National Communications System

Ensuring Essential Communications for the Homeland

Prepared by the Office of the Manager,
National Communications System

FOREWORD

Over its long and distinguished history, the National Communications System has continued to evolve to keep pace with the ever-changing nature of its national security and emergency preparedness (NS/EP) mission - ensuring the President and the Nation of a NS/EP communications system that responds to any crisis, emergency, or attack, and any needed recovery and reconstitution. Now, after a nearly 40-year relationship with the Department of Defense, the NCS begins a new role with the Department of Homeland Security (DHS). On behalf of Secretary Tom Ridge, who serves as the Executive Agent for the NCS, it is my honor and pleasure to guide the NCS as its new manager.

As a result of the events of September 11, 2001, and in an effort to better protect our Nation against both cyber and physical threats, President George W. Bush created the DHS - the largest reorganization of the Federal Government since 1947. As one of the 22 Federal organizations that joined together to form the new Department, the NCS brings to DHS decades of expertise related to NS/EP activities and an industry - Government partnership that sets the standard for all our critical infrastructure sectors.

The new Department has three primary missions: build the capacity to prevent a terrorist attack; reduce vulnerability to a terrorist attack; and enhance the capacity to respond to an attack. The NCS offers unique, time-tested capabilities and relationships such as the information sharing capabilities of the National Coordinating Center for Telecommunications (NCC), as well as industry based telecommunications policy analysis through the President's National Security Telecommunications Advisory Committee (NSTAC) - assets which directly support DHS in all its assigned missions.

NCS capabilities continue to mature and evolve, allowing DHS to be better prepared to respond to and recover from an attack or disaster, manmade or natural. Wireless Priority Service (WPS) is now available in many cities nationwide, with expectations of expanding coverage through much of the Nation as we move into 2004. We also expect more users of the well-established Government Emergency Telecommunications Service (GETS) and Telecommunications Service Priority (TSP) programs, assisting the Nation's leaders in more effectively communicating during an emergency.

The NCS continues to develop other programs and methods of emergency communication, such as the Critical infrastructure Warning Information Network (CWIN), and pilots such as the Global Early Warning Information System (GEWIS) and Back-Up Dial Tone (BDT) show great promise in providing the Department new ways to communicate among senior leaders of industry and Government.

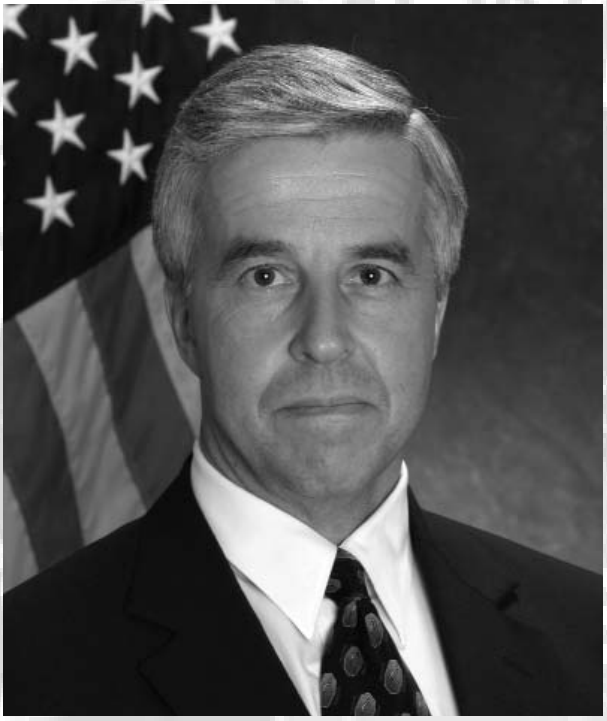
Additionally, the NCS is assessing the potential impact of sector interdependencies between critical infrastructures as part of its role within DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate. Specifically, in close cooperation with the President's NSTAC, the NCS is working with the Financial Services Round Table to evaluate existing telecommunications and financial services interdependencies and promote inter-sector cooperation and partnership. The NSTAC is also analyzing policies and procedures for trusted access to communications facilities to improve physical security practices, and vulnerabilities in the commercial satellite industry that could negatively affect the security and reliability of the Nation's satellite-based communications networks.

With the creation of a single focal point for homeland security and NS/EP within the DHS, the Nation will be better able to anticipate, prepare for, and respond to any future incidents. However, the challenges ahead are substantial. Meeting those challenges requires a full-scale partnership and engagement with the private sector, State and local Government, and the public. I am confident in the NCS' ability to continue fostering partnerships with other Government entities and the telecommunications industry and I look forward to the exciting year ahead.

Robert P. Liscouski
Manager


NATIONAL COMMUNICATIONS SYSTEM
NCS

NCS Leadership



Mr. Robert P. Liscouski
Manager

Mr. Brenton C. Greene
Deputy Manager

CAPT J. Katharine Burton, USN
Assistant Deputy Manager

Dr. Peter A. Fonash
Chief
Technology and
Programs Division

Mr. Frederick Herr
Chief
Critical Infrastructure
Protection Division

Mr. Joseph Stivers
Acting Chief
Plans and
Resources Division

Mr. Thomas J. Falvey
Chief
Customer Service
Division

NCS Committee of Principals

Department of State (DOS)
Mr. Bruce Morrison

Department of the Treasury (TREAS)
Mr. Drew Ladner

Department of Defense (DOD)
Mr. Steven Price

Department of Justice (DOJ)
Mr. Gary Laws

Department of the Interior (DOI)
Mr. W. Hord Tipton

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

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

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

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

Department of Energy (DOE)
Ms. Karen Evans

Department of Veterans Affairs (VA)
Mr. Edward F. Meagher

Department of Homeland Security (DHS)
Mr. Steven Cooper

Federal Emergency Management Agency (FEMA)
Mr. Joseph D. Szwarckop

The Joint Staff (JS)
Lt. Gen. Robert Shea, USMC

General Services Administration (GSA)
Ms. Sandra N. Bates

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

Nuclear Regulatory Commission (NRC)
Mr. Richard Wessman

National Telecommunications and Information Administration (NTIA)
Mr. Frederick R. Wentland

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

United States Postal Service (USPS)
Mr. Peter Myo Khin

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

Federal Communications Commission (FCC)
Mr. Jeffrey M. Goldthrop

NCS Council of Representatives

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

Department of the Treasury (TREAS)
Mr. Harry Hixon

Department of Defense (DOD)
CAPT Lynne Hicks, USN

Department of Justice (DOJ)
Mr. Gary W. Laws

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

Department of Agriculture (USDA)
Mr. Roy Allums

Department of Commerce (DOC)
Mr. Benjamin Chisolm

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

Department of Transportation (DOT)
Ms. Hollace Twining

Department of Energy (DOE)
Mr. Gordon Errington

Department of Veterans Affairs (VA)
Mr. David Cheplick

Federal Emergency Management Agency (FEMA)
Mr. Paul B. Maison

The Joint Staff (JS)
CAPT Lloyd Gilham, USN

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

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

Nuclear Regulatory Commission (NRC)
Mr. Thomas M. Kardaras

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

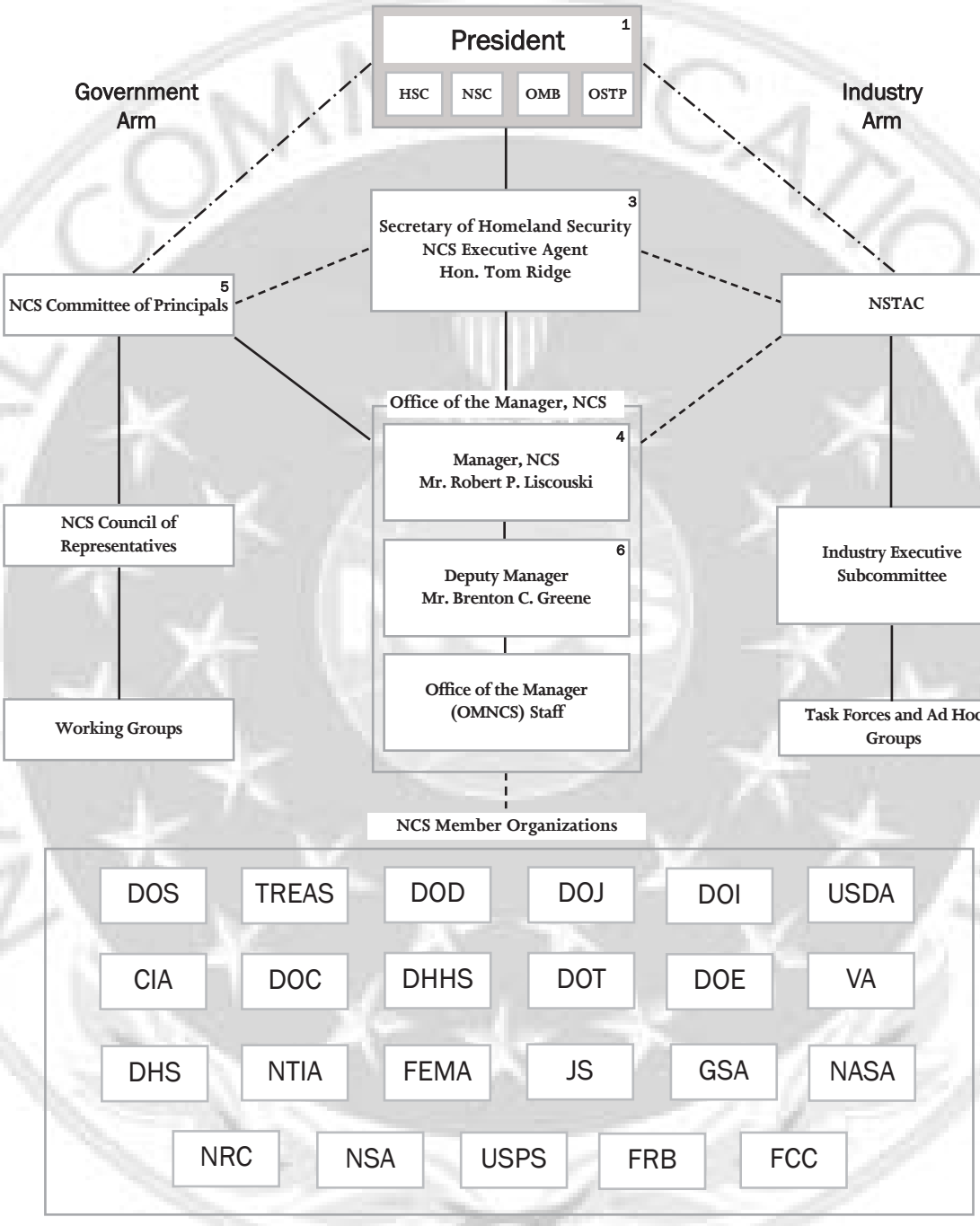
National Security Agency (NSA)
Mr. Gilbert C. Nolte

