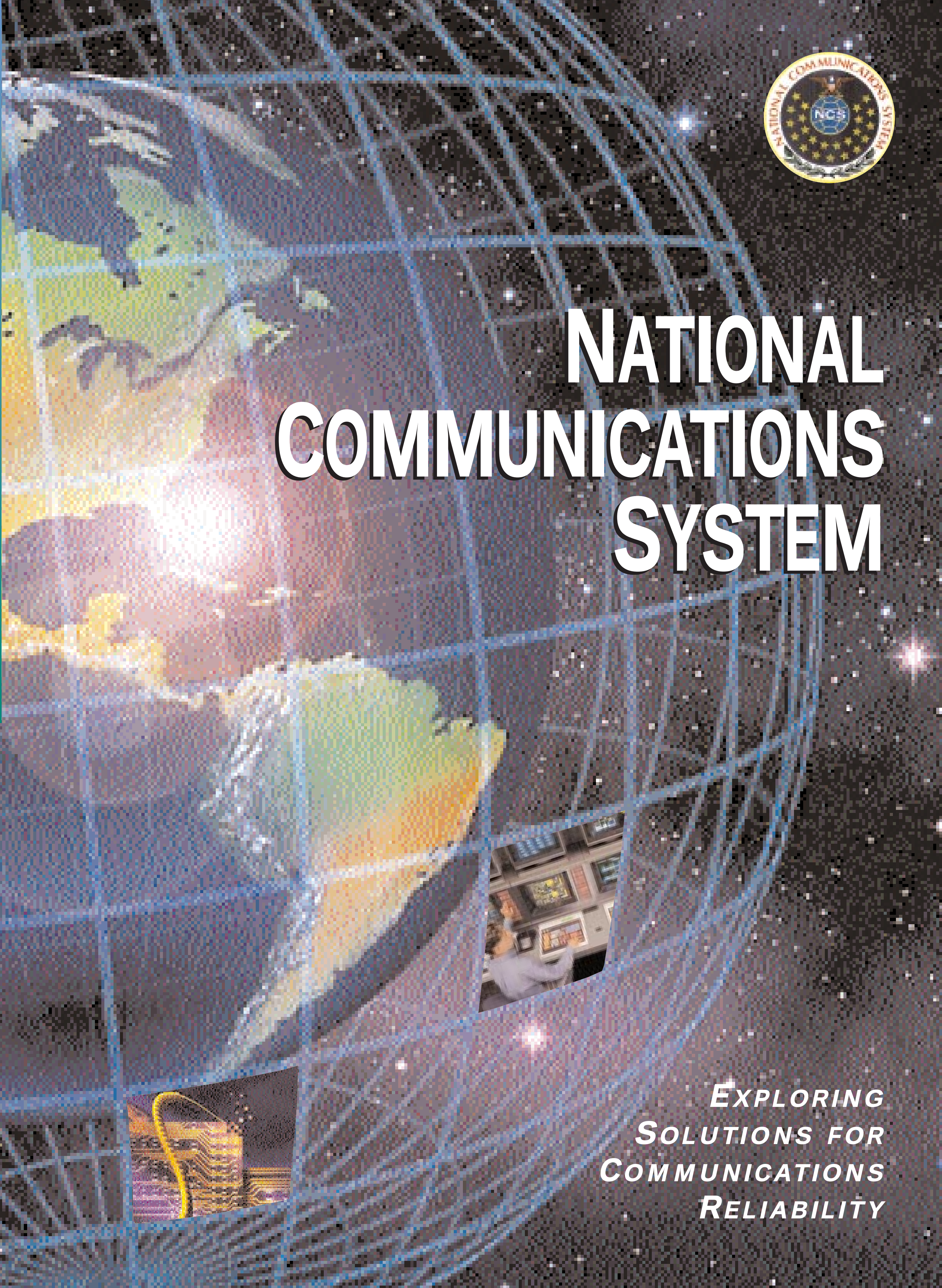
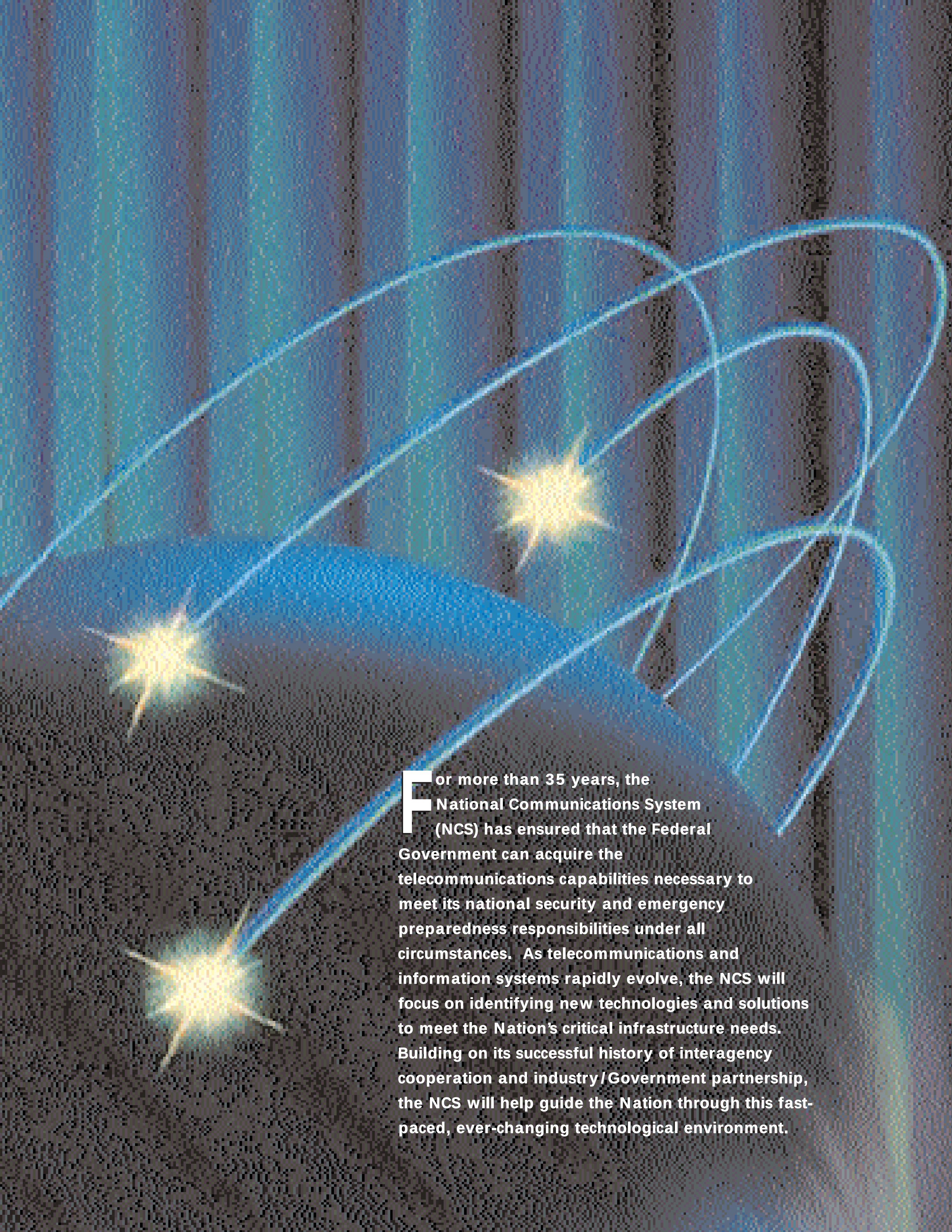
FY 2000



NATIONAL COMMUNICATIONS SYSTEM

Exploring Solutions for Communications Reliability



For more than 35 years, the National Communications System (NCS) has ensured that the Federal Government can acquire the telecommunications capabilities necessary to meet its national security and emergency preparedness responsibilities under all circumstances. As telecommunications and information systems rapidly evolve, 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.

FY2000

NATIONAL COMMUNICATIONS SYSTEM

PREPARED BY THE OFFICE OF THE MANAGER, NATIONAL COMMUNICATIONS SYSTEM

EXPLORING SOLUTIONS FOR COMMUNICATIONS RELIABILITY

FOREWORD

During Fiscal Year (FY) 2000, the National Communications System (NCS) saw significant changes in leadership as Diann L. McCoy became Deputy Manager in November 1999 and I became Manager in June 2000. As the new Manager of the NCS, I am honored to have the opportunity to influence efforts to ensure continued fulfillment of the national security and emergency preparedness (NS/EP) community's telecommunications needs during our journey into the new Millennium.

The overwhelming concern that faced the NCS as the fiscal year began was the potential disruption to NS/EP telecommunications from the Year 2000 (Y2K) computer problem. Preparation for the Y2K transition witnessed an unprecedented level of cooperation between industry and Government organizations, with the NCS playing a major role in facilitating this cooperation. During the Y2K rollover, the National Coordinating Center for Telecommunications (NCC) served as a focal point for information sharing within the telecommunications industry and between the telecommunications industry and Government. The NCC's Y2K database registered more than 96,000 hits during the New Year rollover period and almost 12,000 hits during the Leap Year rollover period. Eighty-two companies in 41 countries reported the status of their networks at a minimum of 10 scheduled intervals over the rollover period. Overall, the existing relationship between industry and Government within the NCC contributed to the success of the Y2K coordination effort.

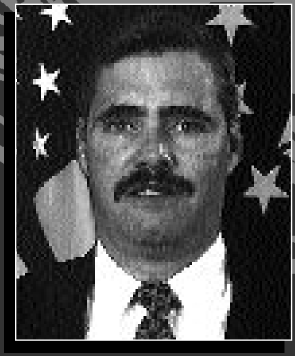
The NS/EP community also took advantage of NCS programs in preparing for Y2K. The Telecommunications Service Priority Program experienced a dramatic increase in the number of requests for authorization codes before the Y2K event. Also, the Government Emergency Telecommunications Service Program issued more personal identification numbers during the year than it had issued in all previous years.

As the Y2K event quietly passed, the NCS was able to shift its focus to the issue of critical infrastructure protection. While reliability, availability, and security of the telecommunications infrastructure have always been major concerns for the NCS and the President's National Security Telecommunications Advisory Committee (NSTAC), the issuance of Presidential Decision Directive 63 in May 1998 focused other parts of industry and Government on the security of critical infrastructures. In FY 2000, the NCS and NSTAC continued to lead by example. In January 2000, the NCC was designated as an Information Sharing and Analysis Center for telecommunications. In May 2000, NSTAC held its 23rd meeting in Colorado Springs, Colorado. In conjunction with its new leadership role in computer network defense, U.S. Space Command hosted the NSTAC meeting to provide a forum for new ideas and discussion with industry partners in this emerging critical infrastructure protection field.

FY 2000 demonstrated that despite our many challenges, the NCS will continue to ensure the availability of telecommunications services to fulfill NS/EP requirements. Although our challenges change, the NCS mission remains the same. The NCS mission is to develop an evolutionary NS/EP telecommunications architecture, to continually identify evolving NS/EP telecommunications requirements, and to promote NS/EP service enhancements that take advantage of new technologies. By continuing to foster industry and Government partnerships to this end, the NCS will continue to develop strategic solutions to ensure that NS/EP telecommunications needs are met. I look forward to working with you on the many challenges the new century will present.

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

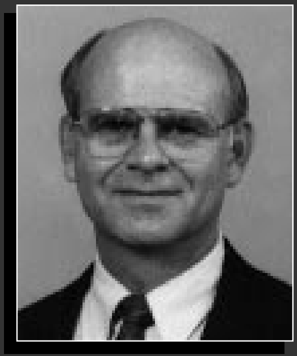
Ms. Diann L. McCoy
Deputy Manager



Dr. Peter A. Fonash
Chief
Technology and Programs

Capt Lynne Hicks, USN
Chief
Operations Division

Mr. Larry E. Wheeler
Chief
Plans and Resources Division



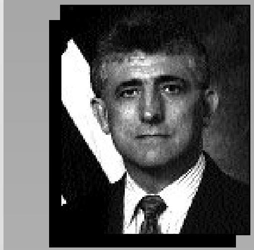
Mr. Frederick W. Herr
Chief
Customer Service Division

NCS Committee of Principals

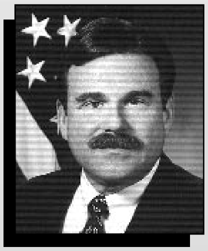
Department of State
(DOS)
Mr. Fernando Burbano

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

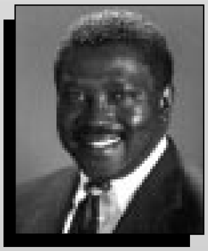
Department of Defense
(DOD)
RADM. Robert M. Nutwell, USN



Department of Justice
(DOJ)
Mr. Robert Miller

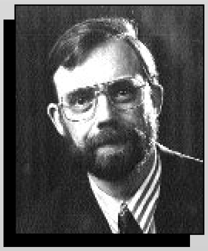


Department of the Interior
(DOI)
Mr. Daryl W. White

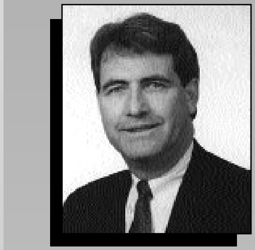


United States Department of Agriculture (USDA)
Mr. Ira L. Hobbs

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.

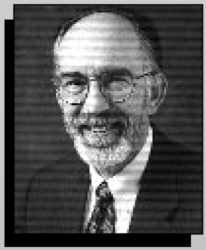
Department of Energy
(DOE)
Mr. John M. Gilligan

Department of Veterans Affairs (VA)
Mr. Robert P. Bubniak

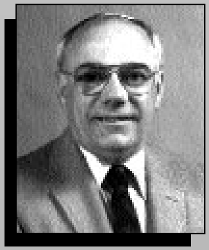
Federal Emergency Management Agency
(FEMA)
Mr. G. Clay Hollister

The Joint Staff (JS)
LTG John L. Woodward, Jr., USAF

General Services Administration
(GSA)
Ms. Sandra Bates



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



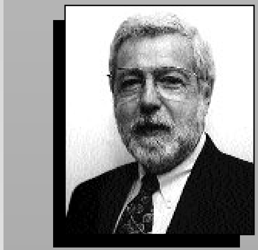
Nuclear Regulatory Commission
(NRC)
Mr. Frank J. Congel

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

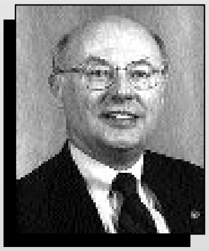
NCS Council of Representatives

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

Department of the Treasury
(TREAS)
Mr. Edd Barnes

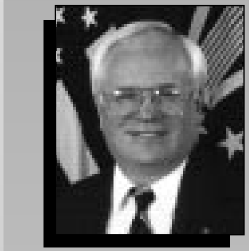
Department of Defense (DOD)
Capt. Todd D. Tracy

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

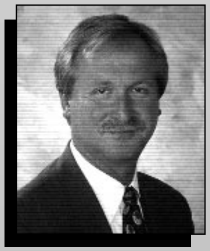


Department of Commerce
(DOC)
Mr. Jorome T. Gibbon

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. Patrick Hargett



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

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

The Joint Staff
(JS)
Capt. Kathryn DiMaggio,
USN

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

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

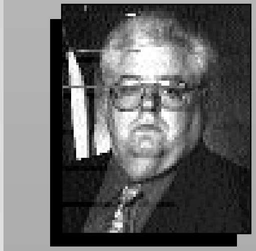
Nuclear Regulatory
Commission
(NRC)
Mr. Joseph G. Giitter

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

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

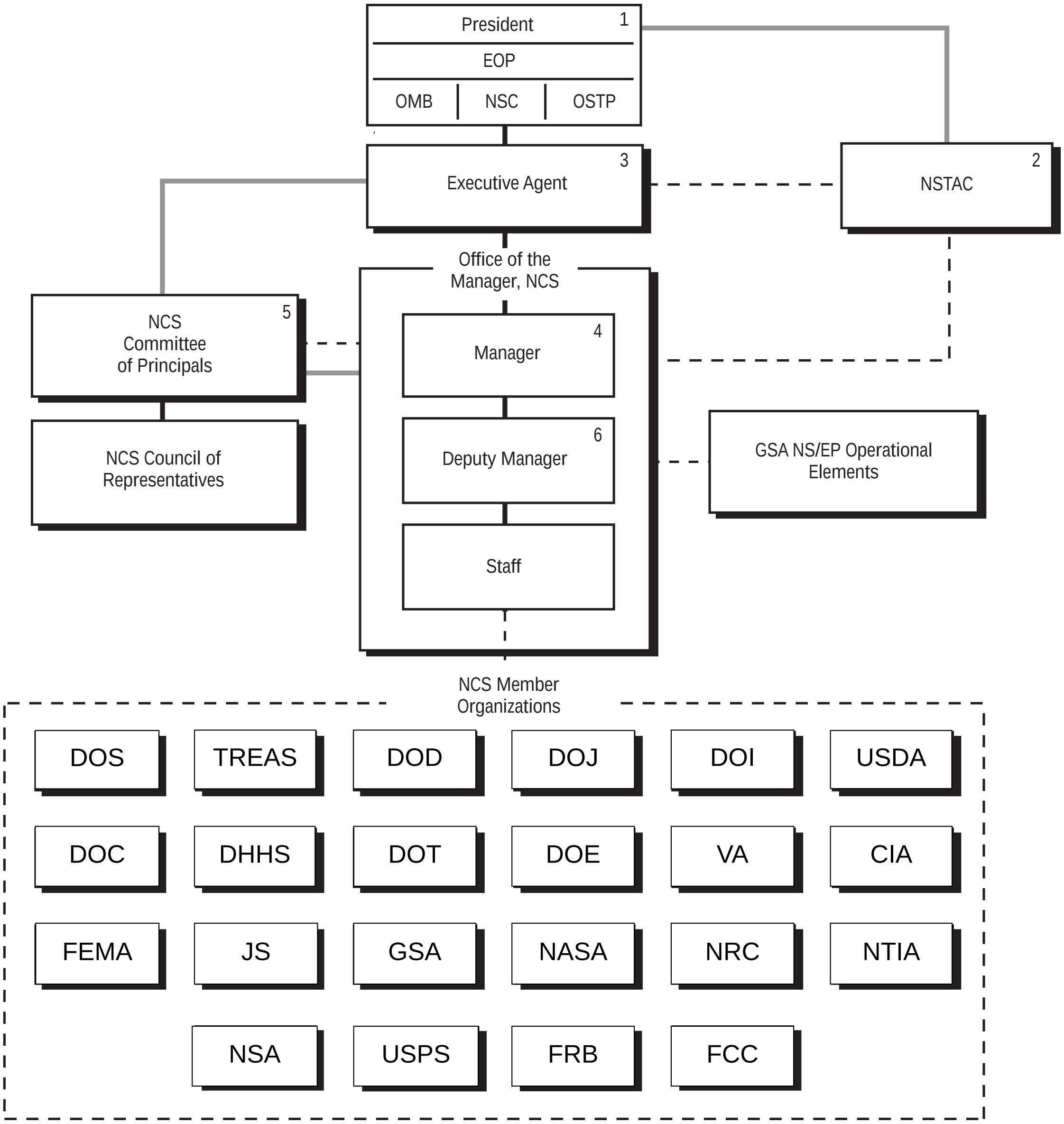
United States
Postal Service
(USPS)
Mr. Timothy J. Patterson

Federal Reserve Board
(FRB)
Ms. Anne E. Paulin



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
6. First line management position that is exclusively NCS

LEGEND

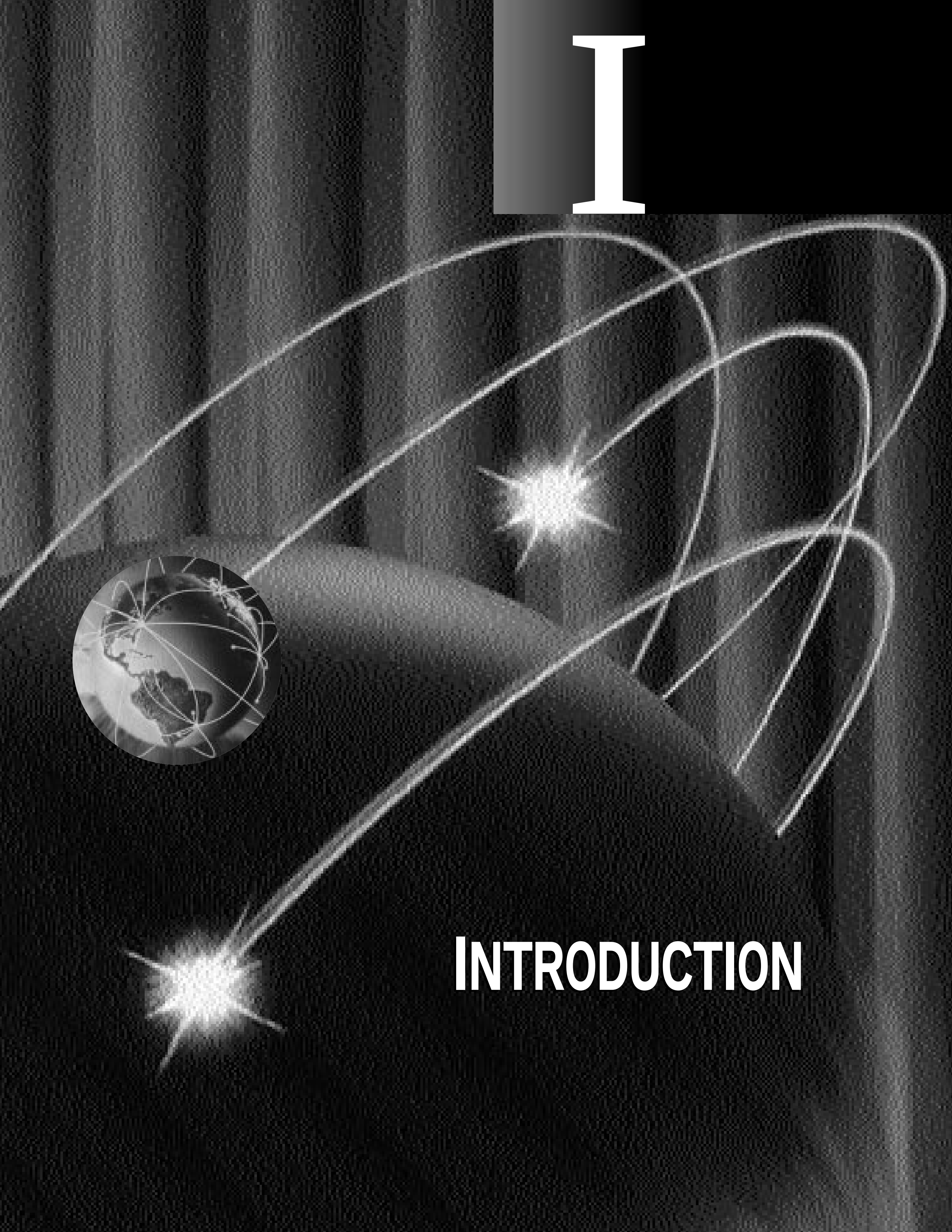
Direction ▬▬▬
Coordination – – –
Advice ▬▬▬

TABLE OF CONTENTS

LIST OF EXHIBITS

Page Number

I



INTRODUCTION

I

INTRODUCTION

The Office of the Manager, National Communications System (OMNCS), in coordination with the National Communications System (NCS) Committee of Principals (COP), publishes the *FY 2000 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 fiscal year (FY) 2000.

BACKGROUND

On August 21, 1963, President John F. Kennedy signed a Presidential Memorandum ordering the formation of the NCS in the wake of communications shortfalls in support of 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 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 service providers in the industry complicated the means for satisfying NS/EP telecommunications requirements. In anticipation of the loss of 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-related companies, the 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. 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 the 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 was its mandate to serve as a focal point for industry/Government NS/EP telecommunications planning. Although the NCS COP served as the mechanism for Federal interagency coordination, the NSTAC and its working group structure became the means for the NCS to work with industry to address the range of NS/EP telecommunications issues.

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 over 35 years, the NCS will continue 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.

