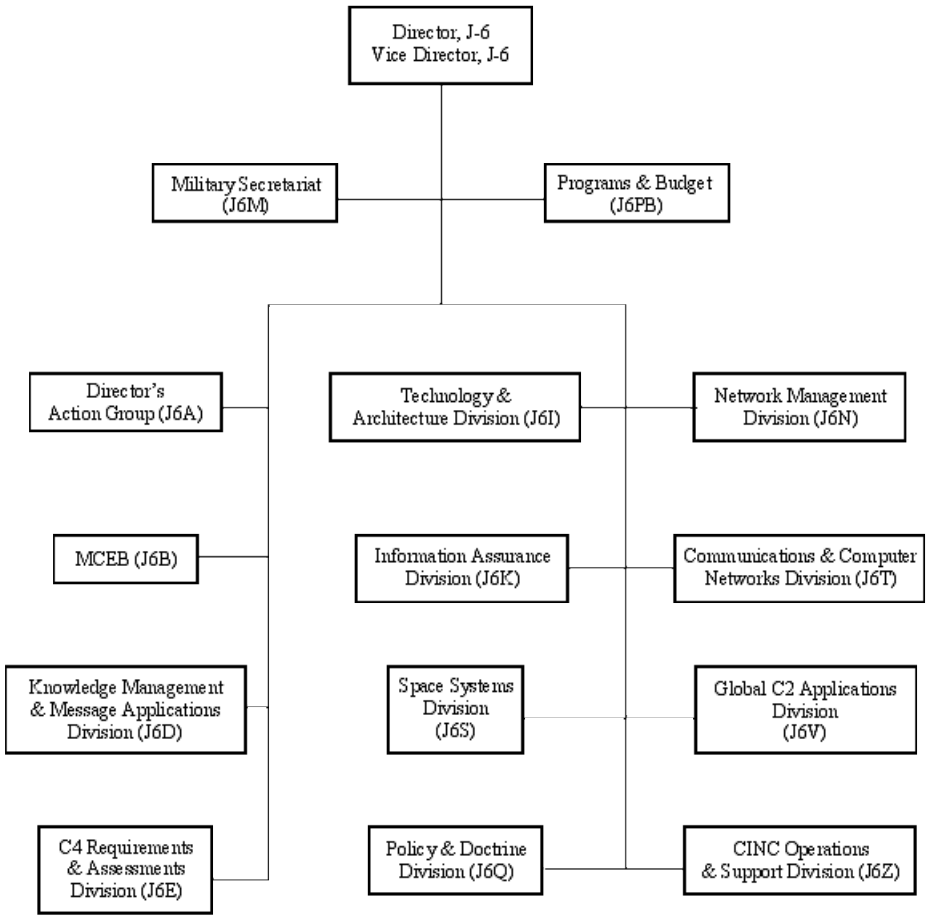
CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

(Refer to DOD Section)

PENDING ISSUES

(Refer to DOD Section)

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE



GENERAL SERVICES ADMINISTRATION (GSA)

MISSION

The General Services Administration (GSA) Federal Technology Service NS/EP mission is to ensure that federally owned or managed domestic communications facilities and services meet the national security and emergency preparedness requirements of the Federal Government.

CURRENT/ONGOING ACTIVITIES

- The GSA Federal Technology Service provides a full-time detailed employee to support the National Coordinating Center (NCC) for Telecommunications at the National Communications System (NCS), and ensures that a NCS Regional Manager/GSA Regional Emergency Communications Planner (RECP) and a Federal Emergency Communications Coordinator (FECC) are identified for each of the 10 standard Federal regions and the National Capital Region to assist the Federal Emergency Management Agency (FEMA), the Office of Science and Technology Policy (OSTP) and the NCS during disasters and national security emergencies.

- The GSA Federal Technology Service provides a full range of network services and information technology (IT) solutions that are meeting the current and future needs of the Federal Government with globally positioned NS/EP capabilities, resources, services, and solutions. NS/EP services are also available to tribal governments as well as State and local governments if they are sponsored by a Federal Government department or agency.

- The Federal Technology Service provides contract vehicles for worldwide telecommunications services, international direct distance dialing, wireless voice and data, satellite services, Internet access, technical services support, information security services, and services necessary for Critical Infrastructure Protection, and used to support the Government Information Security Reform Act. Examples are the GSA Federal Technology Service SAFEGUARD program, which is a toolkit of security products and services aimed at meeting the current security challenges facing the Federal community; the Access Certificates for Electronic Services (ACES) contracts to facilitate secure online access by the public to Government information and services; and the Federal Computer Incident Response Center (FedCIRC), which the Federal Technology Service manages.

- The Federal Technology Service supports the NCS and the National Security Telecommunications Advisory Committee by participating in fact-finding and analysis meetings.

- GSA supports the emergency requirements of several agencies, providing NS/EP telecommunications expertise, planning, and resource support through a variety of memoranda of understanding.

- In immediate response to the terrorist attacks on New York and the Pentagon, GSA activated its Emergency Operations Center, and the Federal Technology Service established a Service Response Center (SRC), staffed 24x7 by Federal Technology Service and industry partners. The GSA National Capitol region and central office moved into emergency operations, sending emergency personnel to the FEMA Emergency Response Center in the District and Mt. Weather. GSA also sent personnel to each of the FEMA Regional Operations Centers to staff Emergency Support Function (ESF) 2 (Communications) and ESF 7 (Resource Support) of the Federal Response Plan. GSA also activated Continuity of Operations Plans in several critical and impacted regions.

- WorldCom, Sprint, and Verizon were immediately contacted to provide technical personnel support to the Federal Technology Service SRC at Willow Woods, and to provide network outage information to Federal Technology Service. The GSA SRC served as a point of contact for Federal Technology Service-provided telecom and other IT facilities and services, and as a clearinghouse for information. Primarily focused on emergency, relocation, and restoration, the Federal Technology Service SRC coordinated closely with the Public Buildings Service (PBS) and the Federal Supply Service to help affected agencies return to operations.