United States Postal Service (USPS)
Mr. Warren Schwartz

Federal Reserve Board (FRB)
Dr. H. Wayne Pacine

Federal Communications Commission (FCC)
Mr. Kenneth P. Moran

The NCS Structure



1. Policy Direction and Direct Execution of War Powers Function
2. National Security Telecommunications Advisory Committee created by E.O. 12382
3. Executive Agent, NCS responsibilities assigned to Secretary of Homeland Security by E.O. 13286, February 28, 2003
4. Assistant Secretary for Infrastructure Protection, 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


NATIONAL COMMUNICATIONS SYSTEM
NCS

I

Introduction

The History Of The National Communications System

SECTION I

INTRODUCTION
THE HISTORY OF
THE NATIONAL COMMUNICATIONS SYSTEM

This document, prepared by the Office of the Manager, National Communications System (NCS), reports on national security and emergency preparedness (NS/EP) activities and telecommunications events, and highlights the agency's innovations, programs, and achievements during Fiscal Year 2003.

BACKGROUND

President John F. Kennedy established the NCS in 1963 as a result of the communications issues discovered during the 1962 Cuban Missile Crisis. During critical periods of the crisis, the Federal Government experienced tremendous difficulty in establishing and maintaining communications between the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state, which proved detrimental to the resolution efforts. Following the crisis, President Kennedy mandated the National Security Council (NSC) conduct an investigation regarding national security communications.

In response, the NSC established an interdepartmental committee to evaluate critical communications networks and make changes as needed to meet the Nation's requirements.

To best serve the needs of the President, the Department of Defense, diplomatic and intelligence agencies, and civilian leadership, the NSC committee found that a consolidated communications system would be required. This system would support critical Government communications functions, especially during periods of heightened national security or in times of crisis; hence, the creation of the NCS. Established by Presidential Memorandum on August 21, 1963, the NCS is responsible for ensuring NS/EP communications function successfully, including interconnectivity and survivability, during times of congestion or when the networks have been damaged or destroyed.

When brought to light, NS/EP communications remained at the forefront of Presidential concern in the Nation's defense. On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which superseded President Kennedy's Memorandum on the NCS. This E.O. assigned the NCS with the mission to coordinate the planning for and provisioning of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution. The E.O. directs the NCS to advise the President, the National Security Council, the Homeland Security Council, the Director, Office of Science and Technology, and the Director, Office of Management and Budget on these matters. Nearly 40 years after the creation of the NCS, these functions remain the core responsibility of the NCS.

ENVIRONMENT FACING THE NCS - THE EMERGING HOMELAND SECURITY LANDSCAPE

A dramatic shift in this country's national security landscape occurred following the September 11, 2001, attacks on the World Trade Center in New York and the Pentagon in Washington, D.C., as the United States responded to terrorist aggression on its own soil. No longer faced with a Cold War threat based on risk averse, deterrence strategies between the world's two superpowers, the United States had to confront a new global war on terrorism defined by asymmetric, rapidly changing threats from rogue states and elusive, decentralized non-state actors.

The Federal Government responded quickly to this new homeland security paradigm. President George W. Bush issued E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, on October 8, 2001, and E.O. 13231, *Critical Infrastructure Protection*, on October 16, 2001. These orders further defined the role of the NCS in national and homeland security efforts.

Almost a year later, the Bush Administration released the, "*National Security Strategy of the United States*," in September 2002, which delineated the Federal Government's strategy for preventing terrorist attacks against the homeland, U.S. interests abroad, and U.S. allies. The Administration also worked with Congress to pass landmark legislation to establish a focal point within the Federal Government for enhancing security at our airports, seaports, land borders, and local communities and preparing for and responding to any incidents that do occur. On November 25, 2002, the President signed into law the Homeland Security Act of 2002, which established the Department of Homeland Security (DHS) and commenced a major reorganization of Government departments and agencies with homeland security missions. As part of the reorganization plan, the NCS and its NS/EP programs were designated for transfer to the new department's Information Analysis and Infrastructure Protection (IAIP) Directorate.

The NCS's Executive Agent transferred from the Department of Defense to the DHS when President Bush signed omnibus E.O. 13286, *Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security* on February 28, 2003. The following day, on March 1, 2003, the NCS officially became part of the DHS.

As part of its effort to secure the homeland from terrorist attacks, the Government took significant action to enhance the security of the physical and cyber-based systems that are essential to national security, economic security, and public health and safety. The U.S. Congress, for example, unified the Federal Government's critical infrastructure protection agencies under one department, the DHS, and the Administration developed, "*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*," and "*The National Strategy to Secure Cyberspace*," to guide the Government's infrastructure protection efforts.

It is within this changing security reality that the NCS continues to carry out its NS/EP mission. Because the telecommunications network serves as the central nervous system for all critical infrastructures, the NCS became a focal point within the Federal Government for addressing telecommunications critical infrastructure vulnerabilities and interdependencies. Though it continued to carry out its NS/EP telecommunications responsibilities in support of and in response to natural disasters, the NCS quickly found itself on the front line of the Nation's defense against terrorism.

In transferring to the DHS IAIP Directorate, the NCS provided many important tools and partnerships that the Department could leverage to carry out its mission to prevent terrorist attacks within the United States, reduce, the Nation's vulnerability to terrorism, minimize damage, and recover from attacks that do occur.

Through the NCS and its National Coordinating Center for Telecommunications (NCC), DHS gained instant connectivity to share information and coordinate responses to threats and crises with the telecommunications and information technology sectors. Despite major changes in the national security environment and the recent instability of the telecommunications and information technology industry, the NCS has maintained one of the oldest and most successful industry-Government partnerships in the President's National Security Telecommunications Advisory Committee (NSTAC). Learning from the NSTAC and the NCC, DHS can explore similar frameworks and partnerships across all critical infrastructure sectors and industries.

The NCS also brought to DHS a suite of proven national-level programs that provide for a resilient telecommunications infrastructure. Many of the NCS programs also enhanced the Department's emergency preparedness and indications and warnings capabilities.

For the NCS, the changing homeland security environment presented a series of new challenges, particularly with respect to its collaboration with a new set of stakeholders. Within DHS, the NCS increasingly interfaced with the intelligence community, coordinated the operation of its cyber-based programs with a newly created cyber security division, and developed tools for carrying out new and existing NS/EP programs in coordination with the DHS Science and Technology Directorate. The need to better understand vulnerabilities resulting from critical infrastructure interdependencies made the

NCS an important collaborator with the Homeland Security Operations Center in understanding potential downstream effects of known threats and threat indicators. In the broader homeland security community, NCS helped DHS form essential, new partnerships with other Federal, State, local, and private entities with homeland security roles to demarcate responsibilities for protecting critical infrastructure and key assets.

With each new challenge, the NCS continues to evolve to meet the changing policy, technology, and threat environments. As it demonstrated during the first year of DHS sponsorship, the NCS will continue to provide its stakeholders with proactive solutions to meet current and future homeland security communications requirements.


NATIONAL COMMUNICATIONS SYSTEM
NCS

II

EMERGENCY RESPONSE ACTIVITIES

SECTION II

EMERGENCY RESPONSE ACTIVITIES

The National Communication System's (NCS) National Coordinating Center for Telecommunications (NCC) is a joint U.S. telecommunications industry and Federal Government operation that responds to the Government's national security and emergency preparedness (NS/EP) telecommunications service requirements during all hazard responses. The NCC supports emergency response efforts by training key emergency personnel, provisioning communications resources, assisting in communications infrastructure restoration, and ensuring NS/EP communications during national disasters and other emergency situations. It is also the primary agency for implementing and coordinating the Federal Response Plan's Emergency Support Function #2 (ESF #2).

The NCS Individual Mobilization Augmentee (IMA) Program provides emergency telecommunications support to the NCC during national and regional crises and emergencies. U.S. Army Reserve Signal Corps officers serve as IMA staff. In addition, the General Services Administration's Regional Communications Managers support the NCC by operating as NCS Regional Managers following a disaster declaration. Finally, members of the NCC's Telecom Information Sharing and Analysis Center (ISAC) facilitate the collaboration and information sharing of vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, Federal Government, and other sources.

During Hurricane Lili (October 2002), Typhoon Pongsona (December 2002), Tropical Storm Claudette (July 2003), and Hurricane Isabel (September 2003), NCC Emergency Operations Teams and the Shared Resources High Frequency Program were activated to provide support to emergency responders. As part of the response to Typhoon Pongsona, Tropical Storm Claudette, Hurricane Isabel, and Exercise TOPOFF-2, NCS Regional Managers were activated. IMAs were also activated during Typhoon Pongsona and Hurricane Isabel. Efforts were coordinated between telecommunications representatives and the Global Network Operations and Security Center to supply fuel and communications systems to help rebuild the regional infrastructure.