ENVIRONMENT FACING THE NCS

LEGAL AND POLICY ENVIRONMENT

Critical infrastructure protection (CIP) continues to be a priority concern among policymakers in the Administration and Congress. In October of 1997, the President's Commission on Critical Infrastructure Protection issued its landmark report calling for a nationwide effort to protect America's infrastructures. Seven months later, President Clinton issued Presidential Decision Directive 63 (PDD-63): *Protecting America's Critical Infrastructures,* to establish a structure for CIP initiatives and policy. In January 2000, the White House published the first version of the *National Plan for Information Systems Protection*. This preliminary version focuses largely on Federal efforts undertaken to protect the Nation's critical, cyber-based infrastructures. The second version will include physical threats to the infrastructure and private sector input on how to implement a national strategy for infrastructure assurance as envisioned by PDD-63.

Congress also directly acknowledged a need for action to protect the Nation's critical infrastructures. On March 15, 2000, the House issued Concurrent Resolution 285, 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."

Shortly thereafter, the Senate established a *Critical Infrastructure Protection Working Group.* A myriad of Congressional committees and subcommittees are examining key aspects of CIP, such as removing barriers to information sharing between industry and Government for the purposes of cyber security.

Although it laid the groundwork through policy directives and legislative proposals, the Government recognizes that a partnership with industry—the owners and operators of the Nation's critical infrastructures—will be the cornerstone of meaningful CIP efforts. Toward that end, the Administration designated lead agencies in each of the recognized critical infrastructures to work with private sector leaders and organizations in pursuit of a national strategy. Moreover, the Government encouraged the private sector to establish Information Sharing and Analysis Centers (ISAC) to facilitate information sharing among industry, and eventually between industry and Government, on infrastructure vulnerabilities, threats, intrusions, and anomalies.

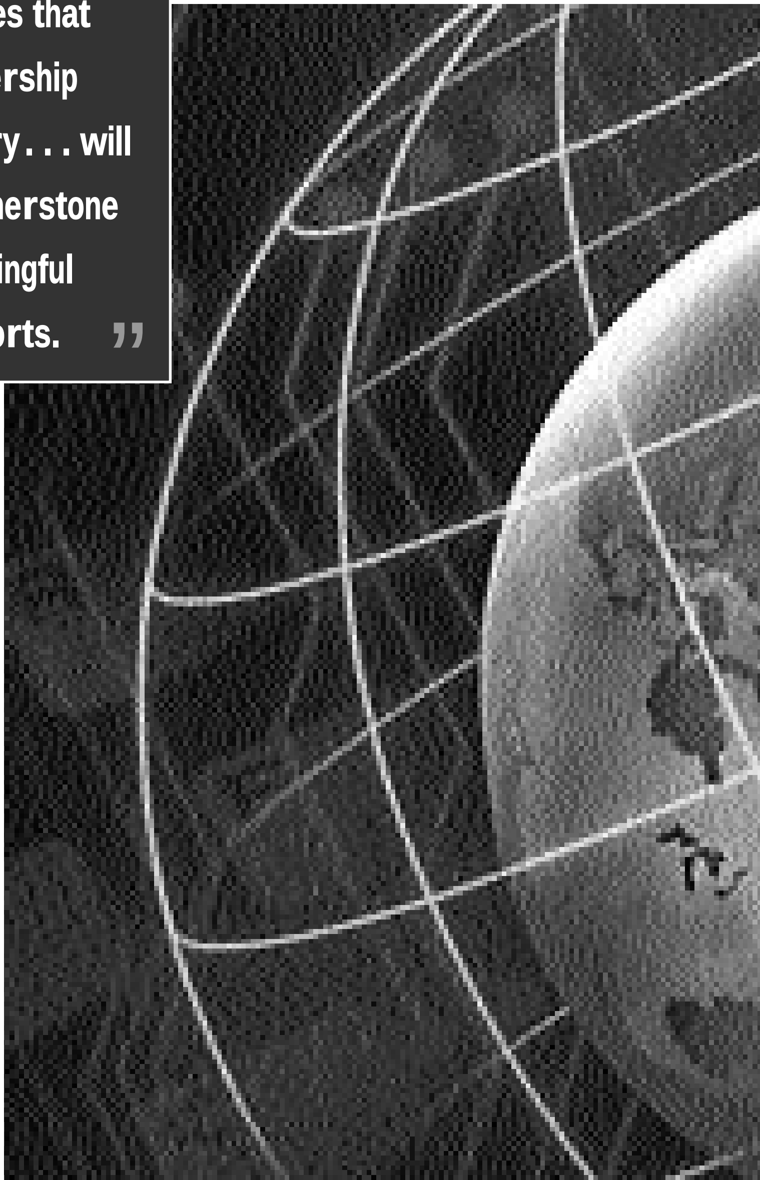
> "... the Government recognizes that a partnership with industry... will be the cornerstone of meaningful CIP efforts."

The NCS continues to leverage its NS/EP mission, broad interagency membership, and historic relationship with industry to take a leadership role in this area. In March 2000, the telecommunications sector designated the NCS's National Coordinating Center for Telecommunications (NCC) as an ISAC—one of the first ISACs to be established and the first to encompass both industry and Government participation. The NCS will continue to draw on its longtime experience as a partner with industry to forge new relationships in addressing CIP.

OPERATIONAL ENVIRONMENT

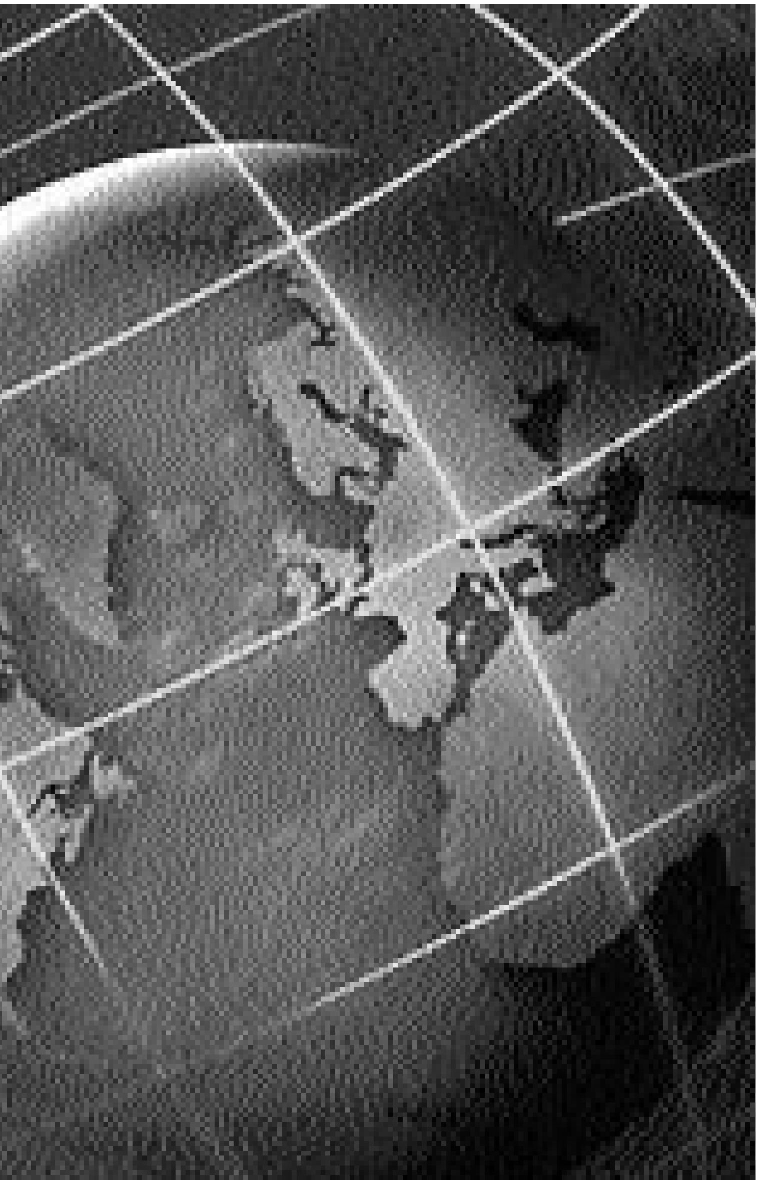
In the middle of FY 2000, two events demonstrated to the Nation how profoundly cyber attacks could affect users worldwide. In February 2000, a series of Distributed Denial of Service (DDoS) attacks occurred within a span of 44 hours. These massive DDoS attacks crippled or shut down several popular Web sites. At the time of the attacks, electronic commerce accounted for $20 billion in the retail market. That figure is predicted to reach $185 billion by 2004, with business-to-business transactions totaling $2.7 trillion. In an economic environment so heavily dependent on the Internet, the February DDoS attacks made network security a highly visible national issue.

The second event, coming only 3 months later, reemphasized the danger of such attacks. The "I LOVE YOU" virus originated in the Philippines on May 4, 2000, and propagated worldwide as



businesses and Government began their work day. By 6:00 p.m. that day, Carnegie Mellon's Computer Emergency Response Team (CERT) Coordination Center had received more than 400 direct reports involving more than 420,000 Internet hosts. Although the damage from such events cannot be calculated precisely, the CERT Coordination Center estimated that damage ranged from $100 million to $10 billion globally.

These events demonstrated how rapidly cyber attacks can propagate throughout the highly interconnected and interdependent infrastructure on which both industry and Government depend. Sophisticated, user-friendly hacking tools that are widely available on the Internet facilitated these attacks, reducing the skills and knowledge required to launch global cyber attacks. While these attacks were destructive, they also increased awareness throughout industry and Government organizations of the need to secure networks. Today industry and Government are more alert, better prepared, and more responsive to subsequent attacks, significantly diminishing their vulnerability to attack.



Hopefully, the heightened awareness of the cyber threat will lead to more industry/Government coordination to protect the networks and systems composing the critical infrastructures on which our Nation depends. 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, more recently, the NCC-ISAC for telecommunications.

TECHNOLOGICAL ENVIRONMENT

The explosive global growth of Internet Protocol (IP)-based networks, coupled with the expanding deployment of bandwidth enhancing technologies, is redefining the landscape for communications capabilities and services. During FY 2000, telecommunications service providers increased investments in data networking equipment, such as IP gateways and servers, that will promote the convergence of traditional circuit-switched networks and newer packet-switched networks. Furthermore, a variety of companies, including AT&T, Sprint, Level 3 Communications, and Qwest Communications, continued to deploy IP-based networks. This shift in focus indicates a general movement away from traditional public switched network technology and toward next generation networks.

Although the evolution of the telecommunications infrastructure toward a diverse, broadband, packet-based network promises enhanced services, it also presents challenges in meeting NS/EP requirements. For example, over today's circuit-switched network, the NCS administers the Government Emergency Telecommunications Service to satisfy NS/EP functional requirements, such as enhanced priority treatment of calls and nationwide coverage. Similarly, the Telecommunications Service Priority Program satisfies NS/EP requirements, such as priority treatment for the provisioning and restoration of circuit-switched services. As the telecommunications infrastructure evolves toward the next generation network, additional packet network-based NS/EP capabilities may be needed to continue fulfillment of NS/EP requirements.

The NCS is already working to ensure that the national telecommunications infrastructure remains responsive to the NS/EP community's requirements in the new technological environment. Anticipating the impact of packet-switched networks and the Internet on NS/EP operations, the OMNCS established a program office to examine and plan for network convergence. Concurrently, the interagency NCS Council of Representatives formed an implementation team to assist with those issues. Lastly, the OMNCS is participating actively in standards organizations to ensure that NS/EP priority, security, and reliability requirements are considered for the next generation network.

REPORT ORGANIZATION

The subsequent sections of this report detail the NCS's FY 2000 activities and accomplishments undertaken to fulfill its mission. Section II describes the emergency response activities of the OMNCS. Section III contains information about the OMNCS's information assurance activities and Y2K activities, plus a description of OMNCS NS/EP telecommunications support, activities, programs, and major interagency initiatives. Finally, Section IV reviews the NS/EP telecommunications support and activities of the NCS member organizations.

The *FY 2000 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.

II

EMERGENCY RESPONSE ACTIVITIES

II

EMERGENCY RESPONSE ACTIVITIES

DISASTER RESPONSE— HURRICANE FLOYD

The National Communications System's (NCS) National Coordinating Center for Telecommunications (NCC) ensures that Federal, State, and local responders receive national security and emergency preparedness (NS/EP) communications support during Presidentially declared disasters. The NCS also supports disaster relief efforts by training key personnel and providing telecommunications resources. During fiscal year (FY) 2000, the NCS focused its support efforts on programs, exercises, and training to improve future disaster recovery response.

The NCS provided communications support to disaster relief efforts in the aftermath of Hurricane Floyd during FY 2000. In addition, the NCS deployed three Individual Mobilization Augmentees (IMA) to assist NCS Regional Managers serving as Federal Emergency Communications Coordinators (FECC).

YEAR 2000 (Y2K) TRANSITION SUPPORT

The NCC performed an essential role in ensuring continued NS/EP telecommunications services during the Y2K transition. By employing a successful information-sharing and coordination strategy among telecommunications industry and Government operations centers domestically and abroad, the NCC served as an essential information gathering and analysis center. The Web-based database used to support NCC Y2K operations registered more than 96,000 hits during the New Year rollover period and almost 12,000 hits during the Leap Year rollover period. Major users of the system included SBC, Telecom Italia, Telekom Malaysia Berhad, Bell Atlantic, Sprint, Belgacom, Portugal Telecom, Saudi Telecom, and GTE.

During the Y2K rollover, the NCC served as a focal point for information sharing and response among the telecommunications industry and Government. The NCC integrated the efforts of the Y2K Telco Forum, Canadian Telecommunications Industry Forum, International Telecommunication Union (ITU), Federal Communications Commission (FCC), General Services Administration (GSA), Defense Information Systems Agency, and all the divisions of the NCS throughout the year for preparation, coordination, and activation of the NCC Operations Center for Y2K activities.

Using its Y2K information sharing system and database, the NCC provided a mechanism for real-time information exchange. During the Y2K rollover period, 82 companies in 41 countries reported the status of their networks at a minimum of 10 scheduled intervals during each 24-hour period. The NCC established specific criteria that companies needed to meet to participate in the Y2K information sharing system.

The Office of the Manager, National Communications System (OMNCS) designed the system to meet the needs of a diverse group with varying requirements. The OMNCS also partitioned participants into domestic and international sharing groups and granted different levels of database privileges. In addition to industry participants, Government agencies (i.e., GSA, FCC, Department of State, and Department of Defense) participated in the Y2K information sharing system. Based on information received, the NCC posted reports every 4 hours on the status of networks domestically and internationally.

Y2K TRAINING

Prior to the Y2K transition, the OMNCS developed the NCC Y2K Database to aid in collecting and disseminating information on Y2K-related issues as they surfaced in the telecommunications infrastructure. The Operations Division conducted a series of training events to familiarize a cadre of users with the function of the database and its associated suite of analysis tools. Training participants included telecommunications industry representatives, NCC Emergency Operations Team (EOT) members, FCC staff, and ITU members responsible for Y2K preparedness operations.

Emergency Readiness Team personnel at the National Coordinating Center for Telecommunications monitor incoming Y2K information during Y2K operations last December. (Photo by Robert Flores.)

TELECOMMUNICATIONS EMERGENCY RESPONSE TRAINING

The Emergency Response Training (ERT) seminars are a highly visible and successful training program for the NCS. These seminars are 2-day events designed to provide industry, Federal, regional, State, and local personnel with the background and information required to successfully respond to a crisis. During Phase III of the ERT Program, 275 attendees participated in four sessions. Six more seminars will be held during Phase III.

Since the training program started in 1993, more than 1,800 attendees have participated in 27 sessions. This program continues to earn recognition for improving the emergency support function (ESF) #2 response and recovery structure. During FY 2000, seminars occurred in:

- Atlanta, Georgia (Federal Region IV)
- Oakland, California (Federal Region IX)
- Irving, Texas (Federal Region VI)
- San Juan, Puerto Rico (Federal Region II).

NCS REGIONAL MANAGERS CONFERENCE

The Operations Division, with support from GSA, held a Regional Managers Conference for the Regional Emergency Communications Planners and the NCS IMAs in January 2000. Conference participants received detailed information about the evolving roles and responsibilities related to disaster planning and response operations in the 10 Federal Regions. The conference fulfilled the following objectives:

- Provided a forum for presenting NCS programs supporting the Federal Regions
- Established new goals and objectives for the expanding NCS regional role
- Identified regional support requirements
- Ensured participants understood ESF #2 roles and expectations
- Prepared regionally assigned drilling NCS IMAs for their responsibilities during emergency response as assistants to the FECC.

The conference was highly interactive, generating discussion among the Regional Managers and NCS IMAs on areas of common interest. Participants generated findings and recommendations for future actions supporting and enhancing NCS mission readiness in areas of planning, staffing, training, and exercise support.

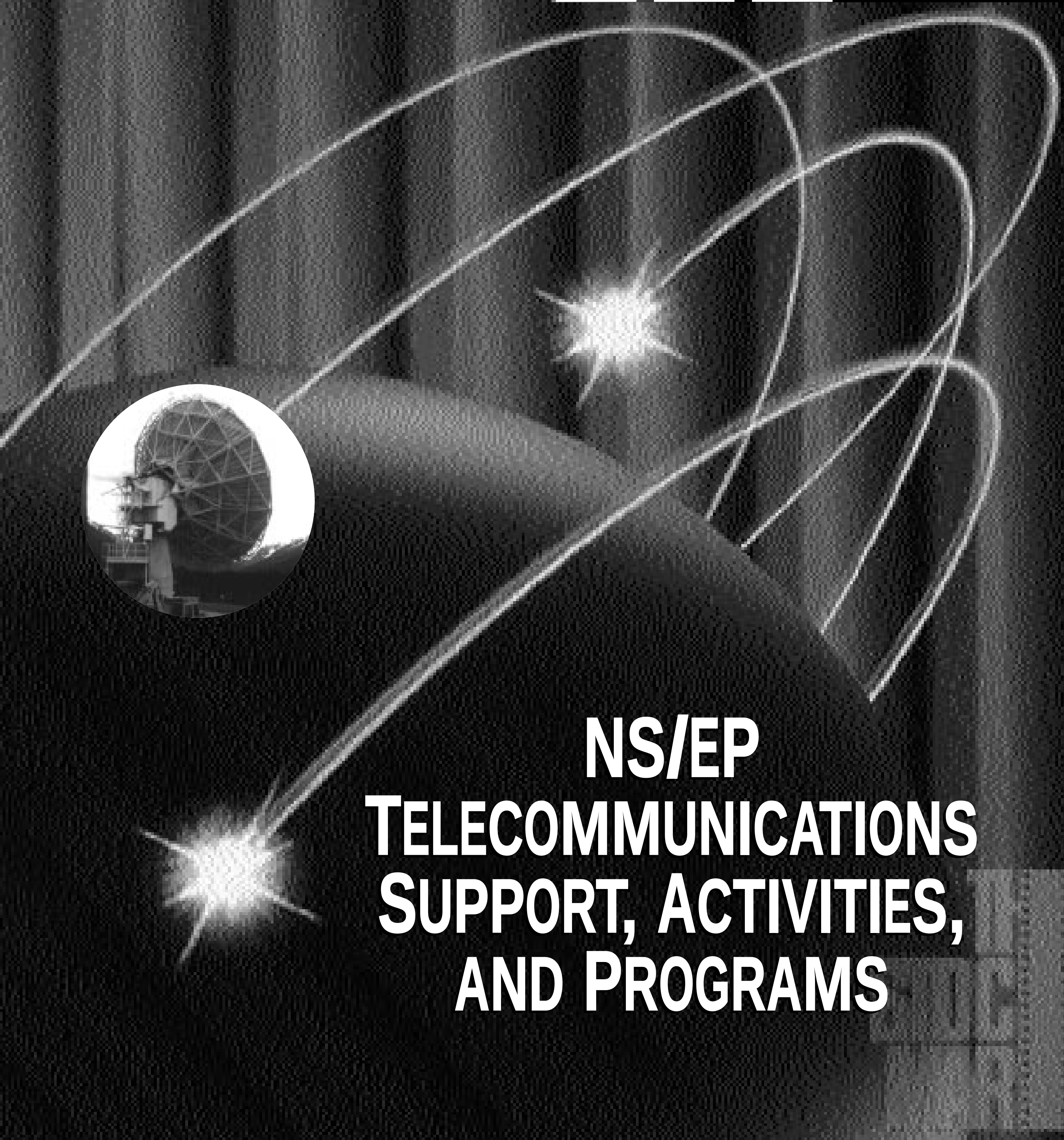
NCS CONTINUITY OF OPERATIONS RELOCATION EVENT

To ensure operational readiness in support of the OMNCS NS/EP mission, NCC EOT and telecommunications industry personnel participated in a 3-day exercise at the OMNCS relocation facility. Through scenario-based activities, participants examined roles and responsibilities, validated operational processes and procedures, and reviewed external coordination and collaboration requirements. In conjunction with this event, the Operations Division supported the Office of Science and Technology Policy in a related training activity that focused on addressing national-level telecommunications issues.

EXERCISE TOPOFF

The Operations Division helped plan and conduct the Department of Justice/Federal Emergency Management Agency-sponsored event. The no-notice counterterrorism exercise took place in several U.S. locations and involved top Government officials.

III



NS/EP Telecommunications Support, Activities, and Programs

III

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) 2000. The two introductory portions of this section, OMNCS Critical Infrastructure Protection (CIP) Activities and OMNCS Year 2000 (Y2K) Preparedness Activities, highlight two significant issues the OMNCS addressed during FY 2000. The remainder of the section presents further details of OMNCS program-specific activities.

OMNCS CRITICAL INFRASTRUCTURE PROTECTION ACTIVITIES

The OMNCS CIP activities support the mission assigned by Executive Order (E.O.) 12472 and the national CIP goals of industry and Government. The OMNCS began FY 2000 with a strategic emphasis on fulfilling its CIP mission by improving its focus on CIP issues, consolidating CIP resources, and creating a strong CIP presence at the National Coordinating Center for Telecommunications (NCC). This approach has enabled OMNCS to leverage its Customer Service, Technology and Programs, and Operations Divisions to take full advantage of their respective areas of management and technical expertise in addressing CIP issues. The following paragraphs discuss the roles of each of these divisions.

The Customer Service Division supports the Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), one with Government members and one with primarily industry members. The NSIEs address technical issues affecting the security of the public network (PN) by sharing information about the unauthorized penetration or manipulation of the PN software and databases affecting NS/EP telecommunications services. NSTAC and Government NSIE representatives exchange ideas on technologies and techniques for addressing threats and vulnerabilities, with an emphasis on identifying causes of intrusions and measures to protect the PN in the longer term. The NSIEs have provided valuable input to the OMNCS's CIP efforts.

The Customer Service Division also annually produces a report, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document*. Historically, this report has focused primarily on the traditional telecommunications infrastructure. Given the growing importance of the Internet and its potential for supporting NS/EP operations, the FY 2000 report examined the electronic intrusion threat to the Internet. The final report is scheduled for publication in early FY 2001.

For several years, this report has provided an essential component for risk assessments and countermeasure development. Based exclusively on open source material, the report describes the techniques involved in computer intrusion and telecommunications and information systems targeting, discusses the motives of those actors who pursue such activities, and identifies adversaries who could use electronic intrusion to attack the PN and interconnected telecommunications and information systems. This report not only has served as a reference for OMNCS's CIP work, but also has been shared throughout the NS/EP community to increase overall awareness of the electronic intrusion threat.

The Technology and Programs Division helps to ensure that OMNCS has the mechanisms and tools to fulfill its mission. In the CIP arena, this division has focused on defining the concept and functions of an Information Sharing and Analysis Center (ISAC) for telecommunications in the NCC and on developing the Information Sharing Analysis System (ISAS), the systems and tools to support the NCC-ISAC's information collection and analysis functions.