- Under the National Plan for Telecommunications Support in Non-wartime Emergencies and the Federal Response Plan, GSA personnel from Regions 1, 2, 3, and 4 staffed ESF 2 for the NCS. A GSA RECP is assigned as the FECC in the disaster area. These individuals supported Federal, State, and local response efforts, coordinating the communications requirements of the response elements and the restoration of critical communications functions with the NCC and the Federal Technology Service SRC.

- Within 24 hours, the first daily Federal Technology Service status report was sent to Federal Technology Service customers, the NCS Committee of Principals and the Council of Representatives, and the Interagency Management Council. This status report provided a complete status update and a centralized single point of contact for Federal telecommunications and information technology solutions and services. Agencies were requested to first contact the SRC so it could direct calls to the appropriate party and mitigate the burden on New York City personnel.

- The SRC logged in about 3,400 requests for circuits in the first 2 weeks and responded to about 1,800 requests. Verizon was severely affected by the attack and was the vendor for 48 of the 52 sites out of service. Verizon has provided free wireless cellular telephones to several Government agencies for 60 days.

- In addition to having supplied the World Trade Center, GSA supplies Federal Telecommunications System (FTS) 2000/2001 long distance service to 121 locations in Manhattan and surrounding boroughs. Outages were

GENERAL SERVICES ADMINISTRATION (GSA) *continued*

reported at approximately 58 of those locations as a result of damage to local access facilities. As of September 25, outages at New York City locations had been reduced from 58 to 52. At the World Trade Center, Federal Technology Service lost 2,825 long distance voice lines and 34 data network circuits supplied by AT&T, Sprint, and WorldCom. Sprint Centrex service was down.

- IT Solutions arranged for Smartcards, card readers, laptops, and LAN wiring to support approximately 3,000 Pentagon customers moving to Crystal City. The NCR IT Solutions team worked directly with the multiple DOD and industry partners providing assistance with desktop connectivity. GSA FTS IT Solutions also opened its space to provide work locations at the Springfield, VA, office to assist the Army's Casualty War Room and Memorial Affairs Operations Center. The GSA IT Solutions team has also been working with the numerous Federal agencies displaced in New York City to reestablish their LAN networks and desktop communications capabilities. A number of regions outside the immediate impact area have received requests from DOD customers for new services on a quick response basis as a result of increased activities following the incident.

- Approximately 34 customer agencies were displaced at the Pentagon, the World Trade Center, and nearby locations that rely on GSA for telecommunications and IT service. No long distance service was lost at the Pentagon. Alternative access paths were established to each customer site in accordance with established emergency restoration priorities.

GSA SIGNIFICANT ACCOMPLISHMENTS

GSA has provided resource support to 46 Presidentially declared disasters and approximately 15 local emergencies, such as fires and floods at Government facilities this fiscal year. Federal Technology Service Emergency Communications Coordinators have supported ESF 7 from Hurricane Allison in the Southwestern United States to the major floods and fires in the Western and Southcentral United States and Puerto Rico. The FTS provided a FECC and staff to support ESF 2 for the Seattle earthquake in February and Hurricane Allison in June.

GSA's Federal Technology Service is coordinating with the NCS Telecommunications Information Sharing and Analysis Center to ensure that the Government has available the critical information and services needed to recover from attacks against its information infrastructure.

Managed Security Services (MSS) have been made available via the SAFEGUARD program to promote the development and deployment of capabilities to provide Federal agencies and departments the ability to proactively protect their information systems and resources. MSS allows agencies to select services such as intrusion detection, audit trail analysis, incident reporting, and several other network management capabilities aimed at improving the overall security profile and protection strategies for Federal information technology

The GSA Federal Technology Service SAFEGUARD program provides products and services to assist agencies in meeting their requirements under the Government Information Security Reform Act, which requires annual agency program reviews, annual Inspector General security evaluations, agency reporting to the Office of Management and Budget (OMB), and an annual OMB report to Congress. The SAFEGUARD program allows an agency to design, implement, maintain, and modify its security architecture to conform to its particular needs.

The SAFEGUARD program is providing progressive levels of support to the U.S. Customs Network Services Critical Infrastructure Protection Plan and has established a new level of collaboration with the National Security Agency (NSA). Anti-terrorism/vulnerability assessments will be conducted for 1,100 bases of the U.S. Army Reserve Corps under SAFEGUARD over the next 3 years.

SAFEGUARD also supports the National Institute of Standards and Technology Computer Security Division's efforts to protect IT systems and networks by developing security management guidance; promoting awareness of security threats, requirements, and division work products; and addressing items such as risk management, security program management, training and awareness, contingency planning, personnel security, administrative measures, and procurement; supporting outreach activities; and providing Computer Security Expert Assist Team support to Federal agencies.

Other agencies benefiting from the SAFEGUARD program include the Bureau of Printing and Engraving, the Department of Housing and Urban Development, Military Sealift Command, the United States Department of Agriculture, the DOD Computer Forensics Laboratory, the Federal Aviation Administration, the Federal Bureau of Investigation, and the Department of the Interior.

GSA SIGNIFICANT ACCOMPLISHMENTS *continued*

The Customer Advisory Board approved more than 500,000 free certificates for the ACES program for future issuance by agencies. Approximately 350,000 of those certificates have been issued.

The ACES program group has been working with the Federal Bridge Certificate Authority to provide interoperability between ACES and other Public Key Infrastructure services.

GSA's FedCIRC provides containment and recovery assistance to Government components that have been victims of computer security related events, such as an unauthorized intrusion, computer viruses, and other occurrences posing a threat to IT resources supporting critical mission functions.

GSA's FedCIRC collaborated with the National Infrastructure Protection Center, the National Security Incident Response Center, the DOD Computer Emergency Response Team (CERT), the Carnegie Mellon CERT Coordination Center, and several IT industry partners to develop effective defenses against the "Leaves Worm." FedCIRC is working with the same entities to develop protections against the "Code Red Worm" and future malicious programs.

In FY 2001 through July 31, FedCIRC had responded to 1,028 incidents. These included 277 Web site defacements and 146 incidents in which intruders gained control of the victim computer.