HURRICANE ISABEL

On September 11, 2003, Hurricane Isabel became the first Category 5 hurricane in the Atlantic since 1998. On September 18th, Isabel made landfall on the Outer Banks of North Carolina as a Category 2 hurricane and moved northwest, knocking out power to millions of people and causing at least 13 fatalities. Presidential disaster declarations were issued for all, or parts of, Delaware, the

District of Columbia, Maryland, North Carolina, Pennsylvania, Virginia, and West Virginia.

The NCS deployed three IMAs to disaster field offices in Raleigh, North Carolina, and Richmond, Virginia, to assist those NCS Regional Managers serving as Federal Emergency Communications Coordinators. The NCS' Telecommunications Service Priority (TSP) Office processed provisioning requests to support Federal Emergency Management Agency (FEMA) disaster field offices in New Castle, Delaware; Washington, DC; Baltimore, Maryland; Elizabeth City, New Bern, and Raleigh, North Carolina; Harrisburg, Pennsylvania; and Richmond, Virginia. TSP provisioning support was also provided to the Allstate Insurance Company offices in Raleigh, North Carolina, and Chantilly and Hampton, Virginia.

In the aftermath of Hurricane Isabel, the telecommunications infrastructure was inundated with commercial power outages. However, many of the affected areas were able to make use of backup power to provide customer service. The NCC itself experienced significant power outages resulting in local area network and e-mail problems, but emergency response operations continued through the use of backup generators.

U.S. - CANADA 2003 ELECTRIC POWER BLACKOUT

On August 14, 2003, a massive power outage affected large parts of the northeastern U.S. and eastern Canada. This was the largest blackout in North American history, affecting an estimated 50 million people and covering an area of approximately 9,300 square miles. One hundred power plants were affected during the outage, of which 22 were nuclear power plants. Several critical infrastructures impacted by the outage included telecommunications, banking and finance, energy, and transportation. The NCC, FEMA, which is now under Department of Homeland Security, and the Department of Transportation coordinated the supply of fuel and generators to the affected areas to ensure that communications systems remained online. The NCC communicated with Industry Canada and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness to obtain information regarding the incident and then distributed this data to key Federal Government officials. The NCC and its Telecom ISAC coordinated extensively with the North American Electric Reliability Council and the Electric Power ISAC during the outage and assisted in the investigation of the power outage.

ELECTRONIC INTRUSION INCIDENTS

An outbreak of the "Slapper" worm was detected on the Internet January 25, 2003, which infected computers running Microsoft SQL Server 2000 or MSDE 2000. The worm generated massive amounts of network packets that overloaded servers and routers and eventually slowed network traffic. During the attack as many as five of the 13 Internet root nameservers were down due to this attack.

Various versions of a virus-like worm (Blaster, LovSan) affected corporate networks worldwide beginning in August 2003. The worm and its variants infected more than 500,000 business and individual computers worldwide, making it one of the worst outbreaks of the year. The virus variants took advantage of a defect in Microsoft Windows software used to share data files across computer networks. The NCC Watch Center and NCC member organizations coordinated efforts to alert the public on the most efficient ways to restore computing capabilities.

SPACE SHUTTLE COLUMBIA DISASTER

On February 1, 2003, the space shuttle Columbia broke up over Texas during re-entry killing seven astronauts. The cause of the accident was foam that hit the shuttle's wing shortly after liftoff. Within minutes of the accident, National Aeronautics and Space Administration officials announced that their contingency plan was put into action. Even before much of the debris had fallen to Earth, emergency teams had been activated and were performing their respective roles. Texas and Louisiana were declared disaster areas and emergency telecommunications were required to support the recovery process. NCC industry members were called upon to provide these services.

III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

SECTION III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section features the accomplishments and activities 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 as it faced many challenging issues during fiscal year (FY) 2003.

Transition To The Department Of Homeland Security

During FY 2003, the NCS continued its transition into the Department of Homeland Security (DHS) and strived to define the role it would play within the Department. The NCS has been placed in the Information Analysis and Infrastructure Protection (IAIP) Directorate, which focuses on the intelligence analysis aspect of homeland security.

The broadening of the NCS mission has brought with it a series of new challenges, particularly collaboration with a new set of stakeholders. Within DHS, the NCS has worked to interface with the intelligence community, coordinated the operation of its cyber-based programs such as the Critical infrastructure Warning Information Network (CWIN) and the Global Early Warning Information System (GEWIS) with a new cyber security division, and developed new tools for carrying out its NS/EP programs in coordination with the DHS Science and Technology Directorate. The NCS's National Coordinating Center for Telecommunications (NCC) has also adjusted to the changing environment, and now works closely with DHS to share information and coordinate responses to threats and crises.

The transition to the new Department, also brought several leadership changes within the NCS. Robert P. Liscouski, also currently the Assistant Secretary for IP, has been formally designated to become the Manager of the NCS. Department approval of the designation is still pending. He would replace Lieutenant General Harry D. Raduege, Jr., who remains the Director of the Defense Information Systems Agency.

In March 2003, Joseph Stivers, Deputy, Plans and Resources Division, became the Acting Chief, Plans and Resources Division. He replaced Larry Wheeler who resigned from the NCS to serve as Director of the IP Planning Office, reporting to Mr. Liscouski, Assistant Secretary of IP. Thomas J. Falvey, formerly the Deputy Director, Office of Intelligence and Security, Office of the Secretary, Department of Transportation, became the Chief, Customer Service

Division, in May 2003. He replaced Air Force Colonel Wilson D. Crafton, now assigned as the Department of Defense (DOD) Liaison to the NCS. Jane Polk, formerly Deputy Chief, Critical Infrastructure Protection (CIP) Division, became the Acting Chief, CIP Division in August 2003. She replaced Frederick W. Herr, who retired after 35 years of service to the Federal Government.

TECHNOLOGY AND PROGRAMS DIVISION

The Technology and Programs Division implements evolutionary national security and emergency preparedness (NS/EP) communications capabilities for a reliable and effective telecommunications infrastructure. The division develops programs, technical studies, analyses, and standards that promote the reliability, security, interoperability, and priority treatment of NS/EP telecommunications.

The division's objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs. Division personnel evaluate emerging technologies to alleviate impediments to interoperability and to satisfy NS/EP requirements. They use this information as they participate in industry and international standards organization meetings to ensure that NS/EP requirements are incorporated into any recommendations.

The following pages highlight the major projects undertaken by the Technology and Programs Division during Fiscal Year (FY) 2003.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

BACKGROUND

The OMNCS established the Government Emergency Telecommunications Service (GETS) to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in NS/EP missions. GETS satisfies these requirements by providing specialized processing in local and long distance public telephone networks. The program ensures GETS users experience a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters. GETS reached full operational capability (FOC) on September 30, 2001.

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

The first objective of GETS planners was to expeditiously field a service that would provide priority call treatment. The service was incrementally improved with specialized calling features. The strategy of developing GETS by using existing assets of the PSN enabled early implementation and provided technical currency by leveraging the continual improvements made by the

industry. Embedding GETS primarily within the software resources of the PSN also made it unnecessary for the Government to purchase, install, maintain, and eventually update network equipment.

The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This resulted in separate GETS contracts with AT&T, MCI, and Sprint, the three largest IXCs. They are the only IXCs that can authenticate and process GETS calls. As such, access to these carriers must be available at all PSN end offices. Although the IXCs began with the same basic set of functional requirements, the implementation approach pursued by each IXC and the inherent differences in the structure of the IXCs' respective networks caused the operational features and capabilities to differ slightly among the providers.

After the IXC implementation, the focus of feature development shifted to the local exchange carrier (LEC) networks. Computer Sciences Corporation (CSC) was awarded the integration contract for development and implementation of GETS features in the LECs and for overall GETS operation, administration, maintenance, and provisioning services. Advanced intelligent network (AIN) technology provided the basis for the first phase of GETS LEC feature deployment, which is alternate carrier routing (ACR). ACR enhances access by automatically attempting all three GETS IXCs.

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

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

As the PSN evolves into packet-based technology to support voice traffic, the GETS Program Management Office (PMO) is working with the telecommunications industry to maximize and protect the NS/EP community's substantial investment in circuit-switched network enhancements. This work includes one-on-one meetings with carriers and vendors to gain an understanding of their network evolution plans, participation in standards bodies influencing how NS/EP calls may be processed in packet networks, and development of requirements related to packet-based call processing in acquisition packages for the IC and IXC follow-on contracts awarded in late 2003 and early 2004.

Operations and Features

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

The utility of this feature was demonstrated during the September 11, 2001, attacks on the U.S.

When a user dials a GETS access number, a tone prompts for a personal identification number (PIN), then a voice recording asks for a destination telephone number. If the access control system is inoperative, a fail open feature allows users to complete their GETS calls. The utility of this feature was demonstrated during the September 11, 2001, attacks on the U.S.

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS has worked to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks.

Interoperability

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

Similar to other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the *Telecommunications Act of 1996*. Resulting industry deregulation has led to a significant increase in the number of service providers. This environment has led to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin telephones and PBXs, in some service areas. Previous testing shows these problems to be particularly prevalent for coin telephones owned and managed by small businesses and PBXs operated by the hospitality industry (hotels and motels). Commonly encountered problems include the need to deposit coins at a coin telephone before dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

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 and toll-free calls.

Successes

GETS was one of the first communications services to be used following the terrorist attacks on September 11, 2001. Despite the heavy telephone congestion occurring immediately following the attacks and during the first week, 95 percent of the 4,000 GETS calls to and from Manhattan successfully got through. Another 3,000 GETS calls were made in Arlington, Virginia, during the same time period with similar success rates. From the date of the attack until September 28, more than 1,000 GETS cards were issued to qualified emergency personnel. During that 17-day span, more than 1,500 people used the GETS Program.