In March 2000, the ISAS achieved initial operational capability (IOC), followed by implementation of an upgraded interim system in July 2000. The interim ISAS is an adaptation of the NCC Y2K database, developed to facilitate industry and Government information sharing on Y2K events throughout the NS/EP telecommunications community. Building on the lessons learned from the NCC Y2K database and the interim ISAS, the Technology and Programs Division will derive functional requirements for more advanced automation, analysis, modeling, data fusion, and correlation processes to support sharing of information regarding all hazards that could adversely affect the telecommunications infrastructure.

The Operations Division serves as the operations focal point for the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications and facilities. The NCC-ISAC carries out the division's role in the OMNCS's CIP activities. NCC membership provides a basis for initial NCC-ISAC membership, which is evolving to reflect a broader base of technologies composing the telecommunications infrastructure. The NCC-ISAC gathers information about vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, Government, and other sources. The NCC-ISAC then analyzes the data with the goal of averting or mitigating effects on the telecommunications infrastructure. Results are sanitized to remove proprietary and classified information and then disseminated in accordance with sharing agreements established by the NCC-ISAC participants.

In contrast with the NSIEs, which focus on the software and databases that support NS/EP telecommunications, the NCC-ISAC's mission encompasses all hazards with the potential to affect the telecommunications sector. The NSIEs focus primarily on sharing information in the longer term, with the objective of improving the overall level and security in the PN. The NCC-ISAC emphasizes collecting, sharing, and responding to information on a near real-time basis to identify potential attacks on the telecommunications infrastructure. This effort is achieved by analyzing reported events and symptoms as rapidly as possible to avert or minimize damage to telecommunications operations, with prevention as a secondary goal. The respective missions and emphases of the NSIEs and the NCC-ISAC complement one another to provide a full range of responses to the vulnerabilities and threats to the Nation's telecommunications infrastructure.

In early May, the NCC-ISAC demonstrated its ability to provide timely and meaningful dissemination of information regarding the telecommunications infrastructure by its response to the ILOVEYOU virus. This hybrid virus and worm originated in the Philippines and propagated worldwide as businesses and Government agencies began their work day on May 4, 2000. With the cooperation of NCC-ISAC members and NSIE representatives, the NCC-ISAC received information about the worm in time to provide a first alert to some Government agencies and telecommunications service providers. This alert allowed these organizations and agencies to respond to the event proactively, resulting in minimal impact. The NCC-ISAC's dissemination of information regarding the ILOVEYOU virus proved effective and yielded some lessons learned that could help refine NCC-ISAC procedures in response to future cyber incidents.

> "The NCC-ISAC's dissemination of information regarding the ILOVEYOU virus proved effective and yielded some lessons learned. . ."

Working together, OMNCS's Customer Service, Technology and Programs, and Operations Divisions are well positioned to identify emerging policy issues and make strategic and operational adaptations to address CIP concerns affecting the telecommunications infrastructure on which the NS/EP community depends.

OMNCS Y2K PREPAREDNESS ACTIVITIES

Before FY 2000, the OMNCS had engaged in planning and support activities in preparation for the millennium transition. During FY 1998 and FY 1999, the OMNCS became increasingly involved in high-visibility Y2K events and activities. In February 1999, the U.S. telecommunications industry Y2K Telco Forum recommended that the OMNCS lead an effort to create a database for communicating Y2K-related awareness information to critical users.

As a result, the OMNCS began developing a database during FY 1999 that provided an early response mechanism for the telecommunications community, domestically and abroad. Moreover, the OMNCS and the NCC first published an industry/Government Y2K Operations Plan on May 19, 1999, and continued to expand and update the document throughout the year.

The OMNCS used September 9, 1999, as an opportunity to exercise its preparation for the critical Y2K rollover date. Because programmers had used "9999" as an end-of-file command for a number of programs, there was a concern that some programs would misinterpret the "9/9/99" date as this end-of-file command. The NCC activated its Emergency Operations Team (EOT) for September 8-9, 1999. While concerns over "9999" proved to be unfounded, this activation allowed a dress rehearsal for industry and Government participants before the most critical date, January 1, 2000.

During the Y2K rollover, the NCC served as a focal point for information sharing and response among the telecommunications industry and Government. The NCC incorporated requirements of the Y2K Telco Forum, Canadian Telecommunications Industry Forum, International Telecommunication Union, Federal Communications Commission (FCC), General Services Administration (GSA), Defense Information Systems Agency (DISA), and all the divisions of the NCS throughout the year for preparation, coordination, and activation of the NCC Operations Center for Y2K rollover activities.

Using its Y2K information sharing system and database, the NCC was able to provide a mechanism for real-time information exchange. The Web-based database used to support NCC Y2K operations registered more than 96,000 hits during the New Year rollover period and almost 12,000 hits during the Leap Year rollover period (February 29, 2000). During the two rollover periods, 82 companies in 41 countries reported the status of their networks at a minimum of 10 scheduled intervals during each 24-hour period. The NCC established specific criteria that companies needed to meet to participate in the Y2K system.

The OMNCS designed the system to meet the needs of a diverse group with varying requirements. The OMNCS also partitioned participants into domestic and international sharing groups and granted different levels of database privileges. In addition to industry participants, Government agencies (e.g., GSA, FCC) participated in the Y2K system. Based on information received, the NCC posted reports every 4 hours on the status of national and international networks to the Information Coordination Center (ICC). Overall, the Y2K database proved so useful that the NCC-ISAC developers based the ISAS database architecture on that of the Y2K database.

Most importantly, the existing relationship between industry and Government within the NCC contributed to the success of the Y2K coordination effort. The following additional factors associated with Y2K information sharing played a critical role in the success of NCC Y2K efforts:

- A universally recognized threat,
- A fixed deadline for mitigating the risk and preparing contingencies,
- Highly visible and focused Government leadership,
- Compelling business and political reasons for industry participation,
- Legislation to protect information and the identity of the provider of the information,
- Government-funded centers to support the process,
- Documented information sharing agreements among all industry and Government participants, and
- An understanding that the process had a finite life span and that the data would then be deleted.

In addition to its central role in maintaining the telecommunications Y2K database, the NCS Operations Division worked to ensure that its NS/EP telecommunications programs, including Y2K database training, the Shared Resources High Frequency Radio (SHARES) Program, and the Telecommunications Service Priority (TSP) Program assisted in completing a successful transition to Y2K. The Division conducted a series of training events to familiarize the Y2K database users with the functions of the database. Additionally, the SHARES Program prepared to provide a backup means of communications using high-frequency (HF) radios. The SHARES program ultimately was not needed during the rollover. Moreover, the number of requests for TSP restoration assignments increased 30 percent as organizations prepared for the Y2K transition. The TSP Program serves as the regulatory, administrative, and operational framework for the priority provisioning and restoration of NS/EP telecommunications service.

The OMNCS also focused on enhancing the National Telecommunications Coordinating Network (NTCN). NTCN ensured that coordinated communications would be available among telecommunications carriers, Federal departments and agencies, and equipment manufacturers during periods of potential outage. The NTCN was activated but not utilized during the Y2K rollover.

Furthermore, the Government Emergency Telecommunications Service (GETS) Program provides nationwide voice band service for authorized Government users engaged in NS/EP missions. Federal, State, and local government officials, as well as Government-sponsored industry personnel, received GETS personal identification numbers (PIN) prior to the rollover period in anticipation of network congestion during the rollover.

The OMNCS's overall response to the Y2K problem reflected the ongoing capability of industry and Government to prepare for and respond to NS/EP telecommunications challenges. Y2K also provided the OMNCS with an opportunity to test mechanisms for sharing information among the telecommunications sector in real-time. The experiences and lessons learned will help shape the development of the NCC as it becomes fully operational as an ISAC for telecommunications. The systems developed and the enhancements made to existing NCC resources for Y2K are being adapted to fulfill the ISAC function. The trust built between industry and Government throughout the history of the NCC and further developed in preparation for Y2K sets the foundation for building trust among ISAC participants to facilitate information sharing.

> "The systems developed and the enhancements made to existing NCC resources for Y2K are being adapted to fulfill the ISAC function."

TECHNOLOGY AND PROGRAMS

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. In fulfilling 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 in the standards and recommendations are developed.

The following paragraphs highlight the major projects undertaken by the Technology and Programs Division during FY 2000. For information regarding the division's CIP activities, see the CIP portion of this section.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

BACKGROUND

The OMNCS established GETS to meet White House requirements for a survivable, interoperable, nationwide voiceband service for authorized Government users engaged in

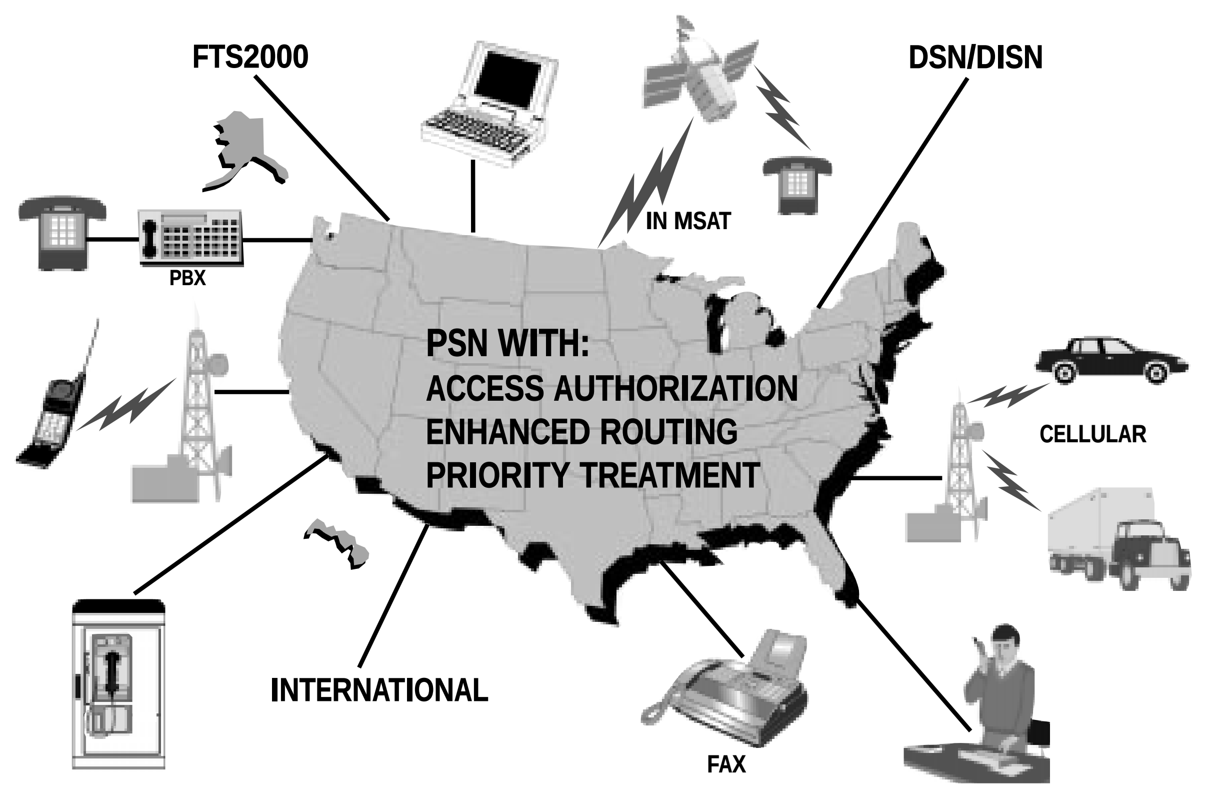
NS/EP missions. GETS satisfies these requirements by providing emergency access and specialized processing in local and long distance telephone networks. GETS ensures users of a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters.

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient, reliable technology for supporting a service that would meet NS/EP mission requirements. The use of the PSN leverages its 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 95 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 and then incrementally improve the service with specialized calling features. The strategy of developing GETS by using the existing assets of the PSN enabled early implementation and provided for technical currency by leveraging the continual improvements made by industry. Using 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, WorldCom, and Sprint, the three largest IXCs. As a result, these carriers are the only IXCs capable of authorizing and processing GETS

Exhibit 3-1 GETS Operational Concept



calls. Therefore, it is critical that access to these carriers be available at all PSN end offices and mobile switching centers (MSC). Each of these IXCs began with the same basic set of functional requirements. However, as a result of the implementation approach pursued by each IXC and the inherent differences in the structure of the IXCs' respective networks, the operational features and capabilities differ slightly among the providers.

Today, the primary focus of feature implementation has shifted to the local exchange carrier (LEC) networks. DynCorp (formerly GTE Government Systems Division) received a separate integration contract (IC) for integration of 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, 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 entered into contracts with LECs for the deployment and operation of these features. During FY 2000, deployment of features continued in several LECs on Nortel, Lucent, AGCS, and Electronisches Wahl System Digital switches.

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 by the switch vendors that leverage recently completed LEC feature development, the GETS Program is investigating enhancements that would help GETS calls terminate from the PSN to customer premises (e.g., private branch exchanges [PBX]). The GETS Program also continues to monitor the potential impact of opportunities offered by evolving network technologies, such as industry's recent movement toward offering voice service as a packet-based service.

OPERATION AND FEATURES

Access to GETS is quick and simple. Users access GETS by dialing a universal access number (1-710-NCS-GETS) using common telephone equipment, such as a standard desk set, secure telephone (e.g., Secure Telephone Unit-Third Generation [STU-III]), facsimile, modem, or cellular telephone. Telephones on the Federal Telecommunications System (FTS) 2001 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 PIN and the destination telephone number. Even if the access control system fails, a "fail open" feature will allow authorized users to complete their GETS calls. The OMNCS can deactivate PINs as a result of fraud or abuse.

PRIORITY TREATMENT AVAILABILITY

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS is working to ensure that 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 that provides a classmark for NS/EP-related signaling messages and a high-priority level for those messages within the SS7 message priority scheme. This standard was reaffirmed 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 improves the likelihood that GETS calls would continue to be processed if congestion were to occur within the SS7 networks.

In 1996, ANSI modified the SS7 standards so that NS/EP traffic would not share the higher priority level with plain old telephone service (POTS) traffic. The GETS Program worked closely with the Network Interconnection and Interoperability Forum (NIIF) to facilitate industry migration to the 1996 standard related to SS7 message priority. GETS representatives worked with NIIF members to build consensus on a migration plan and schedule and won adoption of a resolution codifying the plan.

> **"The GETS Program Office is working with industry to ensure consistent toll-free treatment for service users at privately owned user-to-network access devices."**

In December 1997, NIIF introduced Issue No. 0095, *Implementing POTS IAM Priority Level 0*. Based on the resolution, plans have been received from all members, providing specific dates by which they will comply with the standard. NIIF members are expected to transition noncompliant switches by January 2001. The switches that either comply or will soon have the capability to comply with the standard will serve more than 90 percent of the access lines in the Nation.

INTEROPERABILITY

Many of the significant challenges currently facing GETS involve interoperation with other networks and service providers. The GETS Program Office is working with industry to ensure consistent toll-free treatment for service users at privately owned user-to-network access devices. The GETS Program Office also is working in concert with the GSA to enable Government users to maintain GETS access during the transition from FTS2000 to FTS2001.

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 within the industry. 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. Testing has shown these problems to be particularly prevalent for coin telephones owned and operated by small businesses and PBXs operated by the hospitality industry (e.g., 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 FCC to issue guidance to industry regarding publicizing the 710 NPA to give it stature as an emergency toll-free service per sections 228(c) and 276(b) of the Communications Act.

Based on 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/personal communications services [PCS] networks, PBXs, and payphones) of the need to ensure that 710 calls are not blocked by their equipment. Also, Telcordia (formerly known as Bellcore) modified the Local Exchange Routing Guide (LERG) 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.

The GETS Program Office maintains a partnership with GSA, Sprint, and WorldCom to ensure that the interoperability established between GETS and FTS2000 is maintained during the transition to FTS2001. The GETS Program office fully established interoperation with Sprint FTS2001. Working together, the GETS Program Office, GSA, and WorldCom identified the source of interoperability problems experienced by some WorldCom FTS2001 users and developed a solution in the WorldCom laboratories that is expected to be deployed technology by August 2000.

SUCCESSES

In addition to being used to overcome network congestion and damage associated with natural disasters, GETS played a significant role in Y2K readiness preparations. Federal, State, and local government personnel, as well as Government-sponsored industry personnel supporting Y2K received 10,000 GETS PINs. This represented a 33 percent increase in the number of GETS PIN holders. The GETS Program was successful in identifying appropriate personnel and processing PIN requests over a period of fewer than 3 months, from October to December.

In the past year, the GETS Program made significant progress in its outreach efforts to State and local user groups. The number of State and local agencies (including the American Red Cross) with GETS accounts rose from 177 to 411 in 48 states, the District of Columbia, Puerto Rico, and the Virgin Islands. State and local users now account for 5,364 of the more than 42,387 distributed GETS PINs.

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 the impact of IP network–PSN convergence on current NS/EP services (e.g., GETS and TSP). 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 and the International Telecommunication Union (ITU), to increase awareness of NS/EP requirements, including methods of obtaining priority services over the Internet.

PRIORITY ACCESS SERVICE

NSTAC identified the need for a wireless priority service and recommended to President Clinton that a service be established for NS/EP users. This recommendation provided a basis for the recent FCC Report and Order No. 00-242, which allows commercial mobile radio service to offer Priority Access Service (PAS) to public safety personnel at Federal, State, and local levels to meet the NS/EP needs of the Nation. Timely emergency telecommunications for Federal, State, and local responders at a disaster site can be critical for natural disasters and incidents that threaten national security.

NS/EP use of wireless technology during such incidents has significant advantages. However, increased personal use of wireless communications often creates network congestion and high levels of call blocking precisely when disaster relief officials most need mobile communications. As a result, the OMNCS, working with industry leaders, industry associations, State representatives, and standards bodies, developed the PAS Program 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 FCC, on July 13, 2000, announced a Report and Order on wireless priority access. The Report and Order, which will be effective on October 10, 2000, adopted the wireless, 5-level priority access scheme proposed by the OMNCS and offers Federal liability relief for NS/EP priority service providers.

The OMNCS is working with the FCC to address the regulatory issues associated with implementation of a priority access service. In the interim, the OMNCS completed several studies investigating the technical aspects of PAS implementation.

FEDERAL WIRELESS USERS FORUM

The Federal Wireless Users Forum (FWUF) provides an opportunity for current and future Government users of wireless services to obtain information on various types of services. The OMNCS facilitates the FWUF, focusing on technical issues and policies having implications for NS/EP telecommunications.

PERSONAL COMMUNICATIONS SERVICES

The OMNCS's efforts in personal communications services focus on standardizing the Stage 2 service description for Priority Access and Channel Allocation-Enhanced (PACA-E) service. The Stage 2 description depicts the network architecture and message flows needed to implement the PACA-E service and describes how various network entities interact to provide service. This Stage 2 document is defining a new feature PACA-E egress, which describes how to queue a call attempt on the egress side of the network. When the document is finished, service providers can use it to implement queuing on the egress side of their networks.

The OMNCS actively participates in joint projects with the Telecommunications Industry Association committee standards formulation groups concerning Enhanced Wireless Emergency Services. When developed, these standards will include location services and congestion control.

ADVANCED TECHNOLOGY GROUP

The NCS Advanced Technology Group (ATG) investigates new and emerging technologies that may prove beneficial to NS/EP users in the future. Over the past year, the ATG researched a range of topics, from orbiting satellites to handheld wireless networks. These technologies have the potential to revolutionize the way that NS/EP responders communicate during periods of NS/EP need.

SATELLITE NETWORKS

Satellite and stratospheric telecommunications systems offer the potential for alternate routing of NS/EP calls during instances of damage or stress in the PSN. The NCS is continually investigating the utility of purchasing voice and data services from nonterrestrial service providers.

Digital Broadcast Satellites

The NCS recently published a technical note (Technical Note, volume 7, number 2, July 2000; “Direct Broadcast Satellite Radio”) on direct broadcast satellite radio, also known as DBS Radio. DBS Radio will use a series of geostationary satellites to beam nationwide radio programming to the contiguous United States. Two factors — the willingness of commercial broadcasters to deliver this feature and future actions by the FCC — will determine the potential use of DBS Radio for nationwide emergency broadcast messages.

Satellite Cellular Systems

The NCS followed recent developments in the low-Earth orbit (LEO) satellite systems marketplace with great interest. These systems appeared to offer potential benefits to the NS/EP community for alternate telecommunications routing. However, the suspension of commercial service on the Iridium system highlights the risk of buying services in an emerging technology marketplace. Although Iridium has terminated its commercial service, the Department of Defense (DOD) continues to operate an Iridium gateway, which may offer potential for DOD-affiliated NS/EP responders. The NCS will continue to track this and other developments in the LEO marketplace.

High-Altitude Platforms

Over the past 18 months, the NCS investigated the development of high-altitude platform stations (HAPS). HAPS are helium-filled, lighter-than-air platforms designed to provide International Mobile Telecommunications-2000 (IMT-2000) service. Because they will be integrated with the PSN yet will also maintain diverse routing, HAPS show great potential for use during NS/EP situations.

TERRESTRIAL NETWORKS

Recent advances in terrestrial telecommunications networks include the development of high-speed “broadband” data services over cable modems and PSN digital subscriber line (DSL) modems. Both services offer economical Internet access and data transfer rates at speeds much higher than those of analog modems and at a fraction of the cost of leased lines. The ATG is analyzing the utility of setting up a dispersed NS/EP community.

Mobile Ad Hoc Wide Area Networks

An increasingly mobile workforce, both in the private sector and in the Government, is demanding access to remote data via electronic mail (e-mail), Internet, or Intranets. This demand is leading to the development of wireless networks that can provide data to users on the go. The ATG is investigating the use of infrared 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.

Bluetooth Local Area Networks

The NCS published a technical note in July 2000 on the Bluetooth personal area network technology (Bluetooth). Bluetooth is an embedded, low-power, short-range, radio-frequency (RF) technology that seamlessly connects each intelligent appliance in a household or office in a wireless network. Because of its capabilities, Bluetooth technology is attractive not only for commercial applications but also for its use in the Federal emergency response community.

The capability of Bluetooth to enable the exchange of data among devices, such as notebook computers, personal digital assistants, and cellular telephones, could prove effective in facilitating communications between mobile disaster response elements. Because Bluetooth standardizes communications between mobile devices and local area networks, the technology could enable Federal responders to establish and relocate disaster command centers rapidly. Additionally, the ability of Bluetooth to automatically synchronize communications between wireless devices could provide Federal responders with immediate network access via their own personal communications devices.

ADVANCED INTELLIGENT NETWORK

The AIN is a rapidly evolving telecommunications technology identified by the President's NSTAC and the OMNCS as potentially having the ability 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 (e.g., 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 (e.g., GETS, DISN)
- Evaluate AIN security, survivability, reliability, and interoperability.

The OMNCS coordinates with industry and NCS member organizations to fulfill mission objectives and to identify preliminary services that the OMNCS can introduce into NS/EP initiatives (e.g., 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 also 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 with it 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. Recent accomplishments include analyses of intelligent network and network convergence issues, a study of AIN signaling message priorities used to support GETS alternate carrier routing queries, and a study of next generation networks in relation to AIN capabilities.

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

In concert with its technology activities, the OMNCS manages the Federal Telecommunications Standards Program. This program develops NS/EP-related standards and recommendations through the Federal Telecommunications Standards Committee (FTSC) and through commercial, national, and international organizations. The Chief of the Technology and Programs Division, OMNCS, chairs the governmental interagency FTSC, which was established in 1972.

NETWORK MODELING AND ANALYSIS

The OMNCS has several network analysis tools and databases that can be used to produce either impact or vulnerability analyses of networks. The impact analyses determine characteristics such as surviving connection of networks when subjected to various threatening scenarios (e.g., hurricane, flood, chemical accident). Vulnerability analyses identify critical assets that could significantly affect the connectivity of networks.

A continuing objective is to maintain a current and valid data model of the U.S. PN. OMNCS personnel, with contractor support, continued to adapt current models to changes in PN architectures and routing schemes arising from the introduction of new carriers, networks, and technologies, such as synchronous optical networks, asynchronous transfer mode (ATM), wireless services, and the Internet. The capabilities of the OMNCS network modeling and analysis tools are available for use by NCS member organizations and other Government organizations.