FedCIRC has issued 28 Advisories, 10 Incident Notes, and 74 Special Communications. The FedCIRC Web site currently receives over 71,000 hits monthly.

The final stage of the Federal Government's move of long distance telecommunications services to new FTS2001 contracts with WorldCom and Sprint has been completed. FTS2001 brings advanced, state-of-the-art, commercial-grade services to Government locations around the world. Customers at 165 Cabinet level departments and independent agencies are the beneficiaries of FTS2001 service.

A program review of FTS2001 was conducted to ensure that the requirements of Presidential Decision Directive 63 are fully met.

GSA Federal Technology Service offers a vast array of services on its constantly updated wireless and satellite services contracts. The Department of the Treasury and the Army Recruiting Command have signed for wireless service that will add 21,000 customers in the next 12 months. Satellite services are provided to the Departments of State and Defense. The Centers for Medicare and Medicaid Services (CMS) have made innovative use of DirecTV services to support their distance learning network. The CMS network will support approximately 75 continental United States locations and provide the ability to broadcast high-quality video programming at low cost. The service is ideal for agencies that need to broadcast on an occasional basis and reach many sites.

Since 1999, the Federal Technology Service has awarded 39 Metropolitan Area Acquisition (MAA) contracts in 21 metropolitan areas across the Nation. By the end of this year, we will have completed 27 cities. At that time, two-thirds of the Federal workforce will be within reach of an MAA, with attractive prices and state-of-the-art service offerings.

The Washington Interagency Telecommunication Service (WITS) 2001 program has gained the support of the noncommand and control requirements of the DOD by deciding to transition approximately 155,000 customers to WITS 2001 instead of conducting a separate acquisition to replace its existing contract for local services. DOD estimates it avoided $5 million in acquisition costs and reduced prices by 50 percent compared with its previous contract.

The Federal Technology Service and the GSA PBS are partnering within GSA to develop telecommunications in-buildings solutions. The primary objective is to ensure that our customers receive superb service and we are viewed as one GSA.

The Federal Technology Service provides vendors and agencies access to all its services, including disaster support, contingency planning, and continuity of operations services through the GSA home page (http://www.gsa.gov).

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP TELECOMMUNICATIONS MISSION

The National Aeronautics and Space Administration (NASA) Administrator shall (pursuant to Executive Order 12656) coordinate with the Secretary of Defense to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautics-related systems, equipment, and methodologies applicable to national security emergencies.

TELECOMMUNICATIONS STAFF ORGANIZATION

NASA's Associate Administrator for the Office of Space Flight has programmatic responsibility for representing the organization, on behalf of the Administrator, in the National Communications System (NCS) process. The Associate Administrator for Space Flight assigned the Deputy Associate Administrator for Space Communications as NASA's Committee of Principals member.

NASA's George C. Marshall Space Flight Center, located in Huntsville, AL, maintains lead center responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network (NISN).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

NASA continues to support the NCS in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. These include Telecommunications Service Priority, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, and the National Telecommunications Management Structure.

NASA also continues to actively participate in the Shared Resources High Frequency Radio Program, Government Emergency Telecommunications System, Interagency Committee on Search and Rescue, the Federal Wireless Users Forum, and the NCS Technology and Standards Accomplishments.

NASA NS/EP TELECOMMUNICATIONS ASSETS

- The NISN supports both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency, its contractor and research partners, and international space partners.
- NASA Tracking and Data Relay Satellite System is a constellation of geostationary satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft and other supported customer satellites.
- NASA Deep Space Network supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.
- NASA Ground Network (GN) supports low-Earth orbiting space flight missions. NASA is currently studying the commercialization of the GN facilities.
- NASA Research and Education Network is NASA's component to the Next Generation Internet initiative. It operates as a testbed for developing Internet technologies, applications, and networking tools.

NASA SIGNIFICANT ACCOMPLISHMENTS

Completed the transition of NASA's switched voice services and video teleconferencing services from the Federal Telecommunications System (FTS) 2000 contract to the FTS2001 contract

Continued to establish high performance internetworking capabilities with the Next Generation Internet partners and the university-based Internet 2 project under the Presidential Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet

Completed the installation of three new transatlantic fiber network services between NASA U.S. facilities and NASA services in Moscow, Russia.

NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP TELECOMMUNICATIONS MISSION

The Nuclear Regulatory Commission (NRC) is responsible for ensuring adequate protection of the public health and safety, the common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the United States. Activities licensed and regulated by the Commission include commercial nuclear power reactors; nonpower research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.

The Commission's NS/EP telecommunications provide for highly reliable connectivity between the NRC Operations Center, operating nuclear power plants, emergency operations facilities, and regional incident response centers. This connectivity ensures that the NRC Operations Center will immediately be notified of unusual occurrences and provides decision makers the ability to exchange relevant information during accidents/events at NRC licensed facilities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The NRC Emergency Telecommunications System (ETS), which provides NS/EP communications from nuclear power plants and major fuel cycle facilities, has been transitioned to a post-Federal Telecommunications System (FTS) 2000 system. The new ETS consists of FTS2001 direct access lines at most locations. At 23 sites, ETS is provided using the utilities' corporate communications systems. The Government Emergency Telecommunications Service (GETS) has been highly recommended as a means of enhancing access to long distance service.