In the past year, the GETS Program has continued to make significant progress in its outreach efforts to Federal, State, and local governments and other qualified NS/EP industry and non-profit organizations. As of August 11, 2003, there were 79,198 active GETS cards—an increase of 10,665 cards during the past year—categorized as follows: Federal: 49,052 to 54,666; State: 6,986 to 7,697; local: 7,955 to 8,665; industry: 4,540 to 6,946; and other NS/EP organizations: 1,224.

With the current trend toward more personal and professional wireless communications, more individuals are carrying wireless phones. During the terrorist attacks on September 11, 2001, wireless phone traffic—similar to traditional phone lines—became congested. Yet unlike traditional phone lines, emergency responders were less likely to complete GETS calls through wireless communications because wireless networks did not provide priority treatment. Up until this time, the GETS Program was not funded to provide priority access for wireless communications.

Wireless Priority Service

Background

Early in 1995, the OMNCS initiated efforts to develop and implement a nationwide cellular priority access capability in support of NS/EP telecommunications. Since then, the OMNCS has pursued a number of activities to improve wireless call completion during times of network congestion. In 1998 and 1999, the GETS Program worked with an industry switch vendor to demonstrate end-to-end wireless priority features. The OMNCS also explored the possibility of a national-level database for wireless priority access in 2001.

Resulting from a petition from the NCS in October 1995, the Federal Communications Commission (FCC) released a Report and Order (R&O) [FCC-00-242, July 13, 2000] on wireless Priority Access Service (PAS). The R&O offers Federal liability relief to wireless carriers if the service is implemented in accordance with uniform operating procedures. The FCC explained the R&O PAS was voluntary, but in the public interest, and defined five priority levels for NS/EP calls.

Wireless network congestion was widespread on September 11, 2001. With wireless traffic demand estimated at up to 10 times normal in the affected areas and double nationwide, the need for wireless priority service became a critical and urgent requirement. Reacting to these events, the National Security Council (NSC) issued the following guidance to the OMNCS (minutes from October 5, 2001, Meeting on Selected NS/EP Telecommunications Projects, October 9, 2001):

- Implement an immediate solution to the cellular radio channel congestion problem, targeted within 60 days, using a

readily and commercially available capability for the Washington metropolitan area and recommend whether to expand this immediate solution to other metropolitan areas.

- Develop and deploy a priority access queuing system for wireless nationwide, targeted within 1 year.

In response to this guidance, OMNCS initiated two efforts:

- Immediate—a solution using a single carrier with commercially available and readily deployed technology in Washington, DC, New York City, New York, and the site for the Winter Olympics in Salt Lake City, Utah.

- Nationwide—a long-term solution directed towards the deployment of a multi-carrier, standards-based national capability.

Wireless Priority Service (WPS), in conjunction with GETS, facilitates emergency recovery operations, assisting in the recovery of the Government and the general population to normal conditions after serious disasters and events, such as floods, earthquakes, hurricanes, and terrorist attacks.

WPS is based on the two access technologies most widely available in the U.S., Global System for Mobile communications (GSM) and Code Division Multiple Access (CDMA). The OMNCS has partnered with industry to provide a GSM-based service using standards-based priority queuing. As of June 2003, there are more than 3,000 WPS users, primarily in the Washington, DC, and New York City areas. It is the objective of the OMNCS to provide the WPS capability to an estimated user population of 200,000 GSM users and 150,000 CDMA users.

IMMEDIATE WPS

The Immediate WPS (I-WPS) was designed to expeditiously improve call completion to NS/EP users using commercial off-the-shelf (COTS) technology so that Washington, DC, New York City, New York, and Salt Lake City, Utah, had cellular priority service available as soon as possible. The I-WPS was provided by VoiceStream (now T-Mobile) and was complemented by a backup satellite service provided by Globalstar. The Salt Lake City version of I-WPS was deployed during February 2002, in advance of the Olympic games, and I-WPS was operational by mid-May 2002 in Washington, DC, and New York City.

VoiceStream leveraged an existing GSM feature called enhanced Multi-Level Precedence and Preemption (eMLPP) to provide I-WPS. The eMLPP feature allows emergency calls to queue for the next available radio channel, without preempting any calls in progress. An FCC waiver was required for T-Mobile because it did not conform to the FCC R&O (FCC-00-242, July 13, 2000) requirement to invoke the priority service on a call-by-call basis. VoiceStream filed a Petition for Waiver, supported by a formal statement from the NCS, to the FCC. The technical proposal contained in the petition provided the NCS solution for immediate deployment in New York City and Washington, DC. On December 11, 2002, the FCC released a document seeking comments regarding the petition, and the waiver was subsequently granted.

The geographic markets in which I-WPS was available have been transitioned to the WPS Nationwide Initial Operating Capability (IOC). Subscriptions and usage costs for continued use of this service have been transitioned from the OMNCS directly to the user agencies.

NATIONWIDE WPS

Nationwide WPS is a more comprehensive wireless priority capability. Due to the requirement for nationwide WPS coverage, multiple carriers and multiple access technologies are needed. The two dominant access technologies deployed by U.S. carriers are GSM (T-Mobile, Cingular Wireless, AT&T Wireless, and Nextel) and CDMA (Verizon Wireless and Sprint PCS). Nationwide WPS is being provided in two major phases, IOC and FOC. IOC is a GSM-based solution only, consisting of priority radio channel access at call origination, similar to the I-WPS, but satisfying all the requirements of the FCC R&O, including invocation of the service on a call-by-call basis. A full, end-to-end capability—beginning with the NS/EP wireless caller, through the wireless networks, through the IXC and/or LEC networks, and to the wireless or wireline called party—will be realized by the nationwide FOC, which the NCS plans to provide in both the GSM and CDMA technologies. This service will offer increased probability of call completion during times of widespread network congestion.

Nationwide IOC software development began in July 2002, and installation of this software in commercial mobile radio service (CMRS) provider network switches began in December 2002. The deployment schedule for nationwide FOC was impacted by FY 2003 funding reductions, and, although development and deployment of CDMA was unfunded during FY 2003, implementation of GSM FOC will begin during the second quarter in 2004. GSM FOC will be attained in New York City and Washington, DC, in March 2004 in the T-Mobile network, with additional markets and additional carriers to come on-line throughout the year. CDMA FOC is slated for 2006. Nationwide WPS is made possible by strong industry partnerships with Government during the development of Industry Requirements (IR). Cellular telephony equipment vendors and service providers that are participating in WPS GSM FOC include T-Mobile, Cingular Wireless, Nextel, AT&T Wireless, Nortel Networks, Ericsson, Nokia, Siemens and Motorola. Those that may participate in the WPS CDMA solution include Verizon Wireless, Sprint PCS, ALLTEL, Lucent, Nortel Networks and Motorola.

Nationwide WPS is made possible by strong industry partnerships with Government...

NATIONWIDE INDUSTRY REQUIREMENTS

The nationwide WPS capability is based on wireless standards and IR documents jointly developed by industry and Government. The active and cooperative participation of all stakeholders, including major wireless equipment vendors and service providers, successfully produced these IR documents. IOC requirements were completed in February 2002, only 4 months after direction was received from the NSC. The FOC requirements for both GSM and CDMA have also been completed. These documents will be used as a basis to issue requests for proposals for the nationwide WPS.

The NCS has also taken steps to ensure that the IR documents provide a method for use of the Nation's cellular telecommunications networks by NS/EP personnel that does not hinder public use during emergency events. As a result, the IR documents contain a requirement that stipulates a reasonable amount of capacity is always available for public use. The FCC issued guidelines for

NS/EP use of wireless networks, and only NS/EP leadership and key personnel will be approved to use WPS. For those critical individuals who need it, WPS will be a powerful new emergency communications asset and an important national resource.

Priority Services Team

Although traditional NS/EP telecommunications services were designed around the circuit-switched infrastructure of the Public Switched Telephone Network (PSTN), evolving converged and next generation networks (NGN) will incorporate packet-switched infrastructures. As convergence occurs, emergency telecommunications services (ETS) will be guided by commercial standards resulting from technology evolution.

Third generation and beyond wireless networks as well as packet-switched networks, such as the Internet and the developing Internet Protocol (IP) cable networks, are becoming increasingly more vital to the NS/EP community. The Priority Services Team works with a number of national and international telecommunications industry standards organizations to ensure that evolving commercial standards take into account requirements and technical considerations supporting ETS for the NS/EP community of users.

ETS is a multidimensional initiative that addresses standards development work related to network protocols and signaling systems. The ETS initiative was developed to ensure that developing standards continue to support priority for emergency telecommunications regardless of the network topology. Prime functional areas for ETS include priority establishment, priority access, dynamic restoration, authentication, security, integrity, and management of emergency telecommunications in converging and next generation networks.

Priority Services Team members provide direct support to the U.S. Department of State (DOS) by chairing the International Telecommunications Advisory Committee Study Group 'B' along with serving as senior Government advisors and leaders, for example head of delegations, to a variety of international and national meetings on telecommunications. In addition, team members actively participate in the work of various industry standards development organizations including—

- Telecommunications Committee T1
- Telecommunications Industry Association (TIA)
- International Telecommunication Union, Telecommunications Sector (ITU-T)
- Internet Engineering Task Force (IETF)
- TeleManagement Forum
- European Telecommunications Standards Institute (ETSI) project known as Telecommunication and Internet Protocol Harmonization over Networks (TIPHON)
- Third Generation Partnership Project (3GPP)
- Third Generation Partnership Project 2 (3GPP2)
- TIA/ETSI project Mobile Broadband for Emergency and Safety Applications.

Technical approaches employed for ETS in the above organizations include—

- Firmly establishing NS/EP requirements in work programs
- Developing and providing detailed technical proposals, such as NS/EP contributions, within industry standards programs
- Encouraging industry participants to make technical proposals to augment NCS proposals
- Integrating NS/EP technical service agreements into operational systems as an inherent part of the underlying packet-based infrastructure rather than a retrofitted fix in deployed systems
- Investigating new features emerging in packet-based networks to enhance NS/EP operations, such as electronic mail (e-mail), instant messaging, multicast video, Web access, and tunneling.