INFORMATION SHARING AND ANALYSIS (ISAS) SYSTEM DEVELOPMENT

As mentioned previously, the Technology and Programs Division helps to ensure that the OMNCS has the mechanisms and tools to fulfill its mission. To this end, the Information Integrity, Analysis, and Modeling (IIAM) group is focused on developing the system and tools to support the ISAC's information collection, sharing, and analysis functions.

STRATEGIC ARCHITECTURE

The Technology and Programs Division develops a strategic architecture that defines future capabilities to fulfill NS/EP requirements. The architecture is a melding of requirements, developed by the OMNCS Customer Service Division, with forward-looking, commercially standardized products and services.

FISCAL YEAR 2000 PRODUCTS

Exhibit 3-2 presents highlights of significant accomplishments in the Technology and Programs area. It lists technical notes and technical information bulletins prepared by the Technology and Programs Division for member organizations and other Government agencies.

OPERATIONS

The Operations Division ensures the availability of telecommunications across the entire spectrum of emergencies. The following paragraphs describe activities of the Operations Division during FY 2000. For information regarding the division's CIP activities, see the CIP portion of this section.

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. During FY 2000, NCC activities encompassed national and international Y2K preparation and response, critical infrastructure planning, and a new role in supporting the Network Reliability and Interoperability Council (NRIC) in a voluntary telecommunications outage reporting test.

The NCC performed an essential role in ensuring continued NS/EP telecommunications services during the Y2K transition. By employing a successful information-sharing and coordination strategy among telecommunications industry and Government operations centers domestically and abroad, the NCC served as an essential information gathering and analysis center. Partners included the Y2K Telco Forum, the Canadian Telecommunications Industry Forum, the ITU, the FCC, the GSA, and DISA.

In February 2000, the NCC Manager participated in the annual United States/Canada Civil Emergency Planning Telecommunications Advisory Group meeting

The National Coordination Center for Telecommunications (NCC) ensured continued NS/EP telecommunications services during the Year 2000 rollover. (Photo by Robert Flores.)

Exhibit 3-2 Technical Notes and Information Bulletins

- ▶ "Differential Services—One Solution for Priority Over the Internet," Ray Young. Technical Note volume 7, number 1. March 2000.
- ▶ "Direct Broadcast Satellite Radio," Robert Fenichel. Technical Note volume 7, number 2. July 2000.
- ▶ "Bluetooth Personal Area Network," Steven Karty. Technical Note volume 7, number 3. July 2000.
- ▶ "Wireless IP—Internet Without Wires," Ray Young. Technical Note volume 7, number 4. August 2000.
- ▶ "Digital Subscriber Line Technology," Dale Barr. Technical Note volume 7, number 5. August 2000.
- ▶ "Overview of Significant Optical Networking Projects and Systems." Technical Information Bulletin number 2000-01. January 2000.
- ▶ "Multimedia Over Wireless Asynchronous Transfer Mode." Technical Information Bulletin number 2000-02. January 2000.
- ▶ "Wavelength Division Multiplexing Networks." Technical Information Bulletin number 2000-03. February 2000.
- ▶ "Adopting the Defense Message System: A Guidebook." Technical Information Bulletin number 2000-04. March 2000.
- ▶ "Dense Wave Division Multiplexing Network Potential to Support Crisis Management and Disaster Communications." Technical Information Bulletin number 2000-05. May 2000.
- ▶ "Dense Wave Division Multiplexing Interoperability, Interconnection, and Networking—Catastrophic Failure Survivability." Technical Information Bulletin number 2000-06. May 2000.
- ▶ "All-Optical Networks." Technical Information Bulletin number 2000-07. August 2000.

with representatives from Industry Canada. Attendees discussed Y2K cooperation and common critical infrastructure planning issues.

In April 2000, the NCC Manager traveled to Budapest, Hungary, where he and a representative of Industry Canada provided a CIP overview to the North Atlantic Treaty Organization's (NATO) Civil Communications Planning Committee. The briefing emphasized the need for international cooperation to meet emerging critical infrastructure threats.

In October 1999, an NRIC IV recommendation named the NCC to administer a voluntary outage-reporting trial by commercial mobile radio, satellite, cable, data networking, and Internet service providers. Trial participants are to alert the NCC of outages that are likely to have significant public impact. The NCC scheduled the trial period to begin in September 2000 and to continue for 1 year.

During FY 2000, the NCC broadened its membership to include Cisco Systems, Computer Sciences Corporation, Electronic Data Systems, Nortel Networks, Science Applications International Corporation, and Verizon. This additional industry representation will enhance existing NCC-ISAC capabilities and response functions. Proactive measures by new members during critical cyber incidents during the year highlighted the importance of an extended knowledge base. For information regarding these cyber incidents, see the CIP portion of this section.

NATIONAL TELECOMMUNICATIONS COORDINATING NETWORK

The NTCN enables the timely dissemination of critical information to support PN restoration coordination. It provides a communication capability among telecommunications carriers, equipment manufacturers, and Federal departments and agencies during periods of PN degradation or outages.

A conference bridge links disparate communications systems, including HF radios, NCC-dedicated ringdown circuits, communications satellites, the PN, and the National Telecommunications Alliance's Alerting and Coordinating Network, enabling voice conversations among telecommunications industry users. During FY 2000, the OMNCS completed the enhancements started in FY 1999 in preparation for the Y2K rollover. On request, the OMNCS gave NTCN users detailed instructions regarding operation and training.

TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM

The FCC issued a report and order on November 17, 1988, establishing the TSP Program. The TSP Program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of NS/EP telecommunications services. FCC mandates authorize and require service vendors to provision and restore services with TSP assignments before services without such assignments.

TSP OPERATIONS

During FY 2000, the number of monthly requests for TSP restoration assignments continued to grow as organizations prepared for the Y2K transition and the Office of Priority Telecommunications (OPT) continued its outreach efforts to potential TSP Program users. As in FY 1999, State and local organizations constituted the largest growth area for TSP restoration assignments in FY 2000. Emergency responders used TSP provisionings in responding to the tornadoes in Missouri and fires near Los Alamos, New Mexico, and in support of the U.S. Marshals Service.

The OPT, in conjunction with the TSP Oversight Committee (OC), continued to examine the emerging telecommunications environment and evaluate its potential impact on the TSP Program. Areas of discussion included outreach to new market entrants, such as competitive local exchange carriers (CLEC), broadband services, and subcontractor reconciliation procedures. The TSP OC established a TSP Working Group, facilitated by the OPT, to enable broad participation by TSP Program users and vendors and generate discussion on those topics and other areas of interest to the TSP Program. The OPT hosted the inaugural meeting of the TSP Working Group on June 27, 2000, at the NCC.

TSP INFORMATION TECHNOLOGY SOLUTIONS

The OPT continues to recognize the importance of information technology (IT) solutions to improve information flow and expedite the process for requesting priority provisioning and restoration of telecommunications services for NS/EP users. During FY 2000, IT efforts focused on three areas: the Priority Telecommunications System (PTS) client/server, the revised TSP Web site, and the electronic forms (e-forms) application.

The OPT continued to upgrade and enhance the PTS client/server. The PTS client/server enables the effective and efficient management of the TSP Program by providing the OPT and TSP Program users and vendors with a single, shared source of information relating to specific TSP requests and TSP priority level assignments. The OPT undertook a significant effort to prepare and test the PTS platform for the Y2K transition and ensure the integrity of the data during that time.

In addition, the OPT upgraded the PTS hardware and software elements of the PTS platform and reconfigured the PTS to double the number of users able to access the PTS remotely. The OPT continued to maintain its backup client/server database and validated that the backup system would provide for continuity of TSP operations under any circumstance. Finally, the OPT implemented robust network security measures to enable the PTS to receive a 3-year certification through the Defense Information Technology Security Certification and Accreditation Process.

The OPT continues to enhance its revised TSP Web site (http://tsp.ncs.gov) to efficiently distribute TSP Program information to existing and potential TSP Program participants. Updates to the text, improved navigation capabilities, and the use of a calendar feature increased the site's usefulness. In addition, the site was expanded to include instructions for using the PTS and e-forms applications and helpful suggestions for completing the revalidation and reconciliation reporting processes.

> "The OPT continues to enhance its revised TSP Web site to efficiently distribute TSP Program information. . ."

The TSP community also embraced the use of the e-forms application, which was made available via a secure page on the Web site. The forms, which require a logon identification and password, provide organizations with a relatively small number of TSP assignments with an easy, secure, and universal mechanism to perform various required TSP processes.

TSP OUTREACH STRATEGY

The OPT continued its focus on an effective outreach strategy and implementation during FY 2000. The OPT recognized the importance of informing new telecommunications service providers, including CLECs and resellers, of their TSP obligations to ensure end-to-end priority treatment of facilities supporting

NS/EP services.

Educating and training emergency responders about the TSP Program also remained an OPT priority. OPT personnel provided comprehensive training to potential vendors; Federal, State, and local users; and emergency response coordinators. Specifically, the OPT presented briefings 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 and the Association of Public-Safety Communications Officials' Annual Conference and Exposition.

In addition, the OPT 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

The U.S. Government telecommunications policy is to meet NS/EP requirements and supply adequate and secure electric energy to critical telecommunications facilities. In 1987 the Department of Energy, in coordination with the NCS and the NSTAC, developed the Telecommunications Electric Service Priority (TESP) Program. Today, the OPT administers the TESP Program at the Federal level.

The purpose of the TESP Program is to request that States and electric utilities modify existing electric service priority systems by adding a limited number of specific telecommunications facilities that service NS/EP requirements. If an event, natural or manmade, disrupted electric power supplies to these critical telecommunications facilities, TESP would facilitate their priority restoration of their electric power, enabling essential national defense and civilian requirements to be met. The critical link between electric utilities and telecommunications facilities provided by the program represents an essential component of the response arsenal, particularly when damage to NS/EP assets might be national in scope.

The OPT is developing an outreach strategy plan to increase the level of awareness about the TESP Program within the NS/EP community. The OPT developed a TESP brochure and will distribute it to existing and potential TESP participants. In addition, the OPT implemented an innovative TESP Web site (http://tesp.ncs.gov). Both tools provide an overview of the TESP Program and TESP process and outline eligible critical facilities. The OPT also developed a TESP briefing, which it has delivered to various NS/EP organizations around the country. The OPT plans to continue the revitalization of the program by expanding outreach efforts and implementing various enhancements to the TESP process, including enabling participants to access the TESP database remotely.

More than 229 telecommunications service providers and 561 electric utilities support the TESP Program. As of May 2000, 3,721 critical telecommunications facilities were in the TESP database.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARES HF Radio Program continues to provide emergency communications in support of special operations and all-hazards situations. SHARES now incorporates the resources of more than 1,140 radio stations backed by 79 industry, Federal, and State organizations into a nationwide emergency message handling network.

The SHARES HF Interoperability Working Group, a permanent body established under the NCS COP and COR, published a revised SHARES directory on CD-ROM and revised the structure of the nationwide SHARES Coordination Network by adding five regional stations. Those stations continue to

The SHARES HF Radio Program continues to provide emergency communications in support of special operations and all-hazards situations. (Photo by Robert Flores.)

conduct weekly check-in exercises. Since the check-ins began, the number of stations participating has increased from 140 to 200 stations per week. More than 6,800 check-ins were recorded in calendar year 1999.

The working group continues to conduct three nationwide readiness exercises each year. The overall exercise objectives are to:

- ▶ Provide personnel training on operating procedures and message formats
- ▶ Expand SHARES awareness within the Federal emergency response community
- ▶ Assess the interoperability of new HF technologies.

The SHARES master coordination station KGD-34 continued to operate from the NCC. The NCC radio operations center is configured for voice, data, automatic link establishment, HF to telephone, and HF e-mail operations. The center also maintains two 24-hour HF bulletin board systems, and nine HF antennas.

COMMUNICATIONS RESOURCE INFORMATION SHARING

The Communications Resource Information Sharing (CRIS) initiative continues to support NS/EP requirements. It serves as an information source that identifies communications assets, services, and capabilities for use by the participating NCS member organizations. Twenty-three industry and Federal organizations contribute more than 40 systems that could be shared with other Federal departments and agencies during emergencies.

As an emergency communications resource initiative, CRIS exists to support all-hazards situations. Potential users of CRIS coordinate requests directly with the OMNCS, thus ensuring their requests will not interfere with other ongoing activities.

TRAINING, PLANNING, AND OPERATIONAL SUPPORT

The Operations Division encompasses nationwide training through:

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

With an emphasis on providing emergency telecommunications services to the disaster site, the OMNCS achieves its program goal through a series of training and exercise activities and technology demonstrations.

During FY 2000, the OMNCS focused on Y2K readiness and continuity of operations (COOP) training and exercise events.

TRAINING

The OMNCS provides training to the telecommunications industry, OMNCS staff, NCS Regional Managers, Emergency Support Function (ESF) #2 support agency personnel, and regional and State responders so that they can effectively execute their responsibilities during the various phases of response and recovery operations. During FY 2000, the branch successfully coordinated and performed the following activities:

Y2K Training
The OMNCS developed the NCC Y2K Database to facilitate collection and dissemination of information on Y2K-related issues as they occurred in the telecommunications infrastructure. The Training, Planning, and Operational Support (TPOS) Section conducted a series of training events to familiarize a cadre of users with the function of the database and its associated suite of analysis tools. Training participants included telecommunications industry representatives, NCC Emergency Operations Team members, FCC staff, and ITU members having responsibilities during Y2K response operations.

ERT Seminars
The ERT seminars are a highly visible and successful training program for the NCS. These seminars are 2-day events designed to provide industry, Federal, regional, State, and local personnel with the background and information required to successfully respond to a crisis situation. The OMNCS is currently in Phase III of the ERT Program. During this phase, 275 attendees participated in four sessions. Six more seminars will be held during Phase III.

Since the training program started in 1993, more than 1,800 attendees have participated in 27 sessions. This program continues to receive recognition for improving the ESF #2 response and recovery structure. During FY 2000, seminars were held in:

- Atlanta, Georgia (Federal Region IV)
- Oakland, California (Federal Region IX)
- Irving, Texas (Federal Region VI)
- San Juan, Puerto Rico (Federal Region II).

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 2000, the branch successfully coordinated and conducted the following events:

OMNCS COOP Relocation Event
To ensure operational readiness in support of the OMNCS NS/EP mission, NCC EOT and telecommunications industry personnel participated in a 3-day exercise at the OMNCS relocation facility. Through scenario-based activities, participants examined roles and responsibilities, validated operational processes and procedures, and reviewed external coordination and collaboration requirements. In conjunction with this event, the TPOS Section supported the Office of Science and Technology Policy (OSTP) in a related training activity that focused on addressing national-level telecommunications issues.

Exercise TOPOFF
The TPOS Section was involved in planning and conducting the Department of Justice (DOJ)/FEMA-sponsored event. The no-notice counterterrorism exercise took place in several U.S. locations and involved top Government officials.

REGIONAL PLANNING SUPPORT

The OMNCS assists NCS Regional Managers across the United States by providing them with capabilities, resources, and operational and functional support to aid them in meeting ESF #2 mission requirements. GSA presence with the OMNCS helps Regional Managers fulfill their emergency planning duties. OMNCS efforts include:

- Providing NCS Regional Managers with operational planning documentation, including procedures, program-specific checklists, and a coordinated national approach designed to standardize the best regional operational practices
- Maintaining a vital OMNCS Augmentee Program to support the needs of NCS Regional Managers further upon activation of ESF #2
- Supporting the annual NCS Regional Managers Conference, which generates discussion on regional-level roles and responsibilities and emergency response planning and operations, and strengthens the NCS/GSA relationship at the national and regional levels
- Supporting NCS Regional Managers at various regional planning events, such as Regional Interagency Steering Committee (RISC) meetings
- Developing a Federal Emergency Communications Coordinator (FECC) Roles and Responsibilities document to serve as a guide to newly assigned NCS Regional Managers and a general action checklist for all FECCs
- Developing region-specific disaster risk overviews and telecommunications overview studies to prepare NCS Regional Managers to respond to disasters outside their region
- Integrating new telecommunications technologies into regional planning efforts and working closely with the telecommunications industry in planning activities
- Continuing to develop disaster response after-action reports and ESF #2 lessons learned to capture regional best practices of the FECC supporting the ESF #2 telecommunications requirements of Federal, State, and local disaster response agencies.

TRAINING, PLANNING, AND OPERATIONAL SUPPORT (TPOS) WEB SITE

With the launch of its Web site (formerly the Training, Exercise, and Regional Support Web site) in 1999, the OMNCS created a new medium for sharing information with emergency responders. As we look to the 21st century, the site will continue to provide users with the latest critical telecommunications and operational training, exercise, augmentee, and regional support information.

The site contains six main sections: Operational Support, Operational Planning, Training, Exercise, NCS Augmentee Program, and Regional Support Planning. It also includes such features as an online registration form for ERT seminars, a map of the Federal regions, contact information for each FEMA region, a feedback option, a glossary of relevant acronyms, a search engine, and additional links of interest. The site will continue to evolve during FY 2001, providing users with a variety of valuable information and interactive services.

OMNCS AUGMENTEE PROGRAM

The OMNCS Augmentee Program continues to provide an important service to the NCS NS/EP mission at the national and regional levels. This was evident in FY 2000 when four Individual Mobilization Augmentees (IMA) were called upon to support the NCS and FEMA during the Y2K turnover. The program comprises the NCS IMA Program and the National Defense Executive Reserve (NDER).

During Presidentially declared disasters, the IMA Program provides NCS and NCS Regional Managers/FECCs with U.S. Army Reserve officers skilled in telecommunications to assist in emergency operations and disaster response planning. During annual training and drills, augmentees participate in a variety of ESF #2 planning and training opportunities and may be called to active duty in support of the FECC during disasters for which ESF #2 is activated.

The NDERs are executives from industry, Government, and other senior telecommunications positions who serve as volunteers, currently in wartime only. FEMA administers the NDER program.

INFORMATION SYSTEMS

The Operations Division Information Systems Branch implements and supports information systems required by the OMNCS at its primary and alternate sites. It provides technical support to OMNCS EOTs, offers help desk support to OMNCS staff, and coordinates OMNCS user IT requirements. The branch recently transitioned Emergency Response Link (ERLink) into full operational use.

EMERGENCY RESPONSE LINK

The ERLink is a controlled access Web site designed to foster the exchange of electronic information within the emergency response community. The program resulted from after-action discussions identifying communications difficulties experienced during the Northridge earthquake. The OMNCS undertook the development of a prototype system and presented the system to the director of FEMA. Concurrence was given by the FEMA Director to further refine and develop the concept. Subsequently, the OMNCS built and fielded an operational system.

The key to ERLink's ability to improve response efforts is the dissemination of data from various emergency response sources to a wider segment of the response community. While many have reported interest in reviewing material posted, few of the sources of response information have participated. The code for an improved ERLink system has been delivered to FEMA for response community use.

CONTINUITY OF GOVERNMENT

In support of continuity of Government operations, the OMNCS supports the Executive Office of the President's (EOP) Office of Science and Technology Policy in its role to provide national-level policy and guidance to facilitate reconstitution of the Nation's telecommunications infrastructure.

The OMNCS provides Government communications managers and assists in formulating national telecommunications policy and guidance. In addition, the OMNCS provides a conduit for policy execution through its industry and Government representatives. Specifically, the OMNCS develops planning and procedures documents and provides training and exercise support to OSTP.

NATIONAL EMERGENCY MANAGEMENT TEAM SUPPORT

In support of Continuity of Government (COG) operations, the OMNCS supports the EOP's OSTP in its role to provide national-level policy and guidance to facilitate reconstitution of the Nation's telecommunications infrastructure. The OMNCS provides Government communications managers and assists in formulating national telecommunications policy and guidance. In addition, the OMNCS provides a conduit for policy execution through its industry and Government representatives. The OMNCS develops planning and procedures documents and provides training and exercise support to OSTP.

CONTINUITY OF OPERATIONS (COOP)

E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, directs the NCS to identify telecommunications missions and functions that emergency responders must perform throughout any emergency; develop plans to perform these missions and functions; and develop the capability to execute those plans. During FY 2000, the OMNCS developed a comprehensive, flexible, and scalable COOP plan to ensure the continuity of its essential functions to support this mission.

In conjunction with the COOP development effort, the OMNCS also worked to develop a COOP Multi-Year Strategy and Program Management Plan during FY 2000. This COOP Multi-Year Strategy and Program Management Plan defines the OMNCS roadmap for developing a viable COOP capability. The plan also outlines the OMNCS's approach for testing, maintaining, enhancing, and managing that capability over the next 5 years. In support of this, the plan identifies resource and budget requirements that enable the OMNCS to achieve an effective, proven COOP capability and provides a schedule to complete the required actions.

> "During FY 2000, the OMNCS developed a comprehensive, flexible, and scalable COOP plan to ensure the continuity of its essential functions to support this mission."

For information regarding the OMNCS COOP Relocation Event, see the Exercises portion of this section.

PLANS AND RESOURCES

The Plans and Resources Division provides management and oversight for finance, acquisition, strategic planning, staffing, and all other resources supporting the OMNCS. Plans and Resources Division activities include exercising authority and 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 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 Performance Plan and the Strategic Plan, comprehensively evaluates organizational performance and effectiveness. The OMNCS developed the NCS Performance Plan and the Strategic Plan in response to the Government Performance and Results Act (GPRA) of 1993. The plan embraces the GPRA concept of engaging in a cycle of strategic planning, performance planning, and evaluation of an organization's achievements.

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

For day-to-day operations, the Financial Team provides the overall fiscal direction for the OMNCS. The Financial Team develops and produces all PPBS-related documentation for the OMNCS, including 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 the development, coordination, and implementation 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

Acquisition support includes aiding OMNCS offices in all aspects of the agency-level acquisition process. This includes preparing acquisition strategy documentation, statements of work, acquisition packages, proposal evaluation packages, and support documentation for NCS programs and projects. The Acquisition Team also monitors contractual performance and budget execution performance rates, identifies deficiencies, ensures reporting accuracy, and recommends adjustments.

CUSTOMER SERVICE

The Customer Service Division provides support to the NCS Committee of Principals (COP) and Council of Representatives (COR) and the President's NSTAC. The division also identifies and validates NS/EP telecommunications requirements to ensure the NCS is responsive to customer needs, develops assessment of threats to NS/EP telecommunications, and manages the Government and NSTAC NSIE process. The following paragraphs describe the Customer Service Division's FY 2000 activities. For information regarding the division's CIP activities, see the CIP portion of this section.

NCS COMMITTEE OF PRINCIPALS/COUNCIL OF REPRESENTATIVES

The NCS COP met once, and the COR met twice during FY 2000. At these meetings, the COP and COR were provided information on Year 2000, NCC-ISAC, NSTAC, Joint Task Force-Computer Network Defense, Mobile Satellite Services, Interagency Contingency Communications Plan, and various other OMNCS programs. The COP concurred with the NCS Comments to the NSTAC XXII Executive Report. The COP approved the formation of an Internet Program Implementation Team from among the NCS agencies.

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

The President's NSTAC held its 23rd meeting on May 16, 2000, in Colorado Springs, Colorado, at the invitation of the Commander in Chief, United States Space Command (USSPACECOM). The central theme of the meeting was CIP—information sharing in the telecommunications infrastructure. Major issues addressed included the barriers to and benefits of information sharing, shortage of information technology security professionals, and implementation of Presidential Decision Directive 63 (PDD-63), *Critical Infrastructure*

Protection. During the Business and Executive Sessions of the meeting, the NSTAC Principals, senior Administration officials, and the Commander in Chief, USSPACECOM, discussed these and other issues developed by NSTAC's Industry Executive Subcommittee (IES) during FY 2000.