NRC SIGNIFICANT ACCOMPLISHMENTS

Telecommunications Service Priority coverage has been transferred from the FTS2000 circuits of the ETS to their FTS2001 replacement circuits.
NRC encouraged licensee use of GETS as a part of contingency plans.
GETS use has been promoted as a means of improving emergency telecommunications at nuclear power plant sites.
GETS access numbers were used in the ETS transition test plan.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP TELECOMMUNICATIONS MISSION

The National Telecommunications and Information Administration (NTIA) NS/EP mission, as tasked under Executive Orders 12046, 12472, and 12656, includes serving as the executive branch telecommunications policy adviser to the President, serving as the manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board. Thus, among other things, NTIA advises and assists the President in administering a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support NS/EP functions.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The NTIA/Office of Spectrum Management (OSM) continues to plan and implement, using a phased approach, a series of Federal spectrum management system improvements that include the capability for total electronic transfer and use of Federal spectrum management data and information. It also continues to develop, field, and maintain several spectrum management automation tools for use by Federal spectrum managers to more effectively plan, coordinate, and control use of the radio frequency electromagnetic spectrum during NS/EP and normal conditions. Specific examples of these activities include the following:

- Partnered with the Department of Defense's Joint Spectrum Center to develop and field: (1) SPECTRUM XXI Version 3.0, the follow-on spectrum management software to Version 2.0, for use by all Federal spectrum managers; (2) for evaluation and testing, the Alpha-test version of an icon-based, graphical user interface supported by sophisticated logic. This interface will serve as the method Federal agencies use to develop and submit spectrum certification requests to NTIA; (3) updated CD ROM-based search software and indexes for searching electronic files of Interdepartment Radio Advisory Committee documents; (4) the Alpha-test version of the Statistical Database Viewer prototype to display in several ways various spectrum information, including allocation tables and associated spectrum-use statistics; and (5) other automated capabilities.
- Developed the architecture for alternative site processing of Federal spectrum management data, communications, and operations for NTIA essential personnel.
- Completed update of the previous electronic imaging, optical-character reading, archiving, indexing, and transferring to 60 CD ROMs all of the archived Interdepartment Radio Advisory Council documents from the past 78 years.
- Revised the Federal Spectrum Management System/Information Technology Improvements Plan to include planned outcomes and improvement goals for each identified improvement.

In addition, the NTIA/OSM—

- Participated in national emergency management and response endeavors following the terrorist attacks on September 11, 2001, in Washington, DC and New York City
- Participated in the Information Infrastructure Protection Assurance Group of the Convergence Working Group effort to draft the "Report on the Impact of Network Convergence on NS/EP Telecommunications: Initial Findings and FY02/03 Programmatic Recommendations"
- Participated in Government Emergency Telecommunications Service (GETS) User Council activities and endeavors as well as provided GETS user authorizations to new NTIA emergency essential personnel
- Participated in various activities and endeavors of the President's National Security Telecommunications Advisory Committee
- Participated in the National Communications System (NCS) Committee of Principals and Council of Representatives activities and endeavors
- Participated in NCS Shared Resources High Frequency Radio Program activities and endeavors
- Participated in the National Science and Technology Council's Critical Infrastructure Protection Research and Development Interagency Working Group activities.

NTIA SIGNIFICANT ACCOMPLISHMENTS

Conducted more than 200 meetings of the Interdepartment Radio Advisory Committee and its Subcommittees and ad hoc groups

Processed more than 75,000 frequency assignment actions submitted by Federal agencies for new frequency assignments or revisions of existing assignments

NTIA SIGNIFICANT ACCOMPLISHMENTS *continued*

Represented the U.S. Government on many spectrum policy matters at various meetings of International Telecommunication Union working groups and study groups

Served as the lead agency for the Information and Communications (I&C) Sector of the Nation's critical infrastructures; as such, chaired the I&C Sector Working Group and its subcommittees to promote information sharing and coordinated actions to mitigate critical infrastructure protection risks and vulnerabilities in all levels of the I&C Sector

Conducted monthly training classes for Federal spectrum managers in use of the SPECTRUM XXI Spectrum Management System for Windows.

NATIONAL SECURITY AGENCY (NSA)

NS/EP TELECOMMUNICATIONS MISSIONS

The National Security Agency (NSA) has an operational mission to support the critical intelligence needs of the Department of Defense (DOD) and national security community, and to provide the technical support necessary to develop and maintain the security and protection of NS/EP telecommunications.

TECHNOLOGY AND INFORMATION SYSTEMS SECURITY STAFF ORGANIZATIONS

Within NSA, two organizations share in supporting NS/EP-related activities. The Information Technology Infrastructure Services group plans and operates the telecommunications systems and networks linking Agency elements worldwide and provides Agency connectivity to other Government services.

The Information Assurance (IA) Directorate is responsible for developing information security (INFOSEC) products and providing services to enhance the security of telecommunications systems. Both organizations work in close collaboration with the military services and defense agencies in support of overall DOD initiatives. In accordance with the Directorate's National Manager responsibilities under National Security Directive 42, INFOSEC products and services are also applicable across the Government for the protection of classified and sensitive national security information. NSA's customers include a broad range of users of the National Information Infrastructure and the critical infrastructure communities. Information security activities include a close working relationship with the National Institute of Standards and Technology.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Crypto-Modernization Program

The Crypto-Modernization Initiative is required to modernize the DOD's IA capabilities to replace an aging cryptographic product inventory, meet increased interoperability requirements, keep pace with information technology evolution, and achieve the vision of Defense in Depth espoused by Global Information Grid initiative. During the past three decades, the NSA has delivered a variety of security products to provide high-grade protection of critical command, control, and intelligence systems. Much of this equipment has hard-wire cryptography, which is nearing its useful cryptographic life, and difficult to maintain. The military needs to interoperate dynamically with allied/coalition partners. This need is driving our IA solutions to be directly releasable and/or interoperable with our allies. The evolution of the Department's communications systems to "network centric" architectures requires new IA solutions. NSA has launched an initiative with its customer community to ensure a smooth transition to new algorithms and solutions.

Defense-wide Information Assurance Program

NSA supported the ongoing activities of DOD's Defense-wide Information Assurance Program (DIAP) to provide central oversight and coordination of DOD IA activities. Key aspects of the DIAP include people, operations, and technology. Specific fundamentals in the technology area include the concept of Defense-in-Depth and the notion of Protect, Detect, and Respond. Detect and respond capabilities include use of intrusion detection tools to identify and react to attacks on information infrastructure or systems. In partnership with industry development of the IA Technical Framework was a key contribution in providing architectural guidance for the DIAP. The IA Technical Framework continues to evolve for customer use.

Key Management Infrastructure

NSA developed a high-assurance, robust key management infrastructure (KMI) for the national security community. NSA also began to acquire a new KMI with a centralized service node to simplify key ordering and management operations.