Federal Wireless Users Forum

The Federal Wireless Users Forum (FWUF), established in 1992, enables interaction and information exchange among wireless communications service vendors and Government users for developing industry wide standards for emerging wireless digital technologies. The objectives of the FWUF are to—

- Educate Government users about wireless telecommunications
- Identify the telecommunication needs of Government users
- Facilitate information exchange with other user groups, standards organizations, manufacturers, and service providers to ensure Government user needs are met
- Support the interoperability of emerging wireless services and equipment through increased participation in formulating Federal policy, supporting standardization efforts, and other appropriate activities.

The FWUF is jointly chaired by the OMNCS and the National Security Agency (NSA), and it is directed by a steering committee of members from the DOD, the Department of Commerce, NSA, the Department of the Treasury, the National Institute of Standards and Technology, and the Federal law enforcement community. FWUF holds biannual forums to bring people from Government and the wireless telecom industry together. FWUF activities include—

- Multi-day workshops with industry participation
- Outreach work sessions with a focus on a particular user community
- User application profile development.

Workshop Highlights

The 18th FWUF workshop was held from October 16-18, 2002, in Las Vegas, Nevada. To gain more exposure among commercial wireless service providers and developers, the workshop was scheduled in conjunction with the Cellular Telecommunications and Internet Association (CTIA) Wireless Information Technology (IT) and Internet 2002 convention. Participants benefited from demonstrations of the latest in wireless data

services and technologies and reached agreement on the importance of advancing security and interoperability in wireless communications.

Highlights of presentations during the 18th FWUF workshop included—

- More than 135 million wireless subscribers are served in the U.S., generating $68 billion in revenues—an $11 billion growth from 2001.
- GETS had a 95 percent success rate during the terrorist attacks in 2001.
- Progress is being made in the Wireless Emergency Response Team (WERT) in case of another tragedy similar to the events on September 11, 2001.
- GEWIS looks at performance of the Internet, including domain name servers, topology, peering points, and e-commerce infrastructure.
- The formation of a "wireless Government" will enable more efficient, manageable, and secure mobile workforces to have wireless extensibility with Java-enabled applications to access information across agencies, internally, and with the public.
- Legislators are becoming involved with efforts to develop interoperability within all public safety agencies throughout each State.
- Future Narrow Band Digital Terminal (FNBDT) will enable interoperable, secure communications across a variety of networks and services, extensible to additional applications and crypto suites.

The relationship between the Government and private industry should be a partnership, with more trust involved.

The 19th FWUF workshop was held from April 8-10, 2003, in New Orleans, Louisiana. The workshop consisted of presentations including the following key elements:

- AT&T, Cingular, and Nextel will be added to the WPS Program for GSM Communications by the end of 2003.
- CDMA development and implementation is being planned, anticipating that CDMA carriers will be added to the WPS Program in the future.
- By June 2003 T-Mobile WPS will be available in most of the U.S., except Nevada and California.
- The relationship between the Government and private industry should be a partnership, with more trust involved.
- Carriers should be selected by determining which one best meets users' needs.
- In the wireless sector, there were more than 150 facilities-based carriers and more than 131,000 cell sites, with 137 million subscribers using 600 billion minutes of airtime in 2002. Sector revenues totaled $116 billion, consumer revenues totaled $71 billion, and the cumulative capital invested totaled $118 billion.

- Commercial Mobile Radio Service (CMRS) has the most security experience with end-to-end encryption and digital transmission over Air Interface.

- Interoperability Technology For Public Safety is due out by the end of 2003, providing documentation that current and future technology is meeting the requirements for interoperable systems.

Modeling, Analysis, And Technology Assessment

As directed by Executive Order (E.O.) 12472, the NCS evaluates the ability of the Nation's telecommunications resources to meet NS/EP requirements using modeling and analysis techniques and applications.

Network Design And Analysis Capability

Because the NS/EP community relies heavily on the PSN, the NCS developed the Network Design and Analysis Capability (NDAC) to analyze current U.S. networks and to evaluate the need for additional capabilities. The NCS has invested many years establishing strong working relationships with commercial carriers and Government agencies, and in developing PSN modeling methodologies, tool sets, and unique databases that include proprietary data from the major carriers. The NDAC is used to conduct studies that cover multiple communications areas, such as wireline, wireless, and the Internet. The NDAC is currently studying numerous issues such as the Backup Dial Tone (BDT), the NGN, Internet Service Providers (ISP), IP Network Performance under Cyber Attack, and Traffic Analysis of Critical Federal Telecommunications Infrastructures.

Backup Dial Tone – The BDT study uses NDAC to examine methods and technology approaches to enhance the communications reliability in the Washington metropolitan area under emergency conditions. This effort is in response to Executive Branch concerns that key Federal agencies and emergency responders may be at risk of losing essential wireline communications services under disaster or emergency conditions similar to those of September 11, 2001. Currently in Phase III, the NCS is conducting demonstrations of Satellite Communications (SATCOM), Free Space Optics (FSO), and other technologies to determine their potential to mitigate communications vulnerabilities. Phase IV will include routing diversity studies for Federal agencies in the Washington metropolitan area.

Next Generation Network – The circuit-switched architecture of the PSN is converging with the packet-switched technology of the Internet, soon evolving into the NGN. As the architecture evolves, the tools and techniques used to assess the performance of the PSN must evolve as well. Because the technology, architectures, protocols, and interfaces the service providers may use during this network evolution are in flux, several likely NGN architectures and traffic streams (voice, data, and streaming video) were developed. After the baseline architecture and traffic models were created, multiple traffic overloading scenarios were applied to each to identify any potential network bottlenecks. In addition to traffic overloading scenarios, cyber attack and nuclear attack scenarios were applied to the simulated NGN architectures to assess their impact on overall network performance. A predictive analysis environment was then created to assess the candidate architectures upon network performance, cost, and ability to meet the NS/EP mission.

Internet Service Provider – Although NS/EP communications have long been supported by the PSN, an increasing number of Government users are now using services offered through the Internet; consequently, the logical and physical infrastructures of the Internet must be modeled to support NS/EP analyses. With the ongoing NDAC expansion to include packet-switched networks, the NCS is developing an Internet modeling capability that will capture the physical and logical interdependencies between ISPs from both architectural and traffic perspectives. The ISP study will use this capability to determine the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure.

IP Network Performance under Cyber Attack – Analysis and computer modeling capabilities must answer such questions as, "What impact would a cyber attack have on Federal networks?" "Which Federal telecommunication systems need to be protected?" IP networks span the globe with the Internet being the largest and most well known. Cyber attacks against these networks often affect parts of the network beyond what was specifically targeted, causing a significant degradation to network performance in terms of packet latency, jitter, and signal loss. Once an analytical model of an IP network under attack is developed, simulation models and laboratory experiments of cyber attacks will be used to calibrate the analytical results.

Traffic Analysis of Critical Federal Telecommunication Infrastructure – An analysis capability is being developed to identify the most critical Government locations and the most critical telecommunications providers' locations necessary to ensure Government connectivity during a crisis. NCS is coordinating with GSA FTS2001 personnel to share FTS2001 traffic data, particularly for agencies merged recently with the Department of Homeland Security (DHS).

TECHNOLOGY ASSESSMENT LABORATORY

The NCS has established a Technology Assessment Laboratory (TAL), which currently has an interim authority to operate and is scheduled to go through full accreditation in the near future. The TAL provides the capability to—

- Evaluate Contract Deliverables: Some contracts have software and/or hardware deliverables; the TAL is used to evaluate these deliverables for acceptance purposes.

- Evaluate Products: The TAL provides a platform to research, identify, and evaluate off-the-shelf products [COTS and Government off-the-shelf (GOTS)] that may satisfy specific NS/EP requirements, often obviating development contracts.

- Host Applications and Databases: The TAL provides the host environment for several applications and associated databases developed specifically to ensure survivable and robust communications in support of NS/EP requirements. These applications include, but are not limited to—

  - The NDAC is a set of tools, data sets, and methodologies that enable modeling and analysis of the PSN and, with the addition of the ISP task, the Internet.

- The Internet Monitoring Framework (IMF) is an integrated set of prototype tools for monitoring the status of the Internet.

- **Provide Component-Level Simulation:** Although the NDAC provides a macro view of network behavior, it lacks the ability to adequately simulate the behavior and interaction of individual pieces of software and hardware. The TAL provides for this type of simulation. Such simulations are useful for evaluating new technologies or proposed solutions such as Secure Border Gateway Protocol (S-BGP).

- **Participate in Community Research Projects:** The NCS is moving beyond its current role as a patron or sponsor of research, to become an actual participant in research efforts. Internet community projects—such as The Honeynet Project—provide an excellent opportunity for the NCS to increase its respect and recognition within research and development circles. It will also enhance the NCS' expertise in critical areas. The TAL supports this activity.

- **Support Training:** The TAL provides an environment to support ongoing hands-on technical training, an alternative to expensive vendor-provided training.

Internet Monitoring Framework

Although the mission of the NCS has traditionally focused on the telecommunications infrastructure of the U.S., the borderless nature of the Internet has put the NCS in a position where it must concern itself with network behavior on a global basis. Although awareness worldwide is essential, the focus remains on North America.

The IMF effort is a result of White House direction to develop an Internet situational awareness capability in anticipation of further and more intense cyber attacks. The project, started in FY 2001, has an evolved capability to monitor Internet network-to-network performance. During FY 2003, the NCS prototyped two additional tools, a worm detection system and a Border Gateway Protocol (BGP) route update monitoring system, under the IMF. The worm detection system classifies and reports attack traffic, such as viruses and worms, directed at Internet hosts, and the BGP system monitors for anomalous conditions in BGP router messages that may indicate attacks or other problems with the routing infrastructure. During the coming fiscal year, the NCS will build on this work, developing enhanced prototype tools for visualizing and displaying Internet activity and topology, and correlating between current datasets.