NSTAC'S INDUSTRY EXECUTIVE SUBCOMMITTEE ACTIVITIES

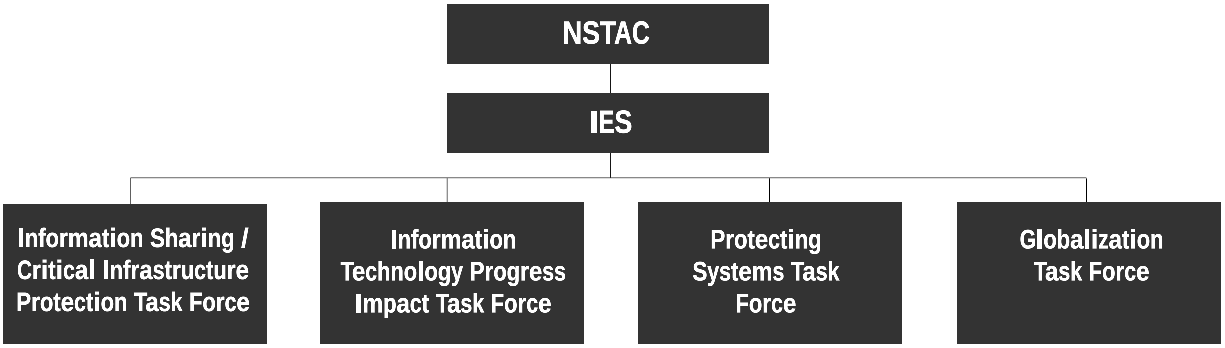
The NSTAC's IES continued to identify and develop issues for the NSTAC and direct the activities of its subgroups. Information sharing for CIP, network convergence, network security, and globalization were four key issue sets addressed by the IES and its subgroups during FY 2000. Exhibit 3-3 depicts the corresponding organizational structure. Specific subgroup activities and the results of their work are discussed in the subsequent sections.

NSTAC'S INFORMATION SHARING/CRITICAL INFRASTRUCTURE PROTECTION TASK FORCE

The IES formed the Information Sharing / Critical Infrastructure Protection Task Force (IS / CIPTF) to address IA- and CIP-related issues. The task force examined Y2K experiences and the historical experiences of the NSIEs and the NCC — including the implementation of the NCC as an ISAC — to identify lessons learned for successful IA / CIP-related information sharing.

The IS / CIPTF concluded that historical and Y2K experiences demonstrate information sharing to be a valuable effort; however, for widespread information sharing to take place, legal, operational, and perceived impediments must be overcome. The task force determined that the potential disclosure of information under the Freedom of Information Act (FOIA) represents one of the key barriers to sharing CIP-related information between industry and Government. As a result, with the assistance of the NSTAC's Legislative and Regulatory Working Group (LRWG), the task force undertook an in-depth analysis of FOIA and the implications for industry-Government information exchange. In accordance with FOIA, the public may request and gain access to records maintained by Government departments and agencies. Due to confidentiality and liability concerns, such potential disclosure of data may deter industry from sharing information with Government. Although numerous exemptions to FOIA's requirement for disclosure of information exist, none clearly cover information pertaining to CIP. Based on the IS / CIPTF's findings, the NSTAC recommended that the President

Exhibit 3-3 The President's National Security Telecommunications Advisory Committee Organization from NSTAC XXIII Cycle


NSTAC
IES
Information Sharing / Critical Infrastructure Protection Task Force
Information Technology Progress Impact Task Force
Protecting Systems Task Force
Globalization Task Force

support the enactment of legislation to protect CIP information voluntarily shared with the Government from disclosure under FOIA.

The IS/CIPTF worked to support and provide guidance to Government officials responsible for implementing PDD-63. NSTAC member companies participated in the Partnership for Critical Infrastructure Security by sharing lessons learned through their NSTAC experiences. IS/CIPTF members also entered into a dialogue with Government officials responsible for drafting version 1.0 of the *National Plan for Information Systems Protection* and provided input for consideration in drafting subsequent versions of the plan.

NSTAC'S INFORMATION TECHNOLOGY PROGRESS IMPACT TASK FORCE

The IES established the Information Technology Progress Impact Task Force (ITPITF) to examine the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services. The IES also tasked the ITPITF to examine the evolving network technologies and capabilities that could assist in satisfying NS/EP functional requirements during convergence and in the NGN. During FY 2000, the ITPITF concluded that the PN is changing from separate switched voice and packet data networks to an interconnected network and will become a unified end-to-end packet-based NGN over the next several years. The ITPITF also identified the resulting potential implications of convergence and the NGN for major NS/EP telecommunications services.

Specifically, the potential implications for GETS include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and lack of commensurate network reliability and security. Therefore, the ITPITF concluded that, to provide GETS-type services during convergence and in the NGN, quality of service (QoS) schemes would need to be expanded to provide services commensurate with NS/EP needs.

The ITPITF also concluded that the TSP Program, as originally conceived, remains relevant during convergence because restoration assignments can still be applied to identifiable segments of the PSN. However, TSP as currently defined, did not and should not have a role in the NGN. If the NS/EP community required similar types of priority services for packet networks, a new program would have to be established to support such services.

Furthermore, the ITPITF stated that although specific NGN standards have not yet been developed to support NS/EP requirements, the emerging NGN technology is capable of supporting these requirements. However, NS/EP traffic will require newly designed and standardized features to overcome new problems associated with packet networks. The ITPITF concluded that such NS/EP requirements are unlikely to be incorporated by industry unless the features needed to meet these requirements are standardized by industry, perhaps with prompting from the Government.

Based on the above conclusions, the NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry, to promptly determine precise functional NS/EP requirements for convergence and the NGN, and ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during NGN standards development and implementation.

NSTAC'S PROTECTING SYSTEMS TASK FORCE

The IES established the Protecting Systems Task Force (PSTF) to examine how the Government can optimally focus its efforts to enhance the security of the Nation's NS/EP telecommunications and IT systems. To this end, the task force examined current industry and Government network security strategies to determine whether alternative strategies might more effectively diminish risk.

The study focused on those network security efforts intended to diminish risk from unauthorized access to or activity in an information system. The methodology for the study was based, in part, on a model of network security developed during a prior NSTAC study that identified four components of network security: prevention, detection, response, and mitigation. The PSTF used this model as a framework for its study and sought to answer the question: Could the risk to network security be reduced more effectively by changing the relative focus of network security efforts among these four components?

The PSTF analyzed data collected from presentations, interviews, network security surveys, and Government policy documents. The task force concluded that security is not a "one-size-fits-all" proposition. Although no optimal focus among prevention, detection, response, and mitigation suitable for all organizations exists, each individual organization can consider how it focuses its network security efforts among these four components and ensure that it employs an optimal strategy to meet its own needs.

> "The [PSTF] concluded that security is not a 'one-size-fits-all' proposition."

The PSTF subsequently identified a number of common themes among the organizations providing input to the study as well as some barriers that may impede the ability of an organization to implement an optimal focus among the four components.

NSTAC'S GLOBALIZATION TASK FORCE

The IES tasked the Globalization Task Force (GTF) with identifying NS/EP telecommunications issues arising from economic, technology, and operations globalization. In FY 2000, the GTF focused its activities on the emerging Global Information Infrastructure (GII) in 2010, the foreign ownership of critical NS/EP telecommunications systems, and technology export policies.

Global Information Infrastructure

The GTF researched and gathered information from industry and Government experts on emerging space-, airborne-, and land-based communications systems and services. These information gathering activities provided the GTF with the insights needed to forecast the GII in 2010 and draw conclusions about NS/EP telecommunications preparedness.

Drawing upon these insights, the GTF characterized the physical network elements, services, and protocols that will be prominently featured in 2010. The task force paid specific attention to the global homogenization of communications capabilities, expected improvements to QoS and network assurance, and the ubiquity and availability of advanced communications technologies as pertaining specifically to NS/EP users.

The GTF concluded that a global homogenization of communications capabilities is occurring as converging technologies and services eliminate domestic and international boundaries. However, although the number and locations of these available communications technologies will continue to increase globally, no guarantees exist that the technologies will be ubiquitous and available at any location in the world. Furthermore, because the GII is rapidly changing and QoS features of packet-based networks are improving, forecasting the additional services or network features that may be necessary to support NS/EP operations in 2010 becomes difficult. Prudent NS/EP communications contingency planning will be necessary to meet global coverage goals and specific NS/EP requirements.

Based on the GTF's conclusions, the NSTAC recommended that the President direct appropriate departments and agencies to conduct exercises in those areas and environments where NS/EP operations can be expected to take place, to ensure that the required high-capacity, broadband access to the GII is available. The NSTAC also recommended that the President ensure that NS/EP requirements such as interoperability, security, and mobility are identified and considered in emerging standards and technical specifications as the GII evolves to 2010. The NSTAC further recommended that any specialized services that must be developed to satisfy NS/EP requirements not satisfied by commercial systems be identified.

Technology Export

The GTF addressed the national security implications associated with current export control policies related to the transfer of strong encryption products, satellite technology, and high-performance computers. In studying this issue, the task force considered opposing viewpoints.

Historically, industry advocates the liberalization of export policies, contending that the Nation's security depends heavily on the economic well-being of its technological base. Proponents of this viewpoint also advocate easing the restrictions that prevent the export of various technologies because manufacturers need to export their technologies to maintain their economic viability, ensure profits to fund research and development (R&D), and remain competitive in foreign markets. However, the U.S. Government has sought to restrict the export of certain items, realizing the need to prevent U.S. adversaries and criminals from obtaining advanced technologies.

To scope the issue, the GTF compiled some basic information on these key technology export policies, including information on the implementation of new export policies and regulations. The GTF concluded that, because technology progresses faster than export policy can keep up with it, effective communications among industry, the executive branch of Government, and Congress remains essential in resolving issues in this arena. The GTF concluded that both industry and Government must continually reevaluate the limits placed on the export of technologies.

Foreign Ownership

The GTF examined foreign ownership regulations and their effect on NS/EP telecommunications. With assistance from the NSTAC's LRWG, the task force examined domestic regulatory history and conducted analyses of several mergers and acquisitions between domestic and foreign telecommunications carriers. Through the case studies, the task force found that the current regulatory structure satisfied the different interests of the parties involved. It is unclear whether further statutory or regulatory changes would effectively enhance the role of national security in foreign ownership situations at present. The GTF concluded that the current regulatory structure effectively accommodated increasing levels of foreign ownership of U.S. telecommunications facilities while allowing the Federal Government to retain the authority to prevent such ownership that might compromise national security interests. Based on the GTF's conclusions, the NSTAC recommended that the President direct appropriate departments and agencies to ensure that the review process for commercial arrangements involving foreign ownership remains adequate to protect NS/EP concerns as the environment evolves and becomes more complex.

NCS INFORMATION ASSETS

NCS ISSUANCE SYSTEM

The NCS Issuance System is the authority for the internal organization, policy, procedures, practices, and management of the NCS.

In FY 2000, the NCS Directive 3-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)*; NCS Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP) Service User Manual*; and NCS Handbook 3-1-2, *Service Vendor Handbook for the Telecommunications Service Priority (TSP) System* were approved and distributed.

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 a chance to learn about the NCS and NSTAC. The home page provided links to NCS and NSTAC history, information about NCS and NSTAC programs and activities, and online versions of NCS and NSTAC publications.

In June 2000, the OMNCS began redesigning many of its Web pages, including the NCS home page. When completed, the redesign will permit NCS Web site visitors better access to sites about NCS programs and activities, as well as updated information about NCS activities.

Among the publications posted onto the NCS home page during FY 2000 were the FY 1999 NCS Report, the NSTAC XXIII Issue Review, and the NSTAC XXIII Reports. The home page includes 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.

> **"... the OMNCS continued development of a wireless priority treatment program to provide NS/EP users priority access to the public wireless network."**

REQUIREMENTS

The Communications Assessment Branch (CAB) is responsible for identifying, evaluating, and validating NS/EP telecommunications requirements for the NCS. The 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 serves to optimize OMNCS customer interface and participation in the requirements process. The following paragraphs describe the accomplishments of CAB during FY 2000.

REQUIREMENTS SHORTFALLS ASSESSMENT

Through the Requirements Forum, the OMNCS completed the *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. As a result of the report, the OMNCS continued development of a wireless priority treatment program to provide NS/EP users priority access to the public wireless network. In addition, the shortfalls report identified a need to address NS/EP user requirements concerning e-mail reliability and interoperability. Pursuant to PDD-63, the report also establishes a basis for the NCC-ISAC, which provides information sharing and analysis, on a near real-time basis, of incidents, operational anomalies, and electronic intrusions affecting the telecommunications infrastructure.

REQUIREMENTS IDENTIFICATION EFFORT

The OMNCS is actively engaged in developing a methodology to solicit and collect NS/EP communications requirements from the NS/EP community. The three primary objectives of the effort are as follows:

- ▶ Obtain input directly from NCS customers concerning their NS/EP communications requirements, specifically to:
  - —Identify new and emerging requirements
  - —Validate identified customer requirements

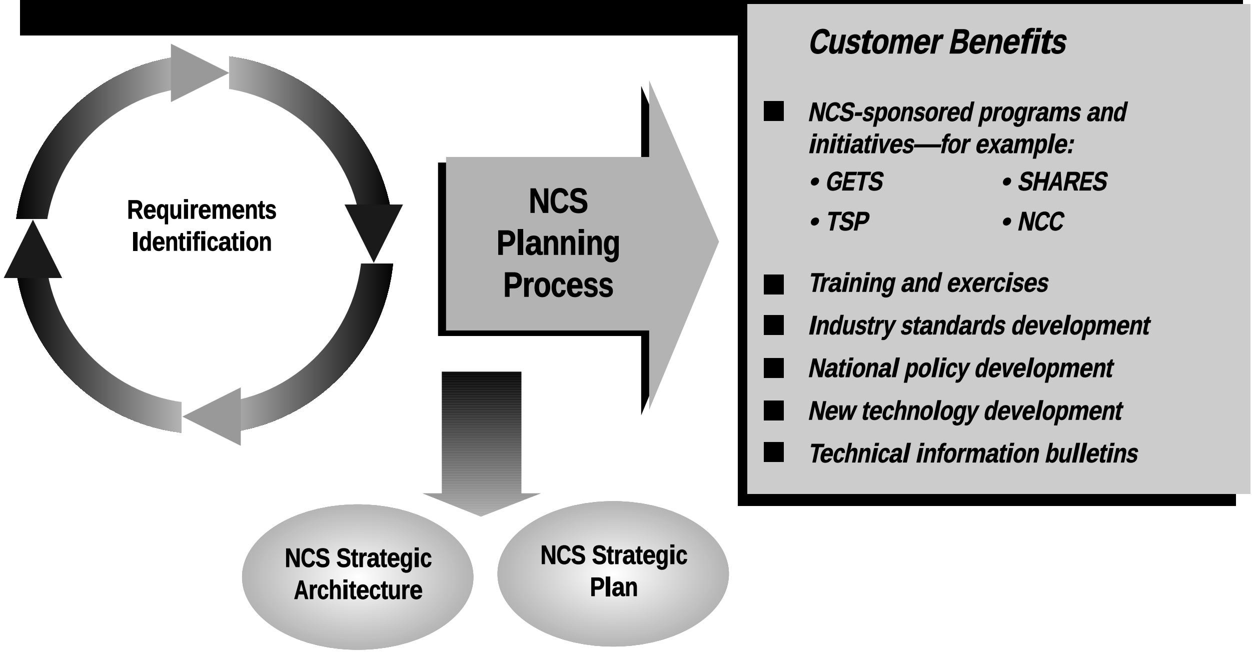
- ▶ Provide customers with an opportunity to express their NS/EP needs for consideration in NCS program and initiative development

- ▶ Ensure more efficient and effective expenditure of limited NCS funds.

The overall effort seeks to identify NS/EP communications requirements through both regional and focused requirements collection activities. The regional effort is customer centric and obtains feedback directly from regional NS/EP responders concerning communications requirements, whereas focused requirements collection activities obtain requirements information from specific areas of concern within the NS/EP community. Current focused requirements efforts concentrate on identifying requirements within the areas of weapons of mass destruction and IA. Future CAB efforts may include an assessment of department and agency Internet-related requirements.

This requirements identification effort will assist the NCS in developing programs and initiatives that will directly benefit NCS customers and will support the development of the NCS Evolutionary

Exhibit 3-4 Requirements Identification Benefits



Customer Benefits

- ■ *NCS-sponsored programs and initiatives—for example:*
  - *• GETS*
  - *• SHARES*
  - *• TSP*
  - *• NCC*
- ■ *Training and exercises*
- ■ *Industry standards development*
- ■ *National policy development*
- ■ *New technology development*
- ■ *Technical information bulletins*

Architecture and Strategic Plan. Exhibit 3-4 illustrates the benefits of NCS requirements identification.

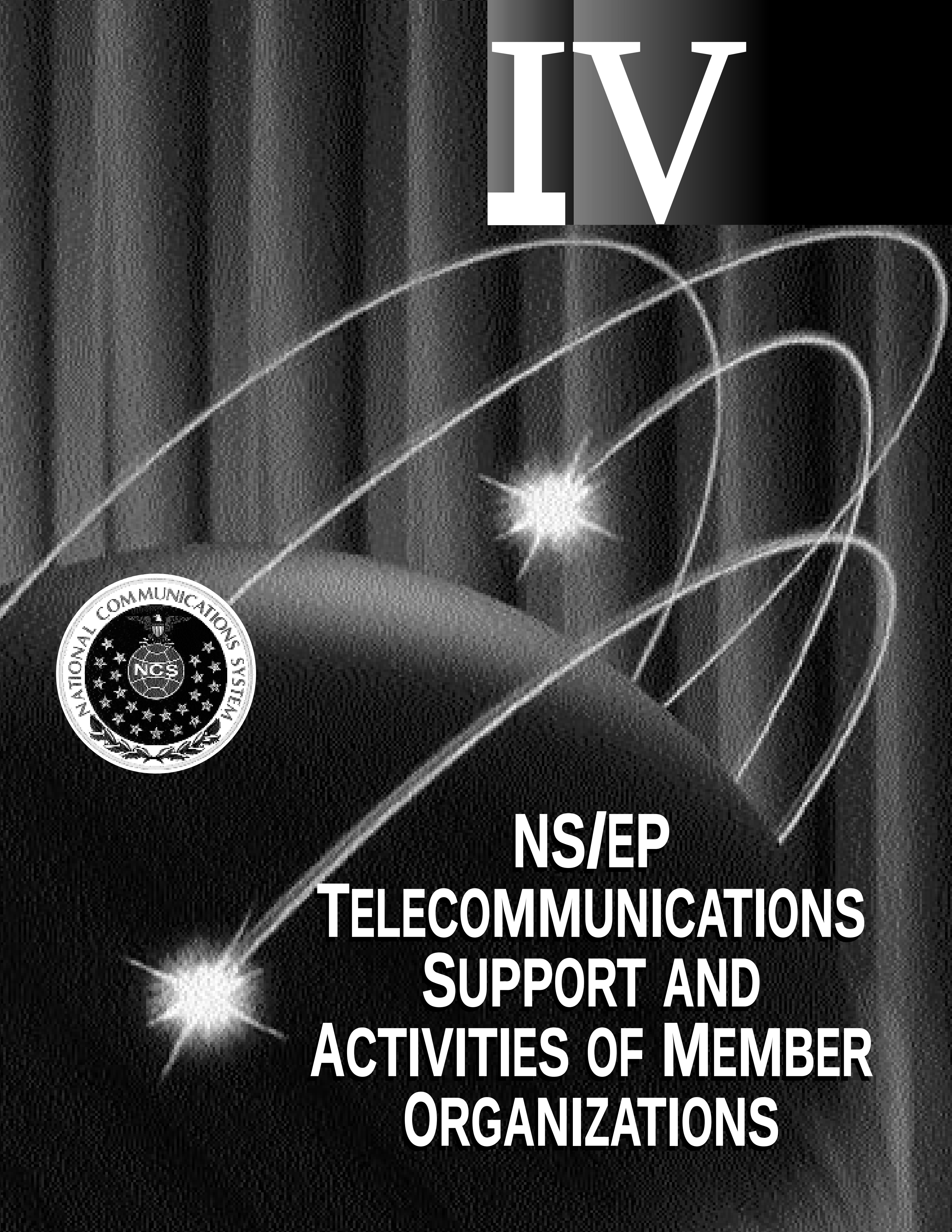
GAP ANALYSIS

The Communications Assessment Staff continued an effort, begun in FY 1999, to identify potential gaps between the Government's requirements for assured communications connectivity and what industry routinely provides. During FY 2000, a gap analysis was completed at the NCC. Consistent with the methodology used in the first gap analysis pilot with the Nuclear Regulatory Commission, the NCC gap analysis involved:

- Confirming the agency's NS/EP missions and functions
- Identifying the minimum essential and critical communications needed to sustain NS/EP operations
- Analyzing the agency's communications infrastructure supporting NS/EP activities
- Identifying any gaps between the agency's NS/EP communications requirements and the level of service it routinely receives from industry.

The NCC gap analysis team concluded that no technological gap existed at the NCC.

IV



NS/EP Telecommunications Support and Activities of Member Organizations

DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to support the President in formulating and executing U.S. foreign policy. This mission determines its telecommunications support requirements. Essential Department of State (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 continuous 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.

DOS SIGNIFICANT ACCOMPLISHMENTS

Modernization Efforts

Year 2000-compliant central infrastructures were deployed for the Department's global classified and unclassified e-mail systems, using a three-tiered architecture based on the X.400 transmission protocol standard. To improve network security and message throughput, infrastructure for an X.500-based Foreign Affairs Directory Service was deployed on the unclassified e-mail system. The classified e-mail system will undergo a similar Secure Foreign Affairs Directory Service enhancement by the end of the calendar year.

Primary Telegram Processing System

The Department replaced its primary Major Relay Station processor and Main State Messaging Center telegram processor with Concurrent 3280 systems. The Concurrent 3280 multiprocessor system uses an S-bus architecture which, depending on configuration, is capable of 6 to 36 million instructions per second and can accommodate from one to six processors. Memory was increased fourfold and Transmission Central Protocol / Internet Protocol capability was added, achieving an immediate threefold increase in processor speed.

Communication Security

The Department created a Public Key Infrastructure (PKI) Program Office to provide an additional layer of infrastructure security protection from increasing threats from cyber attack. Working closely with National Security Agency (NSA), the DOS is the first civilian agency to integrate a near level-4 PKI pilot. Secure e-mail and Web-enabled security will be the principal applications for 500 end users. This technology will greatly enhance the overall level of information security for the DOS. Also, in cooperation with NSA, DOS has successfully tested over-the-air-rekeying (OTAR) with 28 overseas posts. The success of this effort has fueled the Department's determination to proceed with implementing OTAR on its corporate systems worldwide. This action will increase the security of mission-critical systems within the Federal information technology (IT) infrastructure by limiting opportunities for exploitation. The goal of the DOS's OTAR program is to convert each embassy and consulate to OTAR within calendar year 2000. This is expected to reduce the amount of key material required for State systems by 70 percent.

Interagency Collaboration

Following the Overseas Presence Advisory Panel's recommendations, the Department started a program to establish a common IT 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 garner the expertise of specialists from other posts or headquarters organizations in a virtual team environment.

United States Information Agency (USIA) Integration

The Department successfully and fully integrated the United States Information Agency and its advanced IT into DOS. This achievement has provided U.S. diplomacy with a new and stronger voice for promoting global democracy, prosperity, and peace.

Voice Program

The Department provided secure voice access to the domestic and foreign affairs community and assisted interdepartmental agencies in meeting their secure voice requirements.

Counter-Narcotics

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

Support for the Secretary of State

The Department provided and supported protective communications packages for domestic and oversees 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 national security emergency preparedness (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 National Communications System 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 have access to a cost-effective, technologically sound telecommunications infrastructure so that they may carry out their missions.

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.

TREAS SIGNIFICANT ACCOMPLISHMENTS

Federal Law Enforcement Wireless Users Group

TREAS has continued its activities as co-chair of the Federal Law Enforcement Wireless Users Group 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 publicly embarrassing compromises of its electronic data systems and hopes to continue this trend as well as to enhance its existing intrusion prevention, detection, and remediation capabilities.

Support for the Federal Public Key Infrastructure Development

TREAS provided technical, budgetary, and leadership support for the development and use of an interoperable governmentwide Public Key Infrastructure, to enable electronic transactions over the Internet in a trusted environment.