Accreditation Procedures

NSA developed accreditation procedures through the National Information Assurance Partnership to advance processes for approving commercial INFOSEC products and services in accordance with the International Common Criteria for Information Technology Security. NSA sponsored protection profiles for products and systems, including firewalls, virtual private networks, peripheral sharing switches, remote access, operating systems, single level Web, smart cards, intrusion detection systems, public key infrastructure (PKI) protection mobile code, and directory services.

Critical Infrastructure Protection Responsibilities

NSA provided services including threat, vulnerability, and risk assessments to member organizations that provide security guidance and advice, especially with respect to dependence on the critical infrastructure and Presidential Decision Directive 63 responsibilities.

PKI

In partnership with DISA, NSA assumed leadership of the DOD PKI Program Management Office. The Class 3 Release 2 infrastructure went operational in July 2000. As of this writing, more than 110,000 Class 3 Public Key Certificates have been issued in DOD, including 32,000 common access cards. In addition, continued deployment of the Defense Message System has occurred.

Critical Infrastructure Assurance Program

NSA continued support of the Critical Infrastructure Assurance Program. Special focus was provided in the area of new development of intrusion detection tools.

National Security Telecommunications Information Systems Security Committee

The Agency also continued to lead the activities of the National Security Telecommunications Information Systems Security Committee for Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

IA Solution Strategy

NSA continued to evolve the IA Solution Strategy to make available a set of products to construct secure computer networks in support of a wide variety of missions. NSA's approach is to work closely with customers and commercial IT vendors to

NATIONAL SECURITY AGENCY (NSA) *continued*

understand their present and future needs. As a result, the technological underpinnings of the strategy are driven by information management approaches and existing constraints rather than by independent security solutions. Solutions and products provide several benefits, including—

- Writer-to-reader information security services, including data integrity and access control
- Network protection technologies (e.g., ATM encryptors)
- Boundary layer protection technologies (e.g., firewalls and guards)
- Support for applications, such as electronic mail and file transfer
- Protection against unauthorized disclosure or modification of information while enabling the integration of systems functioning at different sensitivity levels
- Security guidance for ongoing NCS programs, including GETS and Emergency Response Link.

September 11 Attacks
In response to the 11 September 01 terrorist attacks, NSA provided quantities of security products on an emergency basis to protect voice and data communications across the national security community. This support included installation, training, and cryptographic keying material.

National Security Incident Response Center
The National Security Incident Response Center (NSIRC) at NSA provides tailored, all source, reporting and operational expertise on matters addressing the threat, detection, reaction, and warning and response to intrusions into U.S. Government networks. Immediately after the events of 11 September 01, the NSIRC began issuing two new series of reports: 1) NSIRC Threat Summaries, which present a summary of recent foreign SIGINT threat information that directly applies to U.S. military and government organizations; and 2) The DIO Global Highlights, a joint effort of the NSIRC and the Joint COMSEC Monitoring Activity, which present a sample of what we know to be adversary SIGINT operations, and the types of U.S. information being disclosed to those SIGINT operations.

UNITED STATES POSTAL SERVICE (USPS)

NS/EP TELECOMMUNICATIONS MISSION

The U.S. Postal Service (USPS) has not been assigned any specific NS/EP telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs, engineers, and develops telecommunications systems, services, and solutions to support day-to-day organizational, administrative, and operational mission requirements. Telecommunications facilities dedicated specifically to NS/EP are therefore limited in scope.

SIGNIFICANT ACCOMPLISHMENTS

The following accomplishments will enhance the ability of USPS to support the overall mission and provide a robust continuity of business program:

- During FY 2001, the USPS continued the rollout of the Associate Office Infrastructure (AOI) program to support the national deployment of the point of service (POS1) systems. The USPS met the goal to implement this standard service suite at more than 16,000 of its retail locations by the end of FY 2001. The Postal Service maintains the world's largest Novell Netware Directory Structure (NDS), with over 265,000 network objects in the NDS tree, and over 1,300 Novell servers providing access for more than 150,000 user accounts.

- In support of the AOI project, Telecommunications Services implemented more than 12,500 very small aperture terminal (VSAT) systems to provide a wireless, satellite-based, backup telecommunications architecture at the large associate offices. These systems replaced Integrated Services Digital Network services previously provided. The systematic implementation of VSAT backup services has impaired the USPS Managed Network Services (MNS) national data network reliability from less than 85 percent to more than 99 percent. This backup architecture eliminates reliance on LEC-based transport (last mile) from the remote facility to the serving wire center of the Public Switched Telephone Network (PSTN). This strategy has also supported the USPS plan of alternative routed services that reduce outages by backup services connecting via alternative paths.

- In support of the USPS POS1 Program, the USPS information technology (IT) Solutions Program implemented over 5,500 VSAT systems nationally as the primary telecommunications architecture at selected small associate (retail and delivery) offices. The VSAT systems are engineered to provide transmission control protocol/Internet protocol- (IP) based local access network (LAN) and wide area network data networking capability for all local telecommunications requirements of the retail and delivery offices. These VSAT systems are also being installed in Alaska, Hawaii, and Puerto Rico to provide a seamless continental United States/outside the continental United States satellite network architecture. Quickly becoming the world's largest and most robust satellite network, it is anticipated that 7,000 additional VSAT (as primary) systems will be installed beginning FY 2002. VSAT systems are also a critical component in the USPS continuity of business program, which will provide alternative network access restoration if a catastrophic failure or natural disaster occurs.

- In addition, in partnership with the National Center for Employee Development in Norman, OK, the Telecommunications Services Wireless Program has developed a data streaming IP video solution to enhance and replace the existing Postal Satellite Training Network. This solution was demonstrated earlier this year and will undergo a pilot implementation at selected locations during first quarter FY 2001. The new video solution will provide all existing PSTN services and an interactive distance learning user keypad with a return Voice over IP satellite channel. This multimedia training tool will be piloted at selected USPS field retail and delivery units and at specific headquarters field units that have a VSAT system (as described above) installed.