Advanced Technology Group

The NCS Advanced Technology Group (ATG) investigates new and emerging technologies that may prove beneficial to NS/EP users. During the past year, the ATG researched a range of NS/EP communications topics such as Telecommunications Electromagnetic Disruptive Effects (TEDE), conducted an Emergency Notification System (ENS) study and pilot project; and, as directed by the White House, conducted a commercial SATCOM feasibility study in support of NS/EP communications.

Telecommunications Electromagnetic Disruptive Effects

Title 5 of the Code of Federal Regulations (C.F.R.), Part 215, assigns the Executive Agent of the NCS as the Federal Government's focal point for electromagnetic pulse (EMP) technical data and studies concerning telecommunications. The NCS, specifically the ATG, coordinates and approves these tests and studies and keeps the National Security Advisor informed of them. The ATG also looks at disruptive affects due to magneto hydro dynamics, high-powered microwaves, directive energy systems, high-radiation environments, solar flares, and the affects of lightning.

Since 1978, the ATG has coordinated and conducted numerous studies in the following topical areas:

- Susceptibility of telecom infrastructure to EMP
- Approaches to protection
- Hardening surveillance and maintenance
- Protection for new technologies and systems
- Affordability of EMP protection program due to competitive work.

Recent studies coordinated and conducted by the ATG include disruptive effects to—

- Routers and servers
- Fiber cable radiation hardness
- Dense Wave Division Multiplexing (DWDM) systems
- Communications infrastructures due to directed energy.

Emergency Notification System

The ENS study, directed by the White House, is designed to examine alternatives for notifying NS/EP personnel and for alerting segments of the general population about emergencies. The study investigates various ways to enhance existing methods of notification, in addition to exploring new methods.

An initial analysis concluded that no single technology or medium could be relied upon to provide timely notification to essential individuals or groups needing critical information. Therefore, the approach is to identify the most effective combination of technologies and communication modalities that would facilitate efficient emergency notification delivery. The ENS pilot provides notification capabilities for critical NS/EP personnel, and Federal and State Emergency Command Centers. The study and ENS pilot are designed to gain a better understanding of the required features, capabilities, and possible vulnerabilities in these types of communications.

Commercial Satellite Communications Feasibility Study

In July 2002, as directed by the White House, the ATG commenced a satellite study to determine the feasibility of using satellites for NS/EP. The objectives of the study are to—

- Develop a comprehensive view of the commercial satellite industry as it relates to non-DOD and Intel communities
- Delineate commercial SATCOM vulnerabilities
- Analyze Government's commercial SATCOM needs
- Determine ways to use commercial SATCOM to meet Government's NS/EP needs
- Determine feasibility of a commercial SATCOM program to satisfy NS/EP communications needs.

The satellite study was divided into three phases:

- Phase-1—completed in April 2003
  - Examined baseline capabilities of existing commercial satellite infrastructure
  - Identified and made an initial assessment of key satellite system vulnerabilities.
- Phase-2—commenced in May 2003
  - Analyzed Federal agencies' satellite communications use vis-à-vis NS/EP functional requirements
  - Postulated candidate commercial NS/EP SATCOM programs
  - Phase-2 report was completed in August 2003.
- Phase 3—Commenced in August 2003 with the following objectives:
  - Convene an industry and Government joint panel of experts to review and validate postulated NS/EP commercial SATCOM programs
  - Analyze risk and estimate program costs
  - Select and initiate an NS/EP commercial SATCOM satellite program(s).

CRITICAL INFRASTRUCTURE PROTECTION DIVISION

The Critical Infrastructure Protection (CIP) Division includes four branches: the Operations Branch, the Planning, Training, and Exercise (PT&E) Branch, the Operational Analysis (OA) Branch, and the Information Technology (IT) Branch. A Division Resource Coordinator and a CIP Project Coordinator assist the CIP Division Chief in managing and coordinating special projects and programs in the areas of budget, contracting, personnel/resources and project management.

The Operations Branch is responsible for response operations, information sharing activities, and priority telecommunications. The Operations Branch coordinates emergency response operations in all-hazards environments. This activity includes activating and staffing emergency operations teams (EOT), producing and maintaining standard operating procedures, developing and maintaining fly-away kits for use during

response operations, and maintaining the readiness of the National Coordinating Center for Telecommunications (NCC) Operations Center and NCC and Office of the Manager, National Communications System (OMNCS) relocation sites. The Operations Branch is also responsible for the day-to-day operations of the NCC and the Telecommunications-Information Sharing and Analysis Center (Telecom-ISAC).

The PT&E Branch is responsible for developing, conducting, and participating in national security and emergency preparedness (NS/EP) and CIP-related national, regional, and organizational exercises and operational training to ensure OMNCS staff and NCS member organizations are prepared to conduct essential emergency response telecommunications functions. The PT&E Branch supports several interagency working groups focused on emergency response, continuity of operations (COOP), and continuity of Government (COG) planning. With the increased emphasis on critical infrastructure protection, the CIP Division established a Division Outreach Coordinator in the PT&E Branch to develop and maintain an integrated outreach strategy. The PT&E Branch also hosts the NCS Individual Mobilization Augmentee (IMA) Unit, which consists of U.S. Army Reserve Signal Corps officers who may be activated for duty to assist the OMNCS during emergency operations.

The OA Branch is responsible for developing analytical assessments of physical and cyber threats to and vulnerabilities of the public network affecting NS/EP telecommunications. These assessments are intended to facilitate insurance of the availability and security of telecommunications services despite threats to or disruptions of the telecommunications infrastructure.

The IT Branch is responsible for providing policy, guidance, and technical support for OMNCS IT. This includes IT acquisition, policy, security compliance and technical support in the development and fielding of operational tools, systems, and networks.

National Coordinating Center For Telecommunications

The NCC is a joint industry-Government body whose mission is to assist in the initiation of national coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities under all conditions of crises or emergencies.

The 2001 attack on the U.S. provided the NCC with lessons learned to enhance NCC capabilities, including—

- Upgrades to the facilities, and technical and communications capabilities at the NCC and at NCS relocation sites
- Updates to operational procedures
- Augmentation of the organizational structure, skill sets, and training of NCC response elements
- Development of improved methods to enhance information management within the NCC Emergency Operations Teams (EOTs) and other OMNCS response elements.

Major NCC activities in Fiscal Year (FY) 2003 included—

- Development and implementation of additional strategies to further encourage new membership to the NCC and Telecom-Information Sharing and

Analysis Center (ISAC), including additional non-traditional service providers and equipment manufacturers. The following companies joined the NCC during FY 2003—Americom, AT&T Wireless, Cable & Wireless, Intrado, Level 3, McLeod USA, Nextel, PhotonEx, and TIA.

- Continued staffing of the 24 hours, 7 days a week (24x7) NCS Watch Desk in the Department of Defense's (DOD) Global Network and Security Operations Center (GNSOC) to foster information sharing with industry and coordinate information sharing among Government Network Operations Centers (NOC).

- Enhanced procedures to ensure effective information sharing with critical partners, such as other ISACs, the Federal Computer Incident Response Center, and the National Infrastructure Protection Center.

- Maintained an effective working relationship with both the Canadian Government and the telecommunications industry in Canada. In June 2003, the Manager, NCC attended the Canadian Telecommunications Cyber Protection meeting. Additionally, the Canadian Federal Government continues to identify personnel from Industry Canada and the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) who could be deployed to the NCC to coordinate response efforts requiring U.S./Canada cooperation.

- Continued a bilateral relationship with Mexico to foster the creation of a Civil Emergency Telecommunications Advisory Group between the U.S. and Mexico, and eventually, a tri-lateral body to work critical telecommunications infrastructure cross-border issues.

TELECOM-ISAC

The Telecom-ISAC is a function of the NCC that builds on existing NCC membership, procedures, and trust relations to facilitate voluntary collaboration and information sharing among 33 industry member companies and associations and between the telecommunications infrastructure industry and Government. During FY 2003, membership in the Telecom-ISAC increased from 24 to 33 member companies and associations, a 37.5 percent increase. New members included Americom, AT&T Wireless, Cable & Wireless, Intrado, Level 3 Communications, McLeod USA, Nextel, PhotonEx, and Telecommunications Industry Association.

A key component of the Telecom-ISAC is the 24x7 Watch and Analysis Operation (WAO). The WAO performs triage for all NCC functions, manages the entire Telecom-ISAC information sharing process, and provides an analysis function for the ISAC. Senior level watch analysts onsite in the NCC Operations Center are closely integrated with the industry representatives of ISAC member companies and the Government operations staff. In FY 2003, the WAO continued to add value to CIP through its extensive ongoing technical and liaison support activity and expansion of the level of daily analysis activities through situation monitoring of impending or ongoing events and incident response capabilities. As of March 1, 2003, the WAO became part of a combined virtual watch within the Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection Division (IAIP),

added a 24x7 Infrastructure Coordination desk at the Homeland Security Operations Center, and continued to staff a 24x7 liaison to the Defense Information Systems Agency (DISA) GNOSC, DOD-Computer Emergency Response Team (CERT), and the Joint Task Force-Computer Network Operations. The WAO also provided a full-time member to a combined team tasked to coordinate activities among the three physically separate watch and analysis components of DHS IAIP.

Global Early Warning Information System

In March 2002, the President's CIP Board tasked the NCS to evaluate the feasibility of creating a Global Early Warning Information System (GEWIS) of cyber attack activity on critical national infrastructures using sensor data currently available from the private sector. The NCS feasibility study recommended using the existing Telecom-ISAC base infrastructure and processes, in particular its WAO, to develop and implement the GEWIS capability.