Seat Management

TREAS headquarters departmental offices has partnered with Wang Government Services under the General Services Administration Seat Management contract. This performance-based contract provides departmental office customers with personal computers (desktop and laptop), standard software, and printers, HelpDesk, infrastructure support (network, local area network 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 as well as 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. This system will streamline the filing process for importers and exporters and reduce the paperwork burden by eliminating multiple and redundant data filings currently required by various 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 to improve risk assessment, enforcement, policy formulation, and analysis. Though the system is under development by the U.S. Customs Service, an interagency board of directors oversees its development and implementation.

Treasury Secure Data Network

TREAS is creating a new infrastructure for processing and distributing classified data in the Historic Treasury Building. This effort is being coordinated with the building renovation team to ensure that the historic integrity of the facility is not compromised but that a state-of-the-art, classified data processing capability is available for all Treasury users who require it.

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 (OSD), 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 communication systems are the concern of a directorate of the Joint Staff.

DOD SIGNIFICANT ACCOMPLISHMENTS

Year 2000

Within the DOD, the scope and complexity of the Year 2000 (Y2K) problem were unparalleled. Nevertheless, the transition to a fully compliant Y2K infrastructure occurred smoothly and was a tremendous success. The Y2K rollover experienced some problems, but they were minimal. By using the team and liaison elements concept, the DOD tracked the Y2K compliance of 9,634 systems of which 25 percent (2,367) were mission-critical.

The Department verified Y2K compliance of 637 military installations around the world and in the United States that rely on the supporting infrastructure systems. In addition, the Department had 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. Throughout the Y2K effort, readiness was treated as a major threat to military effectiveness.

The numerous forums enabled a dialogue of ideas and became the key ingredient that led to the tremendous success of the Y2K rollover and the subsequent leap year compliance.

Global Information Grid

To ensure the smooth implementation of the standards of the Global Information Grid (GIG) architecture, the DOD Chief Information Officer (CIO) has established a cohesive process for provisioning all wide area network / metropolitan area network (WAN / MAN) requirements within the Department. The GIG Network Policy requires all such requirements to be placed on the Defense Information Systems Network (DISN), unless waived.

Toward this end, all requirements for WAN / MAN connectivity in the DOD must first be presented to DISA, which will either recommend a DISN solution or request a temporary waiver until the DISN can be upgraded to support the emerging requirement. If DISA supports a tempory waiver, both DISA and the user are responsible for presenting such a waiver request to the DOD CIO.

A second waiver scenario arises when DISA recommends a DISN solution, but the user rejects that solution. In that case, the user must present the waiver request to the DOD CIO. Both types of waivers — temporary and non-DISN—initially come to the GIG Network Waiver Review Panel (O-6 level), which develops a recommendation for the DOD CIO. Final adjudication occurs when the waiver is presented to the GIG Waiver Board, chaired by the ASD (C3I).

Waivers are considered individually, based on the mission need, congruence with the GIG architecture, and the supporting business case. The CIO staff of the organization requesting the waiver becomes the spokesperson to the panel and board. This process enables the requester to discuss the rationale and technical reasons for the waiver request to the Waiver Review Panel members.

This open dialogue has enabled DISA to better understand the rationale for the waiver. Similarly, this process has afforded the waiver requestor a better understanding of the DISN capabilities.

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 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 Deputy Assistant Attorney General for Information Resources Management, operates and manages DOJ's message processing systems and the Telecommunications Services Center. TSS also provides networking and technical assistance to DOJ's offices, boards, and divisions. Secure 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, and the Immigration and Naturalization Service (INS) continue to administer their own communications security programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

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

- Russell Royston, TSS, provides full-time on site representation for DOJ as the Deputy Chief, Operations Division, National Communications Sytem (NCS).
- Gary Laws, Telecommunications Services Staff, represents DOJ on the Council of Representatives (COR).
- DOJ continues its active participation in the NCS activities of the Council of Representatives (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.
- Additionally, the department is an active participant in the Government Emergency Telecommunications Service Program, the Telecommunications Service Priority Program, and the Shared Resources High Frequency Radio Program.

DOJ SIGNIFICANT ACCOMPLISHMENTS

Justice Consolidated Network

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. Over 20 separate DOJ networks were upgraded and modernized into a single Justice network, consolidating services, reducing costs, improving security, and boosting network performance. Implementation of the JCN infrastructure is complete with 75 percent of the DOJ component sites transitioned or scheduled to transition by December 31, 2000. Network sites are strategically situated near DOJ component locations in every State in the United States, including Alaska and Hawaii. Sites in Puerto Rico, the Virgin Islands, Guam, and Saipan are under development. JCN will provide service at 1,500 locations and interconnect all DOJ components.

The JCN has grown from a pilot program of five sites to the complete network infrastructure. Major program participants include the FBI, DEA, INS, the Bureau of Prisons, and the Executive Office for the U.S. Attorneys. Implementing JCN's concentration nodes in this short time frame took a concerted effort and was accomplished through a high level of cooperation and partnership among components of the DOJ, the General Services Administration's Federal Telecommunications System, and its vendors. By tackling security analysis and planning early in the project, the JCN program has earned the distinction of being the first Federal telecommunications system using public switched network services to be qualified for security accreditation.

To ensure JCN's operational integrity, the Department operates a 24-hours-a-day, 7-days-a-week Network Services Center to monitor operations, measure performance, and provide timely resolution of network problems and restoration of outages by identifying, notifying, and coordinating with JCN users and service providers.

DOJ COMMUNICATIONS SYSTEMS ASSETS/SERVICES

Automatic Data Processing Teleprocessing System

Drug Enforcement Administration Nationwide Very High Frequency Radio System

Drug Enforcement Administration Secure Voice System
Global Criminal Justice Information System

Immigration and Naturalization Service Tactical Radio System

Immigration and Naturalization Service Integrated Network Communications

Joint Automated Booking System

Justice Consolidated Network

Justice Telecommunications Service

National Crime Information Center

U.S. Marshals Service Communications System

U.S. Marshals Service Special Operations Group

DEPARTMENT OF THE INTERIOR (DOI)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to efficiently manage the Nation's natural resources. The Department of the Interior (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 wild 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. Wild fire suppression operations are conducted in close cooperation with State and local government emergency support activities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Telecommunications Systems Division, Office of Information Resources Management, is responsible for DOI telecommunications program management. Bureau telecommunications managers and their staff are responsible for voice and data network operations.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The transition of the Department's voice and data communications services from the General Services Administration's Federal Telecommunications System (FTS) 2000 / AT&T to the FTS2001 / WorldCom contract is a priority effort. Implementing FTS2001 transition plans required extensive attention throughout the year. All switched voice services were successfully transitioned, and the transition and redesign of the Department's data network services will be completed in fiscal year 2001. DOI is significantly improving services and increasing the bandwidth available to the DOI's nationwide data communications network (DOINET) users by changing from a private network to a virtual network architecture on the WorldCom public network. DOINET provides Internet access and supports departmentwide administrative applications, bureau programs, and other agency needs.

The Alaska Regional Telecommunications Network, based on DOINET technologies, provides services to several Federal agencies in Alaska and connects to the continental United States through DOINET. These networks provide economical Internet and shared information processing system access. Shared use of these networks has lowered costs, improved performance, and increased the availability of data and video services. In addition, DOI and USDA are working 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 and systems in response to the National Telecommunications and Information Administration mandated transition to narrowband land mobile radio 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 specialists throughout the DOI have Government Emergency Telecommunications Service (GETS) cards for long distance emergency telephone communications. User policies and instructions accompanied distribution of GETS cards.

DOI SIGNIFICANT ACCOMPLISHMENTS

All DOI mission-critical systems and telecommunications networks were Year 2000 (Y2K) compliant and were operational on January 1, 2000.

The Interior Site Information System, developed to provide a DOI intranet-accessible inventory of telephone systems, data transmission equipment, circuits, facilities, and radio systems supported Y2K and FTS2001 transition activities.

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; managing the protection and use of National Forests, National Grasslands, wilderness areas, and other public lands and facilities under USDA jurisdiction; managing wildland fire control activities on these lands in coordination with local authorities; and inspecting livestock and poultry, and other products to ensure the safety and wholesomeness of food.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

USDA continues to actively support the Government Emergency Telecommunications Service program by working to ensure personal identification number cards are provided to key NS/EP personnel within the Department.

USDA has purchased several high frequency (HF) radios for the USDA Emergency Coordination Center, as well as suitcase portable units for two major computer centers. The USDA Forest Service is maintaining several HF communications facilities in the West. These stations are affiliated with the National Communications System-managed Shared Resources High Frequency Radio (SHARES) program.

USDA also:

- Continues support for the Committee of Principals/Council of Representatives and the President’s National Security Telecommunications Advisory Committee
- Participates on SHARES HF Radio Program, Communications Resources Information Sharing Initiative, Federal Telecommunications Standards Committee , and Federal Wireless Users Forum
- Supports the Department of State Diplomatic Telecommunications Service
- Participates in and represents the USDA on 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 technology.

NS/EP PARTNERSHIP ACTIVITIES

USDA is pilot testing mixed digital/analog land mobile radio systems at several locations in the West. These tests are being carried out to ensure that any unknown problems are surfaced and resolved before a large-scale implementation is begun. With the availability of digital land mobile radio equipment fast becoming a reality, conversion to the new technology is of high importance. However, the USDA is weighing carefully the balance between a swift conversion and the requirements of mission capability, employee safety, and overall cost.

DEPARTMENT OF COMMERCE (DOC)

NS/EP TELECOMMUNICATIONS MISSION

The Department of Commerce (DOC) mission includes activities for domestic and international trade; commodities, invention, economic analysis of census and industry; and technology related patents and standards. Its technology role includes providing tools for monitoring and analyzing environmental weather, oceanic, and geophysical data and for reporting critical early warnings of emergencies to prevent loss of human life and property damage. These missions are ongoing and sustained during national level NS / EP activities in all-hazards emergencies, including stress periods during peacetime, crisis, mobilization, and periods of disaster recovery.

The DOC mission supports the economic strength of the U.S. national infrastructure. This includes 15 activities supporting NS / EP functions identified in Executive Orders 12656 and 12472 requiring the implementation of plans during peacetime and activation of plans during crisis / mobilization and periods of disaster recovery. The Federal Response Plan identifies DOC as a major supporter of seven emergency support functions for reconstitution and support of State and local government critical functions, as well as the control of distributed goods and services. DOC has a leadership role in the national critical infrastructure protection (CIP) program supporting the responsibility to oversee the communications and information sector of the U.S. economy, as well as support the CIP management coordination center, Critical Information Assurance Office (CIAO) as specified in Presidential Decision Directive 63 (PDD-63). More information on these programs is available at the DOC Web page http: / / www.doc.gov.

CURRENT NS/EP TELECOMMUNICATIONS ACTIVITIES

- The DOC Chief Information Officer (CIO) joins the National Communications System (NCS) National Coordination Center (NCC) — The CIO staff representative from DOC has been assigned as a member of the NCS / NCC to provide insight on Commerce issues to the membership from industry and Government as well as coordinate program requirements.
- DOC International Trade Administration (ITA) communications upgrade continues—ITA continues to upgrade data communication platforms supporting access to trade information at world trade centers and U.S. embassies overseas and use the capability of the Department of State / Diplomatic Telecommunications Service network to support international trade communications.
- DOC National Oceanic and Atmospheric Administration (NOAA) completes field installation of advanced weather information processing system National Weather Service (NWS)—NWS implemented a new telecommunication network supporting weather data collection and distribution platforms from field observation offices and processing centers; the new capability provides communications services for the advanced weather information processing system.
- DOC continues to deploy Web services for administrative systems—DOC CIO staff continued to implement a Web platform for automating administrative information systems to allow Internet and intranet access using Web browser technology.
- DOC CIO efforts reflect successful Year 2000 (Y2K) results—The CIO staff prepared Commerce and its operating units for the Y2K transition with the necessary information technology (IT) equipment, software, and application upgrades and achieved a successful transition without major issues.
- DOC CIO monitors cyber events and IT assets for alerts—The CIO operated an IT alert center to monitor activities during the Y2K transition and plans to maintain this capability to support CIP initiatives.
- DOC CIO adds new dimension to IT management support organization—The Secretary of Commerce reorganized the Department's management structure to support the CIO IT requirements of the entire Department, and to support IT security and critical infrastructure program management.
- DOC and NOAA NWS take new initiatives with Defense Message System (DMS) transition—The DOC CIO staff stepped up management direction and coordination to the operating units for transition from Automatic Digital Information Network to DMS transmission services to communicate with DOD and other agencies requiring priority message support services.
- DOC and NOAA NWS add new dimension to the Shared Resources High Frequency Radio (SHARES) Program —The DOC CIO staff coordinated the initiation of high frequency (HF) radio service participation in the SHARES program to support communications in all-hazards emergencies.
- DOC moves CIAO into main facilities to complement CIP efforts—The Secretary of Commerce directed support for the CIAO operations by including the core operations in Herbert C. Hoover Building Headquarters and under the direction of the Assistant Secretary for Export Administration.
- DOC adds HF radio for support of emergency operations—The DOC CIO staff coordinated the initiation of HF radio services in DOC Office of the Secretary and National Telecommunications and Information Administration (NTIA) to support communications in all-hazards emergencies.
- DOC CIO adds Transmission Control Protocol / Internet Protocol (TCP / IP) upgrades to the Department of Commerce Network (DOCnet) to support digital initiatives—The CIO staff coordinated the upgrade of telecommunications services and equipment in the DOCnet program to TCP / IP to support enhancements needed for future digital commerce initiatives.
- DOC / NOAA plans the next generation of weather satellites with DOD—The NWS has started work with DOD on the next generation of weather satellite systems with the cooperation of the National Aeronautics and Space Administration. This effort is part of the Earth observing program of the National Polar-Orbiting Operational Environmental Satellite System slated for operational development in 2005-2008.

- DOC / NOAA initiates interactive weather information network (IWIN)—The NWS staff completed implementation of the first phase of the interactive weather information platform, which provides users with a single source for all environmental emergency reports and alerts. Emergency managers have access to IWIN via the emergency management weather information network Web site on the NWS Web page.

- DOC reviews electronic commerce and Internet services used in Government to determine NS / EP capabilities—With the NCS, the DOC CIO staff plans to review electronic commerce and Internet services to determine the vulnerability and reliability of these services with respect to the Government and develop a risk assessment of NS / EP programs and the supporting critical infrastructure.

- DOC leads Government organizations in Federal Telecommunications System (FTS) 2001 transition for telecom support—The CIO staff is setting a precedent for transition coordination of long distance telecommunications services to the new FTS2001 services contract with WorldCom.

PENDING ISSUES

The DOC staff continue to increase their use of all NCS support service programs, i.e., NCC, Telecommunications Service Priority (TSP) Program, Government Emergency Telecommunications Service (GETS) Program, SHARES, Communications Resource Information Sharing, Priority Access Service and Emergency Response Link (ERLink), especially before and during the Y2K transition. DOC serves as the lead Government agency implementing alternative communications technology with an emphasis on the Internet and electronic commerce. The DOC staff are continuing to expand their use of these services to support not only CIP initiatives but also more regions as they are given national level network access and as the NCS expands the Department's involvement in the strategic plan and the Internet. Cost and human resource factors continue to be key drivers for Departmental participation. Early program involvement by the Department is essential to program success in all Government arenas.

DOC SIGNIFICANT ACCOMPLISHMENTS

- DOC Web page adds new links to virtual Government resources—The CIO staff coordinated the integration of major resources onto the Department Web page to improve access to Government information on the Internet, with links to major sites in the Bureaus and operating units.

- DOC CIO training initiatives foster smarter IT workforce—The CIO staff implemented several new training resources on the Department's Web page to support IT training of the Commerce workforce.

- NOAA NWS Solar Max initiative available on Web site for radiation alerts—The NWS staff installed several new solar radiation sites nationwide to track solar radiation data, analyze the effects of intense solar radiation, predict occurrence, and report alerts on the Solar Max Web page.

- NOAA NWS severe storm warnings have five new alert levels—The NWS has implemented a new alert reporting scheme, numbered 1 to 5, to indicate the severity of storms on land and in space, and to indicate the severity of a variety of environmental conditions that can harm health and property.

- NOAA NWS digital products updated ERLink with warnings—The NWS has provided links to the ERLink server to provide information to emergency planners on the alerts dealing with weather and solar radiation reporting.

- DOC CIO alerting capability included in IT security organization—The CIO staff has implemented a new program capability to report cyber events to IT staff groups throughout Commerce, including alerts that may indicate vulnerability of information systems, equipment, and software as well as Web-accessible sites.

- DOC CIO analysis program completes review of critical assets—The CIO staff completed the first phase effort to review the critical program and facility assets of the Department and operating units as part of the vulnerability assessment in the CIP initiative under PDD-63.

- NOAA NWS provides new three-dimensional (3-D) weather reporting to Web access—The NWS implemented a new 3-D graphics product that allows emergency planners to view the location and dimensions of storms and other weather phenomena from the NOAA Web page.

- NOAA NWS upgrades national weather radio to 526 stations online—The NWS initiated upgrades to the National Weather Radio program with a new system and equipment technology and expanded its coverage to 526 stations that continuously report the current weather and local alerts to regional areas.

- NOAA NWS capabilities receive new super computers for predictions—The NWS staff installed new super computers at its data computing center to enhance the weather modeling and prediction capabilities used by the NWS to track the path of storms and other weather phenomena.

- The DOC revitalizes its continuity of operations (COOP) plans to include critical assets and functions—The DOC Office of the Secretary initiated an effort to revitalize the COOP planning and reporting process for ensuring that operating units plan for emergency preparedness and relocation requirements.

- DOC establishes CIP information sharing and analysis center (ISAC) for information and communications sector—The DOC staffs within Commerce NTIA established a new ISAC to help coordinate the Department and industry efforts under the CIP program per PDD-63.

- DOC increases use of NCS NS / EP support programs during Y2K—The Commerce Department and its operating units significantly increased their use of the NCS NS / EP support programs when preparing for the Y2K transition, such as TSP, GETS, ERLink, and SHARES, and plan to continue these activities under the CIP initiative.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

DHHS CURRENT/ ONGOING ACTIVITIES

During numerous fiscal year (FY) 2000 deployments, the Department of Health and Human Services (DHHS) was grateful to the National Communications System (NCS) for the ability to utilize Shared Resources High Frequency Radio (SHARES) Program stations in the affected areas to aid in coordinating telecommunications resources. DHHS is also thankful for the Communications Resources Information Sharing initiative that the NCS has continued to support.

DHHS continues to utilize and expand its ultra high frequency modulation radio assets. Other agencies have graciously made frequencies available for National Disaster Medical System (NDMS) use.

DHHS SIGNIFICANT ACCOMPLISHMENTS

During FY 2000, DHHS utilized the SHARES program in the development of our field-deployable high frequency (HF) radio kits. Civil Air Patrol and Military Affiliate Radio System stations were particularly helpful with on-the-air testing.

SHARES also aided in linking the DHHS Office of Emergency Preparedness (OEP) with the field command post of the NDMS during the Federal response to the flooding in Tarboro, NC.

HHS HF radio stations were on the air to support the Government's year 2000 efforts, participated in the National Emergency Coordination Network tests conducted by Federal Emergency Management Agency (FEMA), and took part in the weekly SHARES Coordination Network tests conducted by NCS.

In addition to the OEP / NDMS, several operating divisions of the DHHS are considering adding HF radio systems to their Continuity of Operations plans. Automatic Link Establishment (ALE) technology makes the use of 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 leadership demonstrated by FEMA in evaluating the performance of certain HF ALE equipment, and for its 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 developed their communications and electronics skills through their amateur radio experience. During exercises and actual deployments, the amateur radio community 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 Initiative deals with improving command and control communications activities (including secure communications), and ensuring continuity of all Government operations. The DOT continues to participate actively 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 to include:

Government Emergency Telecommunications System (GETS)

The Department has been involved with the NCS GETS program since its inception. DOT organizations account for over 3,200 of the total GETS cards that the NCS Program Office issues. 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 continues to progress in its transition from Federal Telecommunications System (FTS) 2000 to FTS2001 across all DOT Operating Administrations (OA). 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.

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 Program.

DOT SIGNIFICANT ACCOMPLISHMENTS

A connection to the Federal Emergency Management Agency's (FEMA) National Alert and Warning System (NAWAS) was successfully installed, tested, and exercised in the DOT Secretary's Crisis Management Center (CMC). NAWAS will further augment the DOT CMC staff capabilities for alerting, tracking, and responding to disasters.

The Department completed installation of connections to the Secret Internet Protocol Router Network (SIPRNET) classified communications system in the DOT CMC, the Maritime Administration's communications center, and in the DOT Office of Intelligence and Security. This was accomplished before the Year 2000 rollover. SIPRNET access will greatly enhance the Department's ability to collect and disseminate important intelligence information.

DOT participated in the Top Officials 2000 exercise co-sponsored by FEMA and the Department of Justice. This exercise was designed to assess the Nation's crisis and consequence management capacity under extraordinarily stressful conditions, caused by a series of terrorist incidents using weapons of mass destruction. This exercise also allowed DOT to test its Federal Response Plan emergency support function #1 responsibilities.

DEPARTMENT OF ENERGY (DOE)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Idaho National Engineering and Environmental Laboratory

The Idaho National Engineering and Environmental Laboratory (INEEL) Telecommunications Unit completed negotiations with Qwest for renewal of OC12 services. The new contract is placed to provide leased voice and data services to augment the existing INEEL network service and provide survivability for the Government-owned fiber network. It will save the INEEL $2,030 a month and $121,800 over the contract term.

The existing General Dynamics contract was also modified to improve responsiveness to INEEL restoration of communications services. This modification provides one-source General Dynamics nationwide corporate resources to augment the existing personnel, material, and maintenance capability if a major failure to the network occurs. A planned upgrade to switched data services will enhance security of the INEEL data network.

INEEL's external router capability is undergoing a continual review to identify unnecessary services and port usage. The firewall software has been upgraded with the latest security enhancements to deter malicious interruption or modifications to existing services. The INEEL paging service within the greater southeast Idaho region will be expanded in the first quarter of fiscal year (FY) 2001 to broaden the paging area for recall of key emergency personnel.

Oak Ridge Operations Office

The Oak Ridge Operations Office (OR) is planning a wide area radio system to replace the existing conventional analog, wideband very high frequency (VHF) mobile radio system with a new, trunked-capable narrowband ultra high frequency mobile radio system. The system will provide a central infrastructure for the OR Reservation. At the present time, different networks are required at each of the plants with little or no capability of intersite / reservation connectivity. A safety committee formed to study reservation-wide mobile communications concluded this type of system would resolve safety issues. Several emergency preparedness and mutual aid issues will also be resolved with the implementation of this system. OR is still implementing Public Key Infrastructure. When implemented, OR will support encrypted data network traffic.

Savannah River Operations Office

The Savannah River Operations Office (SR) has transitioned 85 percent of its wideband VHF radio equipment, including all emergency services and utilities radio equipment, to a Motorola narrowband VHF trunking system. Eleven of 13 trunking repeater channels have been brought online. Migration to the radio trunking system will be completed during FY 2001. The current development of a remote monitoring and notification system for SR's radio tower facilities will monitor and report power outages, generator status, radio equipment status, and other facility conditions to minimize downtime and increase system reliability.

The SR has completed installation of an alternate-paging transmitter on a separate tower to provide redundancy for the site's primary paging transmitter. The SR paging system is the primary means of notification / call-in for Emergency Response Organization personnel. SR replaced all secure telephone unit III devices in FY 2000 and conducted a telecommunications disaster recovery drill in December 1999 that revealed no major issues.

An Emergency Alert System (EAS) purchased to deliver emergency alerts on the site's cable television system was scheduled for installation in July 2000. The DOE-NET digital signal (DS)-1 circuit will be upgraded to a DS-3 circuit by August 2000, which will provide enhanced data communications with Headquarters (HQ) and other DOE sites.

SR connected two SmartRing nodes and two 5ESS switches to the site's fiber ring. The two 5ESS switches were upgraded from generic 5E12 to 5E13 and are scheduled for upgrade to generic 5E14 by September 2000.

Nevada Operations Office

The Nevada Operations Office upgraded the Northern Telecom SL-100 telephone switch operating system from MSL-08 to MSL-10. Two AT&T cellular telephone sites were installed and are operational at the Nevada Test Site, providing alternative commercial services to the major population areas.