- More than 110,000 Switched Voice Services (SVS) were switched to WorldCom under the USPS MNS contract. Also, over 4,000 SVS were migrated to the Sprint Federal Telecommunications System 2001 (FTS2001) contract, and over 260 SVS services in Alaska were migrated to the WorldCom FTS2001 contract.

- To implement LANs at facilities that cannot be installed via traditional structured wiring for connectivity, Telecommunications Services has successfully implemented numerous wireless LAN systems, following the International Telecommunication Union (ITU) 802.11 and 802.11b standards, for 3 Megabits per second (MBps) and 11 MBps requirements, respectively. In addition, USPS has selected the ITU 802.11b standard for wireless extensions of traditional 10/100BaseT LAN networks on the workroom floor at various processing and distribution centers. Breezecom and CISCO wireless LAN components have been deployed extensively.

- In addition to daily computing and network operational responsibilities, the Information Systems organization also provided certification of new national applications (certifying over 75 in FY 2001) and interoperability testing of common off the shelf products on standard computing systems platforms.

- Throughout FY 2001, significant efforts have been undertaken to ready the agency to shift from a Microsoft NT domain name system-based structure to a Windows 2000 Active Directory architecture.

- During this past fiscal year, the Postal Service created a new policy and operational group within the IT organization to address information security throughout the corporation.

- To support the upcoming federally mandated narrowband requirements for land mobile radio (LMR) systems, the Telecommunications Services Wireless Program has initiated a competitive solicitation for a multiple vendor, indefinite delivery, indefinite quantity contract for radio frequency analysis, engineering, hardware/software implementation, and maintenance contract. This contract vehicle, which was awarded September 1, 2000, provides the most comprehensive handheld, base station and repeater LMR systems solution package within the civilian Federal arena. More than 125 frequency assignments were converted to narrowband in FY 2001.

FEDERAL RESERVE BOARD (FRB)

NS/EP TELECOMMUNICATIONS MISSION

The Federal Reserve Board's (FRB) NS/EP responsibilities relate to the "maintenance of the economic posture" and, in particular, the "maintenance of national monetary, credit, and financial systems." The FRB does not have telecommunications assets listed as National Communications System (NCS) primary assets. Federal Reserve Banks, not the FRB, own or lease the Federal Reserve System's significant telecommunications assets.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Assistant Director of the Information Technology program in the Board's Division of Reserve Bank Operations and Payment Systems has responsibility for oversight of the Federal Reserve Banks' telecommunications services and serves as a liaison member on the NCS Committee of Principals.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial telecommunications infrastructure and payment systems. The FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential telecommunications services supporting large-value payment systems, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. The FRB also continues to sponsor the Government Emergency Telecommunications Service (GETS) for essential Federal Reserve Bank services.

FRB SIGNIFICANT ACCOMPLISHMENTS

The FRB focused its NS/EP activities on its sponsorship role for assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993. By the end of this fiscal year, the FRB will have sponsored 1,209 active TSP assignments. For the period 10/1/2000 to 9/30/2001 the FRB sponsored 243 active TSP assignments, including 84 TSP provisioning assignments for new service resulting form the 9/11/2001 event. The 84 circuits were deemed critical to the maintenance of the national economic posture and to support Fedwire as an NS/EP service. Circuits specifically used by a depository institution severely affected by the disaster to support large-value funds and securities operations were also sponsored.

The FRB continues to request TSP assignments for those circuits using Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions.

The FRB continues to sponsor a TSP assignment for circuits used by other payment systems (e.g., the Society for Worldwide Interbank Financial Telecommunications [SWIFT] and the Clearing House Interbank Payments System [CHIPS] that meet FRB's eligibility criteria).

The FRB has implemented GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption. Further, the Federal Reserve sponsors SWIFT and CHIPS participation in GETS.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The Federal Communications Commission (FCC) has undergone major changes in top management, including the appointments of Commissioner Michael K. Powell as its newest chairperson, as well as three new commissioners: Kathleen Q. Abernathy, Michael J. Copps, and Kevin J. Martin. Several new bureau and office chiefs have been tasked with further developing and implementing management and administrative responsibilities within their respective offices.

The FCC adopted a Notice of Proposed Rulemaking to explore options for allocating spectrum for new advanced mobile and fixed terrestrial wireless services. These "third generation" services should provide worldwide design equipment and service compatibility and multimedia applications.

In accordance with an FCC extension of the Communications Assistance for Law Enforcement Act, wireless, cellular, and broadband personal communications services carriers, implementation of a packet-mode capability and six Department of Justice/Federal Bureau of Investigation "punch list" capabilities must be completed by September 30, 2001.

Under FCC rules, carriers are to begin rolling out phase II of the wireless enhanced 911 service in October 2001, which when implemented, will generally enable the location of 911 calls within 100 meters or more to be reported. This will enable law enforcement and emergency personnel to locate emergencies and do their lifesaving work more quickly, effectively, and efficiently.

The FCC also initiated two rule makings aimed at promoting telecommunications services on American Indian tribal and Alaskan Native lands.

On February 25, 2001, the FCC renewed the charter of the Public Safety National Coordination Committee (PSNCC) for 2 years. The PSNCC solicits input from the public safety community concerning the 700 megahertz (MHz) public safety band intended to provide capability for an interoperable, nationwide public safety communications system.

The FCC sponsored a conference on October 31, 2000, with the Center for Global Security Research on network security reliability in the 21st century, which was intended to increase understanding of telecommunications network security, identify relevant areas of research, and promote understanding of the roles of industry and Government in facilitating a robust communications infrastructure.

The FCC's Network Reliability and Interoperability Council has been working on improving the reliability and interoperability of our Nation's telecommunications networks. This work has included coordinated efforts on all digital subscriber lines, packet switching, and Internet technologies, in addition to the council's traditional work on telephony.

The FCC took steps to make more spectrum available through the development of secondary markets and new technologies such as software defined radios, to facilitate more efficient spectrum utilization.

The FCC initiated a proposed rule making to reallocate 27 MHz spectrum from Government use for non government services. This relocation should enable the development of new technologies and services, and provide spectrum relief for congested private and commercial frequencies.