GEWIS will combine existing data and automated knowledge management capabilities to provide a more holistic view of the Internet infrastructure performance, provide near-real time insight into anomalous Internet behavior, attacks, and potential impacts, and integrate into a superset process involving expert human analysts, rapid dissemination vehicles for actionable, early warning information, and appropriate CIP constituencies.
Early warning will help CIP entities, both public and private, reduce their reaction time to infrastructure events and become more proactive in their defense postures. FY 2003 saw completion of the system requirements analysis phase begun in FY 2002, and preliminary and critical design reviews for Increment 1 of GEWIS. FY 2003 GEWIS development focused on selecting and evaluating prototype data sources and building a scalable and extensible framework that will adapt rapidly to accept new data sources and support extended data fusion models and early warning capabilities.
FY 2003 culminated in delivery of the Increment 1 Initial Operating Capability (IOC) and Increment 1 suite of operational data feeds.

Alerting And Coordination Network

Prior to January 1, 2001, the National Telecommunications Alliance (NTA) managed and operated the Alerting and Coordination Network (ACN)—a switched, private line network—to provide emergency communications among the Regional Bell Operating Companies, their suppliers, and certain Government agencies. When NTA dissolved on January 1, 2001, the ACN was in jeopardy of being disbanded. Because the ACN provides emergency backup communications capability that could help coordinate response to and recovery from a widespread network outage, the Director, Office of Science and Technology Policy (OSTP), directed the NCS to acquire the assets and provide operational support to ensure the continued viability of the ACN. Operational responsibility for the ACN was incorporated into the NCC operations.

In 2002, following the development of a transition plan to support the changeover of the ACN from carrier-based funding to a Government-funded model, the NCS decided to enhance the ACN by implementing a private IP backbone network in a seamless, server-based environment. This new

topology provides several levels of fault tolerance and scalability. The enhanced ACN continues to support the NCC as well as existing ACN participants, the Telecom-ISAC and a new network, Critical infrastructure Warning Information Network (CWIN).

The OMNCS is working with industry to establish procedures for maintaining and utilizing the ACN and expanding its availability within the telecommunications infrastructure. The ACN is evolving to provide coordination across other critical infrastructures in the event of outages in the telecommunications infrastructure. Major changes were initiated in FY 2002 to upgrade the ACN to a Voice over IP (VoIP) network. Conversion of existing ACN connections began in FY 2002 and will be completed in FY 2003.

Critical Infrastructure Warning Information Network

In 2001, the NCS was tasked by the National Coordinator for Security, Infrastructure Protection and Counterterrorism, National Security Council (NSC), to develop, implement, and manage CWIN, designed to facilitate the dissemination among key Federal departments and agencies and industry time-sensitive warnings regarding imminent threats or ongoing attacks against the Nation's telecommunications infrastructure. The NCS engineered the CWIN as a reliable and survivable network capability with no logical dependency on the Internet or the Public Switched Network (PSN). As a result, if either the Internet or the PSN suffer disruptions, the CWIN will not be affected.

Deployment of CWIN to user sites began in mid-FY 2002 and has continued through FY 2003. CWIN participants now include seven Federal watch centers at five geographically dispersed locations and approximately 30 other sites, including telecommunications and ISPs and CIP entities. The CWIN management plan included adding up to 75 participants each calendar year, but may be expanded in the future.

On several occasions in 2003, CWIN proved its utility when it maintained communications among participants when specific cyber networks suffered disruptions. Recognizing CWIN's tremendous value and utility, senior management at DHS expanded the mission of the CWIN beyond "cyber" to include information sharing and coordination for all of the Nation's critical infrastructures.

North Atlantic Treaty Organization Civil Communications Planning Committee

The OMNCS represents the U.S. on the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), its telecommunications working group, and other subsidiary bodies. The Department of State (DOS) detailee to the OMNCS heads the delegation. CCPC purview extends to telecommunications and postal services. During FY 2003, the CCPC met twice in plenary session: once at NATO headquarters in Brussels, Belgium, and the other in Kiev, Ukraine. Its telecommunications working group met four times, and the postal working group met twice. An ad hoc working group tasked to develop a paper on the threat of the Electromagnetic Pulse (EMP)/high-powered microwave to civil communications met three times.

Major CCPC FY 2003 activities and accomplishments include—

- Approved the 2003 CCPC Work Program based upon ministerial guidance. The program includes civil support for alliance military operations, support for civil emergency planning, protection of the civil population against weapons of mass destruction, and cooperation with partner nations.

- Continued to operate under an "Article 5" situation. Article 5 of the North Atlantic Treaty states in part, "The parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." The threat of terrorism is considered a global problem by the 46 NATO nations.

- Drafted a paper outlining the consequences of the EMP and high-powered microwave relative to the disruption of civil communications.

- Formulated plans for a NATO CERT.

- Shared with NATO nations the results and mitigation strategies identified as a result of the anthrax attacks in the U.S. Postal Service.

- Formulated policy regarding support for national authorities during civil emergencies. The examination of civil emergency planning consequences in the areas of the broadcasting sector, digital broadcasting technologies, the usage of broadcasts for public information and warning and other services was conducted. A paper is being developed with conclusions and recommendations for presentation at plenary.

CIP–International Outreach

The OMNCS participated in the following bilateral discussions to gain international cooperation for protection of critical infrastructures:

- Mexico, January 19–21: The Manager, NCC and the DOS representative to the NCS traveled to Mexico City to meet with representatives of the Mexican Secretaria De Comunicaciones Y Transportes to share the successful organizational processes and programs with members of the Mexican government and telecommunications industry representatives. Following, the Manager, NCC and the DOS representative, as part of a larger official U.S. delegation, led by members of the Office of Homeland Security (OHS), attended a day-long session with members of the U.S. and Mexican CIP Steering Committee meeting to establish plans for critical sector working groups.

- Canada, March 18–19: A delegation from Ottawa, Canada, led by the Director General of External Relations and Public Affairs of the Canadian Office of Brussels met with U.S. counterparts of the U.S. CIP Steering Committee in Washington, DC, to review CIP sector work plans, discuss current CIP postures in the U.S. and Canada and propose next steps for action.

- Germany, June 26–27: A high-level delegation led by the Senior Coordinator for International CIP Policy, Bureau of Political Military Affairs, U.S. DOS, and composed of members from industry and the U.S. Government, traveled to Berlin, Germany, to begin the first in a series of

CIP information sharing meetings with members, CIP sector industry representatives, and the German government.

- Netherlands, June 26–27: The Political–Military Affairs Bureau, U.S. DOS, hosted an official CIP bilateral meeting composed of members from the U.S. Government departments and agencies as well as members from Dutch Government agencies concerned with CIP and information sharing issues. The bilateral meeting was a direct result of earlier talks held at The Hague on law enforcement and counterterrorism topics. Members focused on several sector concerns in water and transportation, telecommunications and cyber issues.

The DOS representative continues to attend NATO CCPC meetings in coordination with the U.S. telecommunications representative on behalf of the NCS.

Standing Subcommittee On Upgrades

Under the authority of three Presidential Directives and one Executive Order (E.O.), the Deputy Manager of the NCS serves as Chair of the Standing Subcommittee on Upgrades (SSU), an interagency group of experts responsible for "hotline" operations. The group has the following mandates:

- Convene as necessary to set technical parameters and establish overall milestone schedules for upgrade enhancements, to assign engineering and procurement responsibility, and to review milestone achievements

- Provide guidance and direction to, and approve composition of, the U.S. Technical Experts Delegation, and approve scheduling, agendas, and U.S. positions for bilateral and/or multilateral meetings on technical matters relating to Government-to-Government communications links

- Keep the NSC informed, as appropriate, of the activities of the SSU and U.S. Technical Experts, and request NSC guidance on non-technical (policy) matters as appropriate.

The Deputy Manager of the NCS served on the Delegation to the U.S.-Russian Meeting of Technical Experts held in Moscow September 22-26, 2003, and provided technical advice relative to the U.S. and Russia.

Telecommunications Service Priority Program

The Telecommunications Service Priority (TSP) Program, established by the Federal Communications Commission (FCC) Report and Order (R&O) dated November 17, 1988, provides a regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications services. The FCC authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments. FY 2003 TSP activities included—

TSP Operations

The OMNCS, in close coordination with the TSP Oversight Committee (OC), continued the day-to-day management of the TSP Program, placing special emphasis on the future direction of the Program in a changing homeland security environment. Currently there are more than 52,000 total active TSP assignments in support of NS/EP

communications. During FY 2003, the OMNCS issued more than 325 provisioning TSPs to aid in the installation of critical circuits. The TSP user base increased by more than 50 new organizations, with significant new representation from State and local governments and the financial sector, although military departments continue to be one of the largest traditional users of TSP services.

The OMNCS facilitated meetings of the TSP OC, which identifies, reviews, and recommends actions to correct or prevent systemic problems in the TSP Program. Working with the TSP OC, the OMNCS continued to focus its efforts on several operational TSP issues, including difficulties in the areas of negotiating TSP for non-universal broadband services, determining appropriate priority levels for TSP assignments, and policies and procedures implemented by the Defense Information Technology Contracting Office to provision DOD TSP requests. The OMNCS also initiated a comprehensive customer satisfaction survey, designed to collect feedback from TSP participants. The NCS will complete its analysis of the survey results in FY 2004, using TSP user and vendor input to formulate and implement TSP improvements.

Given the high dependence of the financial services sector on telecommunications assets, the Federal Reserve Board remained a representative to the NCS in FY 2003. This presence helped coordinate CIP activities between the telecommunications and financial services sectors. As a result, the scope of TSP in the financial sector began expanding to include payment systems, securities markets, and futures markets.

TSP Information Technology Solutions

The OMNCS continues to utilize innovative IT solutions in support of TSP Program operations. During FY 2003, the NCS's Office of Priority Telecommunications IT efforts focused on enhancing the usability and data integrity of the Priority Telecommunications System (PTS), the information system used to support TSP provisioning and restoration. These enhancements have resulted in more efficient processes by which OMNCS, TSP users, and telecommunications vendors can input and update information related to crucial NS/EP telecommunications circuits and assets.