Southwestern Power Administration

Southwestern Power Administration has purchased six satellite telephones as backup for existing analog mobile radio, analog and digital microwave, and fiber optic communications systems. These satellite telephones and communications systems are used by Southwestern to control the operation and maintenance activities of its power transmission system, and to allow communications between Southwestern's HQ office, operations and dispatch center, maintenance offices, two U.S. Army Corps of Engineers District power operation sites, and Southwest Power Pool.

Headquarters Emergency Communications Network

The Headquarters Emergency Communications Network (ECN) is an integral part of DOE's emergency management system. The ECN links the DOE HQ Emergency Operations Center and 21 data / 18 video nodes, including all major DOE sites, DOE's deployable radiological emergency response assets, and other Government agencies throughout the United States. Planned expansion provides for up to 51 nodes. The Emergency Satellite Communications System and International Maritime Satellite Organization provide ECN backup.

Last year the ECN added an unclassified link to the Ministry of the Russian Federation for Atomic Energy (MINATOM). The MINATOM link was used successfully in support of the year 2000 rollover. The ECN supported numerous emergency responses and meetings at the executive, interagency, and international levels. Additionally, ECN and satellite capabilities were used to support distance learning activities of the newly established Emergency Operations Training Academy.

DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Telecommunications System 2001 Transition

The Department of Veterans Affairs (VA) is aggressively pursuing the transition to the General Services Administration's (GSA) Federal Telecommunications System (FTS) 2001 contracts. The transition, involving virtually all of VA's major voice and data functions, is planned to have the least impact on service to veterans. The strategy, developed with the assistance of Booz • Allen & Hamilton, helped anticipate many of the issues faced during the transition from FTS2000.

VA used "700" prefix telephone numbers extensively during the FTS2000 contract. In concert with GSA, VA established a gateway to allow VA sites transitioned to FTS2001 to call "700" numbers of sites still on FTS2000. The gateway ensures continuity of critical communication during the transition period.

VA's FTS2001 vendor, Sprint, physically surveyed all major sites to catalog telecommunications assets and incorporate them in the detailed plan for site cutover. Procedures were developed with Sprint to identify a fallback in the event of a failed cutover. The implementation schedule is tracked daily; and lessons learned from the site cutovers are shared among customers, VA transition managers, and Sprint.

VA's approach to the transition process is consistent with its mission of providing high-quality service to the Nation's veterans.

Veterans Health Administration Wide Area Networking

The 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 in the event of a loss of connectivity at one VISN site, 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 Telecommunications System

The VA Nationwide Telecommunications System (VANTS) provides audio and video teleconferencing services to the entire VA. VANTS services are primarily used 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 the Department of Defense.

With the recent bridge expansion, the video teleconferencing section of VANTS can accommodate approximately 64 participants at the 384 bandwidth. The video bridging services run over the Integrated Services Digital Network and have connections to four different 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. This technology allows VA employees to conduct "face-to-face" meetings without the time and expense of travel.

The audio section of VANTS has 576 audio ports for voice teleconferencing. Participants are provided toll-free numbers for easy access from any telephone within the continental United States.

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 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 (IG) Network

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

The new very high frequency network integrates the investigative arm of the IG's Office with Federal and civilian law enforcement services nationwide and 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 6 or more hours now can be completed in about 20 minutes, allowing two to three technicians to do the work that 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 that 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 Office of Communications and Agency Technology Services, under the Deputy Director of Administration, 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 requirements.

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 Telecommunications Service (GETS), 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 operation, 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 to expand CIA-wide participation in NS/EP GETS activities
- 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 U.S. 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) 2000, 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 activity 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 declarations. FEMA's Mobile Emergency Response Support (MERS) detachments deployed to 63 declared disasters. Additionally, FEMA participated in approximately 90 communications tests and provided telecommunications support to special events, such as a MERS display at the King County Emergency Management Communications Academy in Seattle, Washington.

The National Emergency Management System (NEMIS) is an integrated system providing FEMA, States, and other Federal departments and agencies with automation to perform disaster and nondisaster operations. 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 2000, 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.

Project Impact participation by local governments increased to nearly 200 communities. Project Impact operates on a common-sense damage-reduction approach, basing its work on preventive actions at the local level, private sector participation, and long-term investments.

The National Interagency Emergency Operations Center, at FEMA Headquarters, was activated on a 24-hours-a-day basis, for the Year 2000 (Y2K) rollover. Also, FEMA staff participated in the Y2K and the leap year rollovers at the Information Coordination Center. Both rollovers occurred without incident.

FEMA's Internet home page continues to be popular. In FY 2000, an average of 617,537 pages were viewed weekly. There was significant expansion of information published on FEMA's Web site. Information on flood plain hazard mapping and the Dam Safety section were expanded. Information on the National Flood Insurance Program targeted for homeowners, insurance agents, and lenders was also expanded.

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. The Director develops policy and plans, monitors programs for joint C4 systems, and ensures adequate C4 support to commanders-in-chief, the National Command Authorities, and all joint warfighters for joint and combined military operations. The Director leads the C4 community, conceptualizes future C4 systems architectures, and provides direction to improve joint C4 systems. The Director oversees C4 support for the National Military Command System.

TELECOMMUNICATIONS STAFF ORGANIZATION

The C4 Systems Directorate (J-6) consists of a Director, a Vice Director, three Deputy Directors (C4 Command Operations, C4 Systems, and C4 Technology), and appropriate 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)

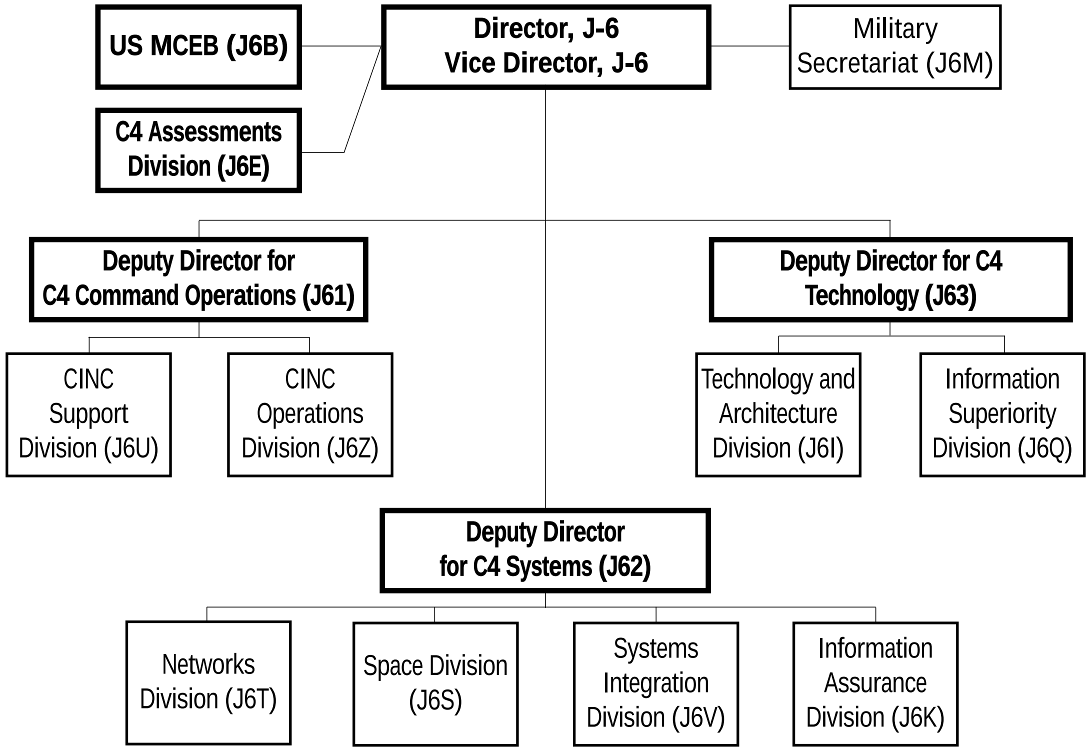
CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

(Refer to DOD Section)

PENDING ISSUES

(Refer to DOD Section)

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE


US MCEB (J6B)
Director, J-6
Vice Director, J-6
Military Secretariat (J6M)
C4 Assessments Division (J6E)
Deputy Director for C4 Command Operations (J61)
Deputy Director for C4 Technology (J63)
CINC Support Division (J6U)
CINC Operations Division (J6Z)
Technology and Architecture Division (J6I)
Information Superiority Division (J6Q)
Deputy Director for C4 Systems (J62)
Networks Division (J6T)
Space Division (J6S)
Systems Integration Division (J6V)
Information Assurance Division (J6K)

GENERAL SERVICES ADMINISTRATION (GSA)

MISSION

The General Services Administration (GSA), Federal Technology Service NS/EP mission is to provide network services and information technology (IT) solutions to ensure federally owned or managed domestic communications facilities and services meet the NS/EP of the Federal civilian departments, agencies, and entities as directed by Executive Order 12474. GSA also provides a Federal Emergency Communications Coordinator to lead Emergency Support Function #2 (Communications) as directed by the National Plan for Telecommunications Support in Non-Wartime Emergencies and the Federal Response Plan. This responsibility includes coordinating telecommunications service, provisioning network services and IT, policy development, and Federal regulatory responsibilities.

CURRENT/ONGOING ACTIVITIES

- The GSA Federal Technology Service provides a full range of network services and IT solutions and stands ready to meet the current and future needs of the Federal Government with globally positioned resources, services, and solutions. FTS and NS/EP services are also available to tribal governments as well as State and local governments with the sponsorship of 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, Internet access, technical services support, and information security services.
- The Federal Technology Service continues to support the National Communications System (NCS) by providing one detailee to the National Coordinating Center (NCC) and 11 Regional Emergency Communications Managers and Federal Emergency Communications Coordinators.
- The Federal Technology Service provides agencies access to information on all FTS services, including disaster support, contingency planning, and continuity of operations services through the GSA FTS home page (http://fts.gsa.gov).
- The Federal Technology Service has established contract vehicles in response to Presidential Decision Directive 63 (PDD-63) mandates and emergency requirements.
- The Federal Technology Service Emergency Relocation Center is collocated with the NCS, NCC relocation center, and the Federal Emergency Management Agency (FEMA) Network Operations Center, located at FEMA's Mount Weather facility.

GSA SIGNIFICANT ACCOMPLISHMENTS

The Federal Telecommunications System 2001 contract offers competitively priced, state-of-the-art, comprehensive NS/EP telecommunications services worldwide. It offers domestic and international long distance voice and data telecommunications services. Managed network services and managed secure services increase the reliability and security of agencies' voice and data networks.

The Metropolitan Area Acquisition (MAA) contract offers a wide variety of local voice and data services, including the most current, commercially available enhanced telecommunication services and technologies with great savings potential. The following cities have MAA contracts: Minneapolis, MN; Baltimore, MD; Buffalo, NY; Cincinnati, OH; Cleveland, OH; Los Angeles, CA; Atlanta, GA; Miami, FL; Indianapolis, IN; St. Louis, MO; Dallas, TX; Denver, CO; New York, NY; Chicago, IL; Boise, ID; San Francisco, CA; Albuquerque, NM; Boston, MA; Philadelphia, PA; and New Orleans, LA.

The GSA Safeguard contract provides services and products for strengthening the Nation's defense against unconventional threats to the United States, including terrorist attacks, attacks on the critical infrastructure, and cyber attacks.

GSA provided NS/EP telecommunications, housing, security, and resources support to FEMA and other Federal departments and agencies, including State and local governments, during federally declared emergencies throughout the United States, including the fires in New Mexico.

Access Certificates for Electronic Services (ACES) facilitates secure online access by the public to Government information and services. ACES provides a governmentwide public key infrastructure (PKI) with strong authentication using identity-based digital signature certificates. PKI is useful to achieve improved access control, data integrity, and technical nonrepudiation. ACES was designed to reduce the up-front cost associated with establishing a PKI and further reduces costs to agencies by aggregating Government requirements.

The GSA Federal Technology Service Applications 'n Support for Widely-diverse EndUser Requirements (Answer) is a multiple vendor contract vehicle designed to provide a full range of IT support services.

GSA's Federal Technology Service manages the Federal Computer Incident Response Capability (FedCIRC). In support of PDD-63, "Policy on Critical Infrastructure Protection," FedCIRC provides a central focal point for incident reporting, handling, prevention, and recognition. The purpose is to ensure that the Government has available the critical services needed to withstand or quickly recover from attacks against its information infrastructure.

continued on next page

GSA SIGNIFICANT ACCOMPLISHMENTS *continued*

GSA's Federal Technology Service manages the Blue Pages Project, a governmentwide effort to make the Federal listings in commercial telephone directories easier for the public to understand and to use. This project will culminate in year 2000 as the new format is implemented across the United States.

Federal Wireless Telecommunications Services provides nationwide analog / digital cellular voice and data service. Other services include Cellular Digital Packet Data and mobile Web. Nationwide and international paging services include one-way, two-way, and advanced messaging service.

Electronic Commerce, Internet and Email Access provides value-added electronic commerce, Internet access, and electronic mail access services in the 48 contiguous States, Alaska, Hawaii, and the District of Columbia.

Satellite Services: GSA Federal Technology Service has wide variety of contracts that offer fixed, mobile, and broadcast satellite services that allow for communication from remote or isolated locations and support distance learning.

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. The Associate Administrator for Space Flight also assigned NASA's Lead Center role for Space Operations to the Johnson Space Center, Houston, Texas. The Director, Space Operations Management Office (SOMO) serves as the functional manager for agencywide space operations communications.

NASA's George C. Marshall Space Flight Center, located in Huntsville, Alabama, maintains Lead Center responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network, one of several operational elements of SOMO.

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 Service, Interagency Committee on Search and Rescue, and the NCS Technology and Standards Accomplishments.

NASA NS/EP TELECOMMUNICATIONS ASSETS

NASA 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 & Education Network is NASA's component to the Next Generation Internet initiative. It operates as a test bed for developing Internet technologies, applications, and networking tools.

NASA SIGNIFICANT ACCOMPLISHMENTS

Migrated four previously autonomous networks into standard service offerings under one 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.

Migrated voice teleconferencing services from Government-owned and operated facilities to commercially provided services. Initiated transition of voice and video services from the Federal Telecommunications System (FTS) 2000 contract to the FTS2001 contract.

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 plant control rooms, emergency operations facilities, and regional incident response centers. This connectivity ensures immediate notification to the NRC Operations Center of unusual occurrences and provides relevant information during accidents/events at NRC licensed facilities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Telecommunications System (FTS) 2000 provides reliable service to all nuclear power plants, associated emergency operations facilities, and major NRC fuel facilities. NRC provides circuits for seven emergency operations functions by multiple lines. The NRC continued to work with the National Communications System (NCS) on an option involving use of Government Emergency Telecommunications Service (GETS) to provide access to long distance service in lieu of FTS2000 at nuclear power plants. The NRC has completed its evaluation of options for post-FTS 2000 emergency telecommunications. The current FTS2000 service will be transitioned to a combination of utility-provided circuits and FTS2001 service. GETS will figure prominently in this long-term emergency telecommunication solution.

NRC has continued to participate in the Emergency Response Link (ERLink) program, which provides a secure, Internet-based platform for exchanging emergency response information. Over the last year, NRC provided information to ERLink supporting two emergency exercises.

The NCS supported the NRC Year 2000 (Y2K) contingency planning and response in a number of ways. NRC has established a node on the National Telecommunications Coordinating Network to better coordinate NS/EP telecommunications issues with NCS. The NRC sponsored all commercial nuclear power plants and major fuel cycle facilities for GETS access as part of the Y2K contingency plan effort. The NRC will continue to sponsor these sites for GETS access to support the Emergency Telecommunications System.

NRC SIGNIFICANT ACCOMPLISHMENTS

NRC used ERLink in two nuclear power plant emergency drills to transfer information such as status summaries and press releases.

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.

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 Resources Board. Thus, among other things, NTIA advises and assists the President in the administration of a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support national security or emergency preparedness 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: (1) SPECTRUM XXI Version 2.0, the follow-on spectrum management software to the Initial Operating Capability (Version 1.0), for use by all Federal spectrum managers; (2) EL_SID Alpha Version, an icon-based, graphical user interface supported by sophisticated logic that Federal agencies will use to develop and submit spectrum certification requests to NTIA; (3) spectrum requirements system prototype for integration into SPECTRUM XXI; (4) statistical database viewer prototype to display various spectrum information in several ways, including allocation tables and associated spectrum-use statistics, and other automated capabilities.

- Developed a computer-accessible, secure communications mechanism for Federal spectrum managers to: (1) search, select, sort, and obtain all information used in the Interdepartment Radio Advisory Council (IRAC) process; (2) view and obtain the latest agenda material (agendas, minutes, and documents on the agenda) used in the IRAC process; and (3) transfer information electronically to NTIA for inclusion in the IRAC process.

- Completed the electronic imaging, optical-character reading, archiving, indexing, and transferring to 60 CD-ROMs all of the archived IRAC documents for the past 78 years; developed CD-ROM-based search software; produced and distributed complete CD-ROM sets to all IRAC members.

- Completed transition to workstation environment from antiquated mainframe computer for processing all Federal frequency assignment requests and actions, thereby enabling more effective and efficient spectrum support for Federal spectrum managers.

In addition, the NTIA/OSM—

- Participated in National Emergency Management Team training activities

- Participated in Government Emergency Telecommunications Service (GETS) User Council activities as well as provided GETS user authorizations to new NTIA emergency essential personnel

- Participated in various activities of the President's National Security Telecommunications Advisory Committee

- Participated in National Communications System (NCS) Committee of Principals and Council of Representatives activities

- Participated in NCS Shared Resources High Frequency Coordination Network Interoperability Working Group activities

- 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

Represented the U.S. Government on many spectrum policy matters at the World Radio Conference 2000 in Geneva, Switzerland, as part of the U.S. delegation

Served as the lead agency for the Information and Communications (I&C) sector of the Nation's critical infrastructures; as such, established the I&C Sector Working Group and its five subcommittees to promote information sharing and coordinated action 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, support to NS/EP-related activities is split between two organizations. The Technology and Systems Organization plans and operates the telecommunications systems and networks that link Agency elements worldwide and connect the Agency to other Government services.

The Information Systems Security Organization develops information security (INFOSEC) products and provides services to enhance the security of telecommunications systems. Both organizations collaborate closely with the military services and defense agencies in support of overall DOD initiatives. In accordance with NSA'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 represent a broad range of users of the National Information Infrastructure and the critical infrastructure communities. NSA's information security activities include a close working relationship with the National Institute of Standards and Technology.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- Supported the ongoing activities of DOD's Defense-wide Information Assurance Program (DIAP) to provide central oversight for and coordinate DOD Information Assurance (IA) activities. Key elements of the DIAP are people, operations, and technology. Specific new 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, NSA was a key contributor to the overall architectural guidance for the DIAP. The IA Technical Framework was updated this past year. New material includes system security methodology, defending the enclave boundary, defending the computing environment, support infrastructures, and IA for tactical environments. A new version of the framework will be published in September 2000 focused on Federal Government use, not just DOD.

- Developed a high assurance, robust Key Management Infrastructure (KMI) for the national security community. Also began to acquire a new KMI with a centralized service node to simplify key ordering and management operations.

- 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. Sponsored nearly 20 protection profiles for products and systems. These include protection profiles on firewalls, virtual private networks, peripheral sharing switches, remote access, operating systems, single-level Web, smart cards, intrusion detection systems, and public key infrastructure protection.

- Provided services, including threat, vulnerability, and risk assessments, to member organizations that lead to security guidance and advice, especially with respect to dependence on the critical infrastructure and Presidential Decesion Directive 63 responsibilities.

- Assumed, in partnership with Defense Information Systems Agency, leadership of the DOD Public Key Infrastructure Program Management Office. The Class 3 Release 2 infrastructure went operational in July 2000. As of this writing, more than 40,000 Class 3 Public Key Certificates have been issued in DOD. In addition, modifications and continued deployment of the Defense Message System have occurred.

- Continued support of the Critical Infrastructure Assurance Program. Special focus was provided in the area of new development of intrusion detection tools and techniques.

- Continued to lead the activities of the National Security Telecommunications Information Systems Security Committee for Assistant Secretary of Defense for Controls, Communications, and Intelligence.

- 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 information technology vendors to completely 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 collectively provide:

  —Writer-to-reader information security services, including data integrity and access control

  —Network protection technologies (e.g., asynchronous transfer mode 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 containing different sensitivity levels.

- Provided security guidance for ongoing National Communications System programs, including Government Emergency Telecommunications Service and Emergency Response Link.

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 to carry out if a national emergency or other declared disaster occurs. Instead, the USPS designs telecommunications systems and services to support day-to-day organizational, administrative, and operational mission requirements. Telecommunications facilities dedicated specifically to NS/EP are therefore limited in scope.

USPS SIGNIFICANT ACCOMPLISHMENTS

The following accomplishments will enhance the ability of USPS to support the overall mission and provide a robust Continuity of Business (COB) program:

- The Postal Service has aggressively addressed Year 2000 (Y2K) compliance on a national scale. During fiscal year (FY) 1999 and FY 2000, USPS commissioned an Executive Council to manage the Y2K Program Plan. USPS remediated more than 500 business computer applications, comprising more than 100 million lines of code; 38,000 facilities; 120,000 workstations and servers; 150,000 mail processing equipment components; 200,000 infrastructure components; 2,000 interfaces to key customers and suppliers; and the readiness of almost 1,000 critical suppliers and service suppliers. The Postal Service reviewed all network infrastructure components, including data network transmission control protocol/Internet protocol (TCP/IP) routers, electronic digital private branch exchange (EDPBX) and electronic key telephone systems (EKTS), to ensure Y2K compliance. Y2K compliance upgrades for over 250 EDPBX systems and over 160 key telephone systems were completed. Throughout FY 2000, the USPS implemented over 30 EDPBX telephone systems and upgraded an additional 15 systems. Also during FY 2000, more than 180 new EKTSs were installed; and more than 25 new structured wiring systems were implemented for local area network (LAN) infrastructure.

- During FY 2000, the USPS continued the rollout of the Associate Office Infrastructure (AOI) program to support the national deployment of the Point of Service (POS) systems. The Distributed Systems/Central Management Facility (DS/CMF) was opened in FY 1998 and staffed in Raleigh, NC, to provide a full range of support and remote management services for Novell and NT servers. The USPS met the goal to implement this standard service suite at over 8,000 USPS retail locations by the end of FY 2000. USPS currently operates and maintains the world's largest corporate intranet and Novell Netware Directory Structure (NDS), with over 265,000 network objects in the NDS tree, and over 1,300 Novell servers providing access for over 150,000 user accounts.

- In support of the AOI project, Telecommunications Services implemented over 5,500 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 increased the USPS Managed Network Services (MNS) national data network backup reliability from less than 85 percent to greater than 99 percent, compared to the previous ISDN backup service. This backup architecture eliminates reliance on local exchange carrier-based transport (last mile) from the remote facility to the serving wire center of the Public Switched Network.

- In support of the POS implementation, the USPS Telecommunication Services Radio Frequency and Wireless Program Team implemented more than 2,500 VSATs as Primary communications systems at selected Small Associate (retail and delivery) Offices. The VSAT systems, once installed, will be engineered to provide TCP/IP-based LAN and wide area network data networking capability for all local telecommunications requirements in the retail and delivery offices. Quickly becoming the world's largest and most robust satellite network, these VSAT systems are also being installed in Alaska, Hawaii, and Puerto Rico to provide a seamless continental U.S./outside the continental U.S. satellite network architecture. It is anticipated that 8,000 additional VSAT (as primary) systems will be installed beginning in FY 2001. VSAT systems have been proven to be a critical component in the USPS COB program, providing a resiliant, reliable, quick-to-implement (within 24 hours), satellite-based, broadband (outbound) alternative network access restoration, to be deployed in the event of catastrophic or natural disasters.

- 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 public switched network 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 specific headquarters' field units that have a VSAT system (as described above) installed.