The FCC privatized standards-setting and certification processes for telecommunications equipment, such as telephone, fax machine, or modems. This move is expected to bring innovative equipment to the marketplace faster, without harming the telephone network.

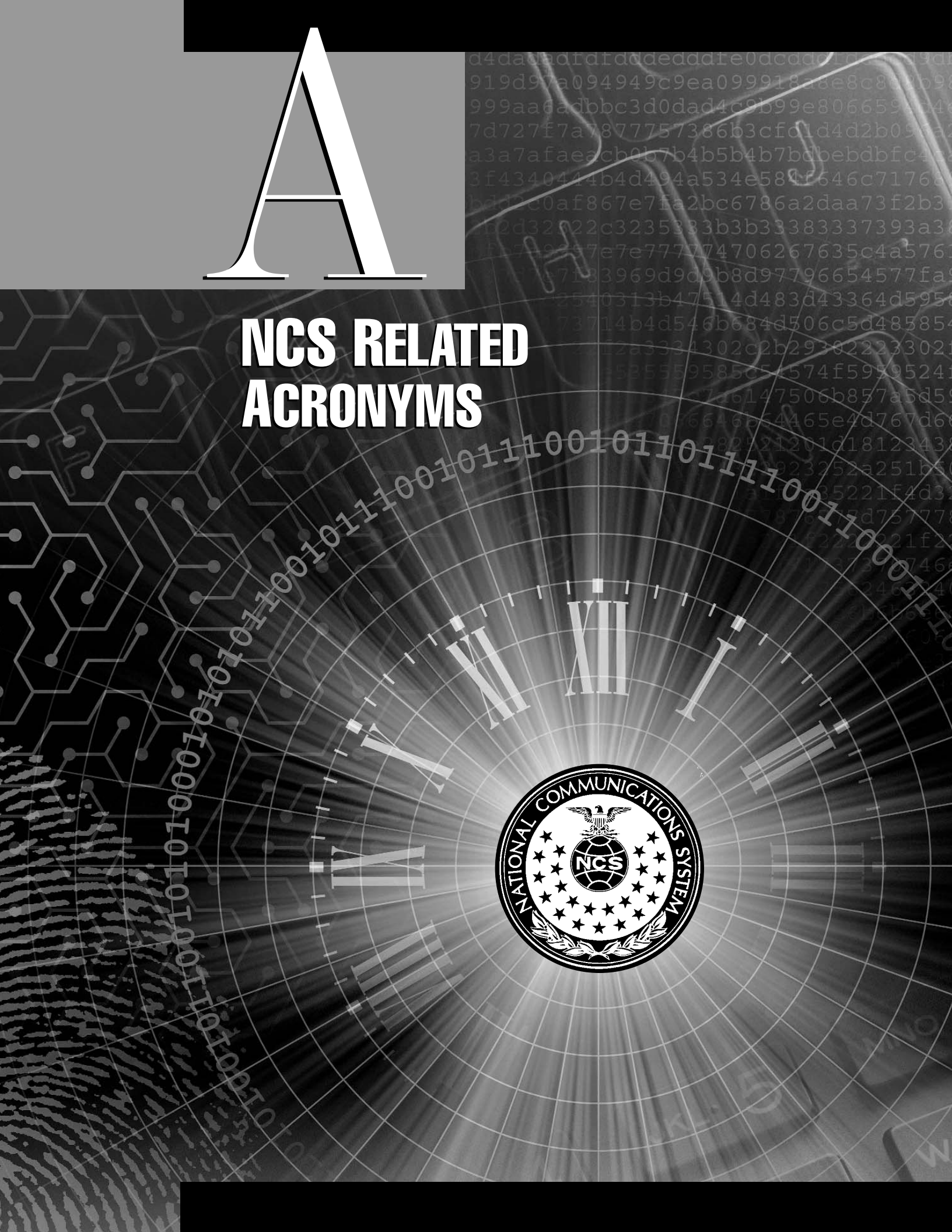
The FCC issued a Notice of Proposed Rulemaking in response to petitions to change the Emergency Alert System (EAS). Petitioners proposed changes to the EAS equipment, test procedures, and the authorized event codes.

In approving the license transfers from VoiceStream Wireless and Powertel to Deutsche Telekom, the Commission clarified that sections 310(a) and (b)(4) of the Communications Act do not prohibit foreign governments from having indirect ownership of Commission radio licenses in excess of 25 percent unless the Commission finds that the public interest would be served by denial in a particular case.

FCC personnel provided support to the Secret Service and other Federal and local law enforcement groups during the Presidential inauguration.

A

NCS Related Acronyms



A

NCS Related Acronyms

A	
ACES	Access Certificates for Electronic Services
ACN	Alerting and Coordinating Network
ACR	Alternate Carrier Routing
AGCS	AG Communications Systems
AIN	Advanced Intelligent Network
AL	Albuquerque Operations Office
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
AOI	Associate Office Infrastructure
ASD	Assistant Secretary of Defense
ATG	Advanced Technology Group
ATM	Asynchronous Transfer Mode
B	
BICC	Bearer Independent Call Control
C	
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computer
CAB	Communications Assessment Branch
CCP	Classified Connectivity Program
CCPC	Civil Communications Planning Committee
CEP	Civil Emergency Planning
CERT	Computer Emergency Response Team
CHIPS	Clearing House Interbank Payments System
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CMRS	Commercial Mobile Radio Service
CMS	Centers for Medicare and Medicaid Services
COOP	Continuity of Operations

COP	Committee of Principals
COR	Council of Representatives
CRD	Capstone Requirements Document
CTF	Convergence Task Force
CWG	Convergence Working Group
CWIN	Cyber Warning Information Network

D

DEA	Drug Enforcement Administration
DHHS	Department of Health and Human Services
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMAT	Disaster Medical Assistance Team
DNMS	Digital Network Management System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOENet	Department of Energy Corporate Network
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DOTMLPF	Doctrine, Organization, Training and Education, Material, Leadership, Personnel, and Facilities