Throughout FY 2003, the TSP Web site (http://tsp.ncs.gov) was regularly revised to distribute crucial TSP Program information to the NS/EP community. Among the information included on the site are specific instructions for using the PTS and e-forms applications, which offer easy, secure, and universal mechanisms for performing various TSP processes.

TSP Outreach Strategy

During FY 2003, the growing membership of the TSP Program was a reflection of the increased participation of non-traditional actors in homeland security activities. Ongoing outreach efforts were maintained to new telecommunications service providers, State and local NS/EP personnel, first responders, and federally sponsored private sector entities. Cross-infrastructure CIP initiatives also figured prominently among FY 2003 TSP outreach activities, as various financial institutions, the Nuclear Regulatory Commission, the Transportation Security Administration and the American Association of Railroads were briefed and/or trained on TSP processes.

Although the TSP Program has been proven effective in support of homeland security efforts and the ongoing war on terrorism, the OMNCS and TSP OC determined that increasing the TSP user base to include more crucial public safety and security assets remains a high priority. For example, the OMNCS and TSP OC found that a low percentage of 911 Public Safety Answering Points (PSAP) were currently enrolled in the TSP Program. To reach these PSAPs, the OMNCS will implement a targeted outreach campaign in FY 2004, utilizing regional workshops, published articles, and working relationships with major national public safety organizations.

Network Security Information Exchange Activities

The joint meetings of the President's National Security Telecommunications Advisory Committee (NSTAC) and Government Network Security Information Exchanges (NSIE) provide a trusted environment in which industry and Government representatives can exchange information on threats to and vulnerabilities of the Public Network (PN). The NSIEs focus on technical issues affecting the security of the PN, such as unauthorized penetration or manipulation of the PN software, databases, and other infrastructures supporting NS/EP telecommunications services.

The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the PN and its supporting infrastructures. In FY 2003, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including protecting intellectual property assets/rights, security training and awareness, and threat guidelines for electronic attacks to the PN. The Security Requirements Working Group (SRWG) produced the document titled, *Operations, Administration, Maintenance, & Provisioning (OAM&P) Security Requirements For Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*, providing requirements that will allow vendors, Government agencies, and service providers to implement a secure telecommunications network management infrastructure. The document was presented and accepted for T1M1 and American National Standards Institute (ANSI) standards.

In FY 2003, the NSIEs met in the United Kingdom (UK) at a meeting jointly co-hosted by British Telecommunications and the UK National Infrastructure Security Coordination Centre. Included in the NSIE meeting were briefings and endorsements by leading figures in the UK information assurance and security community, including the Security and Intelligence Coordinator & Permanent Secretary (Cabinet Office), the Director of the Communications-Electronics Security Group, and the Director of NISCC. As an outgrowth of this meeting and British Telecommunications (BT)'s participation in the NSIEs, the UK has established a UK NSIE program of industry and UK government participants. Using the trusted environment of the NSIEs, the Border Gateway Protocol (BGP) Working Group was formed in FY 2003 to study and develop filtering guidelines for BGP.

Shared Resources High Frequency Radio Program

The Shared Resources (SHARES) High Frequency (HF) Radio Program continues to provide emergency communications in support of all-hazard situations and special

operations. Approved by the Executive Office of the President in 1989, SHARES provides the Federal emergency response community with a single, interagency emergency message handling system for the transmission of NS/EP information by bringing together existing HF radio resources of Federal and federally affiliated organizations when normal communications are destroyed or unavailable. SHARES incorporates the resources of 1,105 HF radio stations contributed by 91 Federal, State, and industry organizations and located in all 50 states and overseas.

During FY 2003, SHARES conducted 95 on-air operations. The SHARES Coordination Network was raised to Operational Level 2 to support four separate HIGH (Orange) threat advisory level conditions since DHS instituted the Homeland Security Advisory System in March 2002. SHARES response to these special operations has been greater during FY 2003 than any SHARES operations conducted over the past decade.
One thousand ninety-six SHARES stations, representing 54 Federal, State, and industry organizations, located in all 50 states, Puerto Rico, Virgin Islands, and the District of Columbia, participated in the operations. SHARES also conducted special operations support of Hurricane Lili, Typhoon Pongsona (Guam), the Super Bowl, and the Columbia Disaster. A total of 9,706 station availability reports were submitted to the 15 SHARES Coordination Stations during these operations.

During FY 2003, readiness continued to be emphasized. SHARES continues to conduct three nationwide SHARES exercises per year, as well as the weekly SHARES Net conducted for a 2-hour period each Wednesday. The SHARES Interoperability Working Group (IWG), a permanent body established under the NCS Council of Representatives (COR), continued to meet bi-monthly to coordinate SHARES network activities and to address issues affecting interoperability of Federal HF radio systems. The IWG, composed of 143 members representing 103 organizations, continued to expand the digital and Automatic Link Establishment structure of the nationwide SHARES Coordination Network, and continued to support new HF technologies. The IWG also expanded awareness of SHARES throughout the Federal emergency preparedness community by conducting 23 SHARES Outreach Program events.

Planning, Training, And Exercise Support

The Planning, Training and Exercise (PT&E) Branch is responsible for ensuring a cadre of skilled civilian and military reservist personnel are qualified and ready to provide emergency response support during crises and emergencies. During FY 2003, the PT&E Branch successfully coordinated and performed the following activities:

- Emergency Response Training (ERT) Seminars: ERT seminars are a highly visible and successful training program for the NCS. In October 2002, the final presentation of the PHASE 3 course of instruction was given in Federal Region V (Chicago, Illinois) to an audience of approximately 75 Federal, State, and local emergency planners and operators. During FY 2003, the NCS kicked off the PHASE 4 series of visits and presentations within each of the Federal regions. The PHASE 4 course of instruction showcases the NCS priority telecommunications programs and facilitates an interactive tabletop discussion among the seminar

participants of communications resources and challenges that impact emergency response operations. The seminar goals are to increase awareness of the capabilities of Emergency Support Function (ESF) #2 and to emphasize the best use of finite industry and Government resources.

- Emergency Operations Team Training: During FY 2003, the improved version of the Local Exchange Mapping (LECMap) software, now called the *Integrated Mapping and Analysis Program (IMAP)*, was introduced and a series of training sessions provided all personnel with an introductory orientation and hands-on familiarity. The new software enables users to plot landline and wireless telecommunications network connectivity throughout the U.S. and the Caribbean, and to approximate the degree of service disruption after a severe storm or other disasters. Internal training was provided periodically during the year to familiarize personnel with ESF #2 responsibilities during a disaster. In addition, a re-deployment training exercise was executed to familiarize team members with the alternate location facilities and working environment.

- Exercises: The OMNCS conducts and participates in both internal and external exercises to maintain expert knowledge of, and proficiency in, the management, integration, and employment of NS/EP telecommunications resources. The bi-annual Top Official II (TOPOFF-2) exercise is an example of a series of external exercise events that involved the NCS telecommunications industry representatives and the NCS Regional Managers.

OMNCS Individual Mobilization Augmentee Program

The OMNCS continues its IMA Program, which is supported through the Department of the Army's IMA Program. The augmentees may be activated and deployed to assist the OMNCS staff, or they may be deployed to regional locations as ESF #2 Emergency Communications staff to assist the NCS Regional Managers during national emergency operations and disaster response planning. The NCS IMA Program provides a valuable array of skilled Army Reserve personnel to augment telecommunications response activities. During Presidentially declared disasters, the IMA Program provides the NCS with a surge capability to deploy and react to a myriad of situations associated with ESF #2 operations. IMA personnel are often among the first Federal disaster response personnel to reach a disaster scene. Many of these reserve officers are telecommunications professionals in their full-time civilian careers and are able to apply their skills when responding to Federal emergencies. The IMA Program continues to provide an extremely important and invaluable service to the OMNCS NS/EP mission at the national and regional levels.

During FY 2003, the NCS Augmentees provided 14 duty days to support disaster relief operations. In December 2002, Augmentees were deployed to the Regional Operations Center in Oakland, California, and the Disaster Field Office in Guam to provide assistance after the Super Typhoon Pongsona disaster. The Unit retired three officers and welcomed three new members in FY 2003.

Continuity of Operations

As directed by E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*, and Presidential Decision Directive (PDD) 67, the OMNCS maintains an active and robust Continuity of Operations (COOP) program that ensures its critical mission functions will be sustained throughout any emergency. The OMNCS continues to update contingency plans, procedures, and facilities to effectively ensure continuation of its critical mission functions during an all-hazards emergency.

A robust and effective COOP testing, training, and exercise program has been developed to determine the validity of the plans and to ensure the operational readiness of the OMNCS personnel who will be responding to the emergency. Through its involvement in the Interagency COOP Working Group, the OMNCS is participating in the planning of the May 2004 National Capital Region deployed COOP training and exercise event (FORWARD CHALLENGE 04) for the Federal Executive Branch.

CIP Division Outreach

The NCS CIP Division officially launched its tradeshow and events program this spring 2003, exhibiting with a new information booth at the *Emergency Medical Service (EMS) Today Conference* in Philadelphia, Pennsylvania. Since then, the booth has made numerous other appearances to promote the NCS and its Priority Telecommunications programs and services. Designed and developed in the winter of 2002, the Tradeshow Outreach Program has become a significant element of the more comprehensive strategy for the NCS to reach out to audience segments that have a NS/EP mission.

The program's goal is to promote awareness of the NCS and its priority telecommunications services to support NS/EP efforts across Federal, State, and local government, critical infrastructure industries, and other authorized NS/EP organizations. The telecommunications programs that are featured with fact sheets and other media materials are TSP, GETS, Wireless Priority Service (WPS), SHARES-HF Radio, and One-Stop Shop Services (OSSS). CIP services support the initiation, coordination, and restoration of NS/EP telecommunications during national crises or emergencies, and regional disasters. The Tradeshow Outreach Program identifies the ways in which these services can benefit various emergency management organizations and the importance of incorporating such services into their emergency response