- More than 110,000 switched voice services (SVS) were switched from a previous provider to WorldCom under the USPS MNS contract. Also, over 4,000 SVSs were migrated to the Sprint FTS2001 contract; and over 260 SVSs in Alaska were migrated to the World Com FTS2001 contract.

- For unique field implementations that cannot be installed via traditional structured wiring for LAN connectivity, Telecommunications Services has successfully implemented numerous wireless LAN systems, following the International

continued on next page

USPS SIGNIFICANT ACCOMPLISHMENTS *continued*

Telecommunication Union (ITU) 802.11 and 802.11b standards, for 3 Mb/s and 11 Mb/s requirements respectively. In addition, USPS has settled on the ITU 802.11b standard for wireless extensions of traditional 10/100 BaseT 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 carrying out daily computing and network operational responsibilities, the Information Systems organization certified new national applications (certifying more than 150 in FY 2000) and performed interoperability testing of commercial off-the-shelf products on standard computing system platforms.

■ Throughout FY 2000, significant efforts have been undertaken to ready the agency to shift from a Microsoft NT Domain Name Server-based structure to a Windows 2000 Active Directory architecture.

■ During FY 2000, the USPS completed the annual update to the USPS Infrastructure Tool Kit and the Postal Computing Environment Handbook. These documents provide a standardized IT architecture that defines the evolving computing and telecommunications infrastructure. This architecture follows a utility company model to focus on the infrastructure required to deliver a standard suite of services to all users located in field facilities.

■ 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, awarded to Com-Net Ericsson during FY 2000, provides the most comprehensive handheld, base station, and repeater LMR systems solution package within the civilian Federal arena.

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 1,055 active TSP assignments.

The FRB continues to sponsor a TSP assignment for circuits used for 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. During the Year 2000 (Y2K) rollover, the FRB expanded its use of GETS to include subscriptions for the additional personnel monitoring critical telecommunications assets and payment systems during this period. In addition, the FRB sponsored GETS subscriptions for SWIFT and CHIPS.

The FRB established an account with Emergency Response Link (ERLink) to retrieve information associated with telecommunications outages. The FRB used ERLink to monitor telecommunications outages during the Y2K rollover and continues to use it to retrieve information in support of disaster response operations.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Much of what the Federal Communications Commission (FCC) does will either directly or indirectly affect the NS/EP telecommunications activities of other Government departments and agencies. The following are some of the actions the FCC has taken during fiscal year 2000.

Year 2000

- Monitored efforts of telecommunications and broadcasting companies to address the Year 2000 (Y2K) problem and worked with their customers to ensure their services would not be disrupted.
- Worked with the International Telecommunication Union (ITU) and other international organizations to inform foreign governments and foreign telecommunications companies about the Y2K problem to facilitate sharing of information on possible solutions.

Providing Communications Opportunities

- Adopted new policies and rules to reduce the need for new area codes.
- Held the first meeting of the Public Safety National Coordination Committee, established for the "Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010 and Establishment of Rules and Requirements for Priority Access Service" (PAS).
- Allowed commercial mobile radio service to offer PAS to public safety personnel at the Federal, State, and local levels to meet NS/EP needs.
- Allowed two regional Bell operating companies to provide long distance service: Bell Atlantic (now Verizon) may provide service in New York only, and SBC in Texas only.
- Issued report on the availability of high-speed and advanced telecommunications services (speeds in both directions of at least 200 kbps) showing more than 2.8 million subscribers as of December 31, 1999 (an increase from 375,000 in late 1998).
- The 2000 World Radio Communications Conference included two major agreements: facilitate development of technology for wireless phones that can call to anywhere, from anywhere, and can access the Internet from anywhere on Earth; and develop policies to maximize spectrum use to provide new terrestrial and satellite services to people worldwide.
- Adopted rules creating a new, noncommercial, low-power FM radio service consisting of stations with maximum power levels of 10 watts, reaching an area with a radius of between 1 and 2 miles; and 100 watts, reaching an area with a radius of approximately 3½ miles.
- Mandated nationwide implementation of 711 access to telecommunications relay services to enable people with hearing or speech impairments to hold conversations with people without such impairments. Also assigned easy-to-remember three-digit dialing codes for quick access to community information and referral services (# 211), and traffic and transportation information (# 511).
- Promoted local telephone competition and consumer choice by ensuring that competitors can link to residential customers by leasing portions of the existing telephone network.
- Conducted special proceedings to focus attention on bringing both basic and advanced telecommunications services to tribal lands and launched a new Web site dedicated to Indian initiatives.
- Revised rules to promote public safety and competition among 911 wireless equipment manufacturers by enabling handset-based methods of providing location information for 911 calls to compete in a reasonable way with network-based solutions.

Mergers

- Approved mergers between Bell Atlantic and GTE; U S West and Qwest; and SBC Communications, Inc. and Ameritech Corporation. Encouraged infrastructure investment through competition by requiring rural digital subscriber line deployment and other procompetitive measures in the SBC-Ameritech merger. Conditions on the merger will create irreversible momentum towards deployment of advanced services and local telephone competition.

Enforcement

- Established an Enforcement Bureau responsible for firm, fast, and flexible enforcement of the Communications Act and the FCC's rules, orders, and authorizations while promoting competition, protecting consumers, and fostering efficient spectrum use while furthering public safety goals.
- Issued notices of apparent liability and/or consent decrees involving voluntary payments to the U.S. Treasury, along with additional consumer protections for violations and alleged violators of the Telephone Consumer Protection Act.
- Issued forfeiture orders to companies engaged in slamming, which is the practice of changing a consumer's telephone service provider without the consumer's express approval. Examples are—

  —Amer-I-Net Services Corporation, $1,360,000

  —Brittan Communications International Corp., $1,000,000

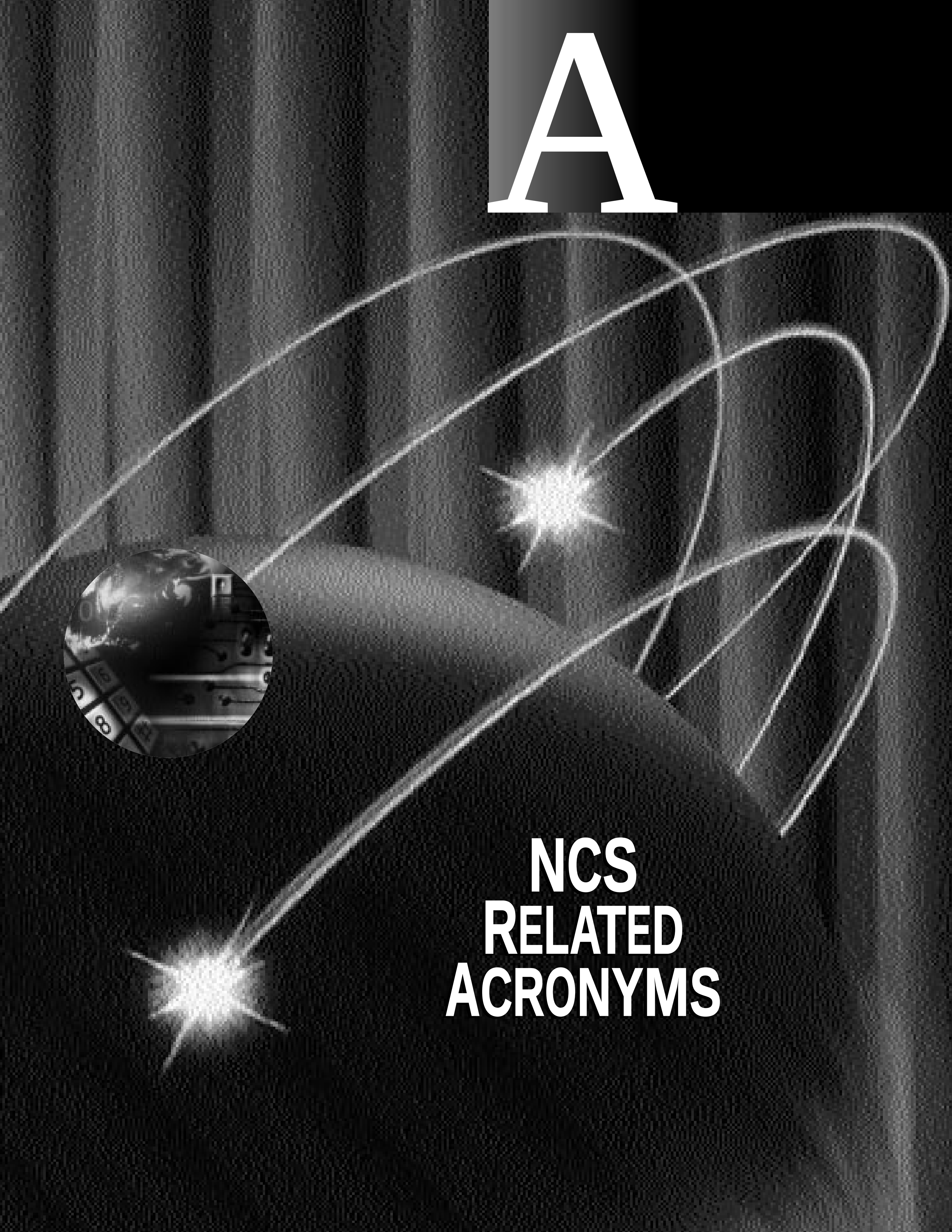
  —Business Discount Plan, Inc., $2,400,000

  —Long Distance Direct, Inc., $2,000,000.
- Again handled more than 1,200 interference complaints from Federal, State, and local public safety emergency officials.

Communications Assistance for Law Enforcement Act of 1994

- Congress enacted the Communications Assistance for Law Enforcement Act of 1994 to ensure that telecommunications carriers' facilities are capable of providing legally authorized electronic surveillance. The FCC required that all capabilities of the Telecommunications Industry Association interim standard (J-STD-025) and six of nine "punch list" capabilities requested by the Department of Justice / Federal Bureau of Investigation be implemented by wireline, cellular, and broadband personal communications services carriers by September 30, 2001. This provision was intended to ensure that law enforcement had the most up-to-date technology to fight crime; however, a Federal court has overturned much of this item.

A



NCS RELATED ACRONYMS

A

NCS RELATED ACRONYMS

3-D	Three-Dimensional

A

ACES	Access Certificates for Electronic Services
ACR	Alternate Carrier Routing
AIN	Advanced Intelligent Network
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
Answer	Applications 'n Support for Widely-Diverse EndUser Requirements
AOI	Associate Office Infrastructure
ASD	Assistant Secretary of Defense
ATG	NCS Advanced Technology Group
ATM	Asynchronous Transfer Mode

B

Bluetooth	Bluetooth Personal Area Network Technology

C

C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computer
CAB	Communications Assessment Branch
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CLEC	Competitive Local Exchange Carrier
CMC	Crisis Management Center
COB	Continuity of Business
COG	Continuity of Government
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
CRIS	Communications Resource Information Sharing

D

DDoS	Distributed Denial of Service
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
DMS	Defense Message System
DOC	Department of Commerce
DOCNet	Department of Commerce Network
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOINET	Department of the Interior Network
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DSL	Digital Subscriber Line
DS / CMF	Distributed Systems / Central Management Facility

E

EAS	Emergency Alert System
ECN	Emergency Communications Network
EDPBX	Electronic Digital Private Branch Exchange
E-Forms	Electronic Forms
EKTS	Electronic Key Telephone System
EM	Emergency Manager
E-Mail	Electronic Mail
E.O.	Executive Order
EOP	Executive Office of the President
EOT	Emergency Operations Team
ERLink	Emergency Response Link
ERT	Emergency Response Training
ESF	Emergency Support Function

F

FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FECC	Federal Emergency Communications Coordinator
FedCIRC	Federal Computer Incident Response Capability
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
GIG	Global Information Grid
GII	Global Information Infrastructure
GN	Ground Network
GPRA	Government Performance and Results Act
GSA	General Services Administration
GTF	Globalization Task Force

H

HAPS	High-Altitude Platform Stations
HF	High Frequency
HPC	High Probability of Completion
HQ	Headquarters

I

I&C	Information and Communications
IC	Integration Contract
ICC	Information Coordination Center
IES	Industry Executive Subcommittee
IG	Inspector General
IIAM	Information Integrity, Analysis, and Modeling
IMA	Individual Mobilization Augmentee
IMT-2000	International Mobile Telecommunications-2000
INEEL	Idaho National Engineering and Environmental Laboratory
INFOSEC	Information Security
INMARSAT	International Maritime Satellite Organization

INS	Immigration and Naturalization Service
IOC	Initial Operational Capability
IP	Internet Protocol
IRAC	Interdepartment Radio Advisory Council
ISAC	Information Sharing and Analysis Center
ISAS	Information Sharing and Analysis System
IS/CIPTF	Information Sharing/Critical Infrastructure Protection Task Force
ISDN	Integrated Services Digital Network
ISPG	Information Security Policy Group
IT	Information Technology
ITA	International Trade Administration
ITPITF	Information Technology Progress Impact Task Force
ITU	International Telecommunication Union
IWIN	Interactive Weather Information Network
IXC	Interexchange Carrier

J

JABS	Joint Automated Booking System
JCN	Justice Consolidated Network
JS	Joint Staff

K

KMI	Key Management Infrastructure

L

LAN	Local Area Network
LAO	Large Associate Office
LEC	Local Exchange Carrier
LEO	Low-Earth Orbit
LERG	Local Exchange Routing Guide
LMR	Land Mobile Radio
LNP	Local Number Portability
LRWG	Legislative and Regulatory Working Group

M

MAA	Metropolitan Area Acquisition
MERS	Mobile Emergency Response Support
MINATOM	The Ministry of the Russian Federation for Atomic Energy
MNS	Managed Network Services
MSC	Mobile Switching Center

N

NANPA	North American Numbering Plan Administrator
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAWAS	National Alert and Warning System
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NDER	National Defense Executive Reserve
NDMS	National Disaster Medical System
NDS	Netware Directory Structure
NEMIS	National Emergency Management Information System
NGN	Next Generation Network
NIIF	Network Interconnection and Interoperability Forum
NMCS	National Military Command System
NOAA	National Oceanic and Atmospheric Administration
NPA	Numbering Plan Area
NRC	National Regulatory Commission
NRIC	Network Reliability and Interoperability Council
NSA	National Security Agency
NS/EP	National Security And Emergency Preparedness

NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
NTCN	National Telecommunications Coordinating Network
NTIA	National Telecommunications and Information Agency
NWS	National Weather Service

O

OA	Operating Administrations
OC	Oversight Committee
OEP	Office of Emergency Preparedness
OMNCS	Office of the Manager, National Communications System
OPT	Office of Priority Telecommunications
OR	Oak Ridge Operations Office
OSD	Office of Secretary of Defense
OSM	Office of Spectrum Management
OSTP	Office of Science and Technology Policy

P

PACA-E	Priority Access and Channel Allocation-Enhanced
PAS	Priority Access Service
PBX	Private Branch Exchange
PCS	Personal Communications Services
PDD-63	Presidential Decision Directive 63
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PL	Planning Letter
PN	Public Network
POS	Point of Service
POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PSTF	Protecting Systems Task Force
PTS	Priority Telecommunications System

Q

QoS	Quality of Service

R

R&D	Research and Development
RF	Radio Frequency
RISC	Regional Interagency Steering Committee

S

SHARES	Shared Resources High Frequency Radio Program
SIPRNET	Secret Internet Protocol Router Network
SOMO	Space Operations Management Office
SR	Savannah River Operations Office
SS7	Signaling System 7
STU-III	Secure Telephone Unit – Third Generation
SVS	Switched Voice Services

T

TCP / IP	Transmission Control Protocol / Internet Protocol
TESP	Telecommunications Electric Service Priority
TOPOFF	Top Officials
TPOS	Training, Planning, and Operational Support
TREAS	Department of the Treasury
TSP	Telecommunications Service Priority
TSS	Telecommunications Services Staff

U

USDA	United States Department of Agriculture
USIA	United States Information Agency
USPS	United States Postal Service
USSPACECOM	United States Space Command

V

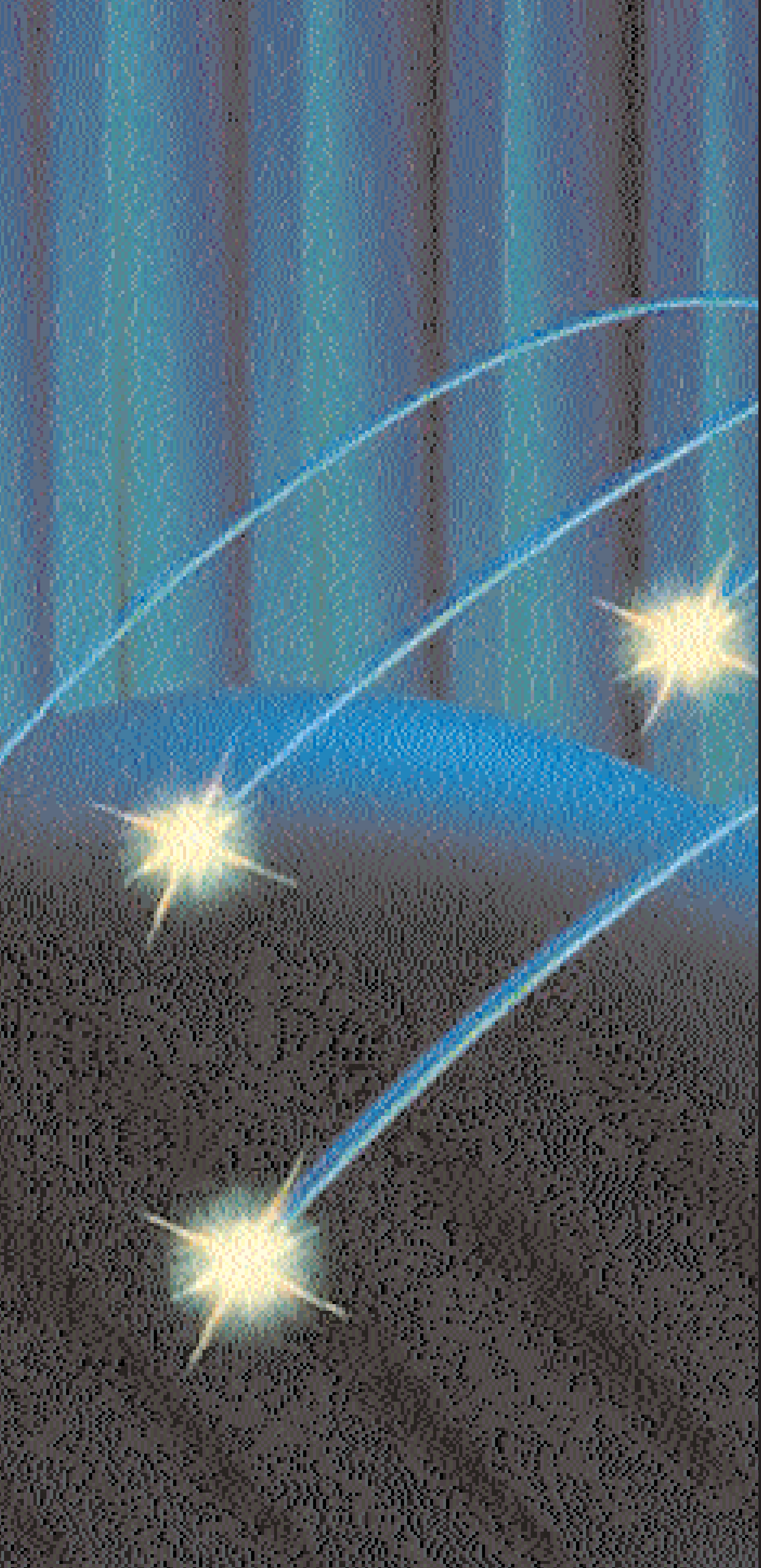
VA	Department of Veterans Affairs
VANTS	Department of Veterans Affairs Nationwide Telecommunications System
VHA	Veterans Health Administration
VHF	Very High Frequency
VISN	Veterans Integrated Service Network
VSAT	Very Small Aperture Terminal

W

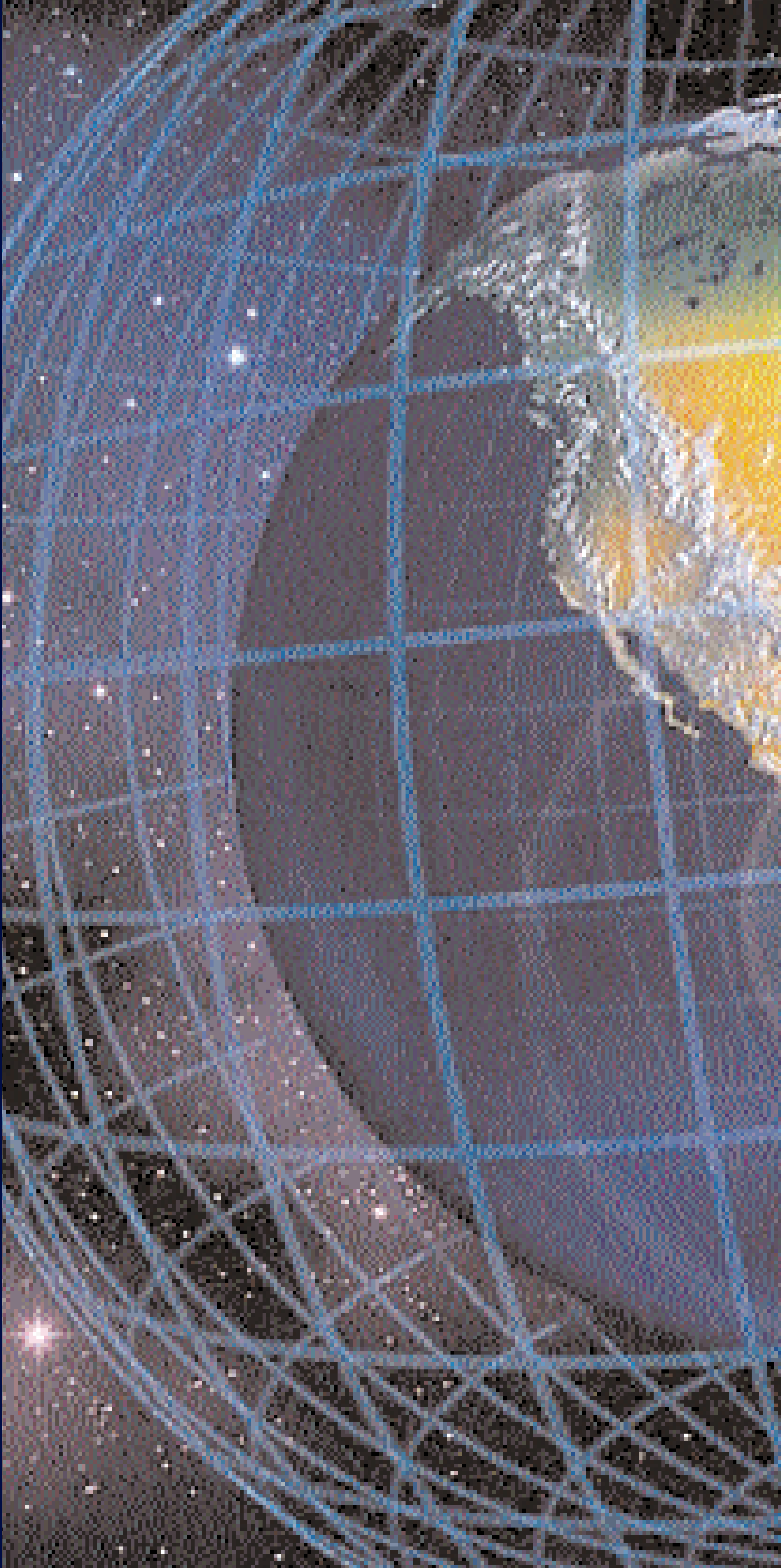
WAN / MAN	Wide Area Network / Metropolitan Area Network

Y

Y2K	Year 2000



After three and one-half decades, the NCS continues to be 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 we can build to ensure that our future communications needs will be met.



NATIONAL COMMUNICATIONS SYSTEM (NCS)

701 South Court House Road
Arlington, Virginia
22204-2198

http://www.ncs.gov