E

EAS	Emergency Alert System
ECN	Emergency Communications Network
E-Forms	Electronic Forms
E-Mail	Electronic Mail
E.O.	Executive Order
EOC	Emergency Operations Center
EOT	Emergency Operations Team
ERT	Emergency Response Training
ESF	Emergency Support Function
ETS	Emergency Telecommunications System

F

FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCP	Functional Capability Package
FECC	Federal Emergency Communications Coordinator
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FLEWUG	Federal Law Enforcement Wireless Users Group
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
FTS	Federal Telecommunications System
FTSC	Federal Telecommunications Standards Committee
FWUF	Federal Wireless Users Forum
FY	Fiscal Year

G

GETS	Government Emergency Telecommunications Service
GHz	Gigahertz
GIG	Global Information Grid
GN	Ground Network
GNOSC	Global Network Operations and Security Center
GPRA	Government Performance and Results Act
GSA	General Services Administration

H

HF	High Frequency
HPC	High Probability of Completion
HQ	Headquarters
HS	Hanford Site

I

I&C	Information and Communications
IA	Information Assurance
IAM	Initial Address Message
IC	Integration Contract
IEPS	International Emergency Preference Scheme
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IG	Inspector General
IIAM	Infrastructure Integrity, Analysis, and Modeling
IMA	Individual Mobilization Augmentee
INFOSEC	Information Security
INMARSAT	International Maritime Satellite Organization
INS	Immigration and Naturalization Service
IP	Internet Protocol
IPT	Integrated Product Team
IS	Information Superiority
ISAC	Information Sharing and Analysis Center
ISAS	Information Sharing and Analysis System
ISCIPTF	Information Sharing for Critical Infrastructure Protection Task Force
ISPG	Information Security Policy Group
IT	Information Technology
ITA	Information Technology Architecture
ITU	International Telecommunication Union
IXC	Interexchange Carrier

J

JCN	Justice Consolidated Network
JMD	Justice Management Division
JS	Joint Staff

K

KBps	Kilobits per Second
KMI	Key Management Infrastructure

L

LAN	Local Access Network
LEC	Local Exchange Carrier
LECMap	Local Exchange Carrier Mapping
LMBATF	Last Mile Bandwidth Availability Task Force
LMR	Land Mobile Radio
LNP	Local Number Portability
LRTF	Legislative and Regulatory Task Force
LRWG	Legislative and Regulatory Working Group

M

MAA	Metropolitan Area Acquisition
MBps	Megabits per Second
MHz	Megahertz
MNS	Managed Network Service
MSC	Mobile Switching Center
MSS	Managed Security Service

N

NANPA	North American Numbering Plan Administrator
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCC-ISAC	National Coordinating Center for Telecommunications-Information Sharing and Analysis Center

NCS	National Communications System
NCW	Network Centric Warfare
NDS	Netware Directory Structure
NEMIS	National Emergency Management Information System
NGN	Next Generation Network
NIEOC	National Interagency Emergency Operations Center
NIIF	Network Interconnection Interoperability Forum
NISN	National Aeronautics and Space Administration Integrated Services Network
NITC	National Information Technology Center
NPA	Numbering Plan Area
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NS/EPC	Committee for National Security and Emergency Preparedness Communications
NSIE	Network Security Information Exchange
NSIRC	National Security Incident Response Center
NSTAC	National Security Telecommunications Advisory Committee
NTA	National Telecommunications Alliance
NTCN-HF	National Telecommunications Coordinating Network-High Frequency
NTIA	National Telecommunications and Information Administration
NV	Nevada Operations Office
NWCIP	National Wireless Communications Infrastructure Program

O

OASD/C3I	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OCIO	Office of the Chief Information Officer
OEP/NDMS	Office of Emergency Preparedness/National Disaster Medical System
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPCZ	Overseas Presence Collaboration Zone
OR	Oak Ridge Operations Office
OSM	Office of Spectrum Management
OSTP	Office of Science and Technology Policy
OTAR	Over-The-Air-Rekey

P

PAS	Priority Access Service
PBS	Public Buildings Service
PBX	Private Branch Exchange
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
POS1	Point of Service
POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PSNCC	Public Safety National Coordination Committee
PSTN	Public Switched Telephone Network
PTS	Priority Telecommunications System

R

R&D	Research and Development

RDXTF	Research and Development Exchange Task Force
RECP	Regional Emergency Communications Planner
RM-HF	Regional Managers High Frequency Radio Network

S

SATCOM	Satellite Communications
SHARES	Shared Resources High Frequency Radio Program
SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SNL	Sandia National Lab
SRC	Service Response Center
SS7	Signaling System 7
STU-III	Secure Telephone Unit—Third Generation
SVS	Switched Voice Service
SWIFT	Society for Worldwide Interbank Financial Telecommunications

T

T-CIP	Telecommunications Critical Infrastructure Protection
TESP	Telecommunications Electric Service Priority
TIA	Telecommunications Industry Association
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks
TREAS	Department of the Treasury
TRS	Trunked Radio System
TSP	Telecommunications Service Priority
TSS	Telecommunications Services Staff

U

UHF	Ultra High Frequency
USDA	United States Department of Agriculture
USMS	United States Marshals Service
USPS	United States Postal Service
USSPACECOM	United States Space Command
UWB	Ultra-Wideband

V

VA	Department of Veterans Affairs
VANTS	Department of Veterans Affairs Nationwide Teleconferencing System
vDOINET	Department of Interior Network
VHA	Veterans Health Administration
VHF	Very High Frequency
VISN	Veterans Integrated Service Network
VSAT	Very Small Aperture Terminal

W

WIN	Wireless Intelligent Network
WITS	Washington Interagency Telecommunication Service
WTC	World Trade Center

The NCS remains a focal point for industry and Government cooperation to ensure that reliable, interoperable, and secure telecommunications are available to fulfill the Nation's NS/EP requirements under all conditions. The existing industry/Government partnership provides a solid foundation upon which the NCS can build to ensure that the Nation's future communications needs are met.

NATIONAL COMMUNICATIONS SYSTEM (NCS)

701 South Courthouse Road
Arlington, Virginia
22204-2198

http://www.ncs.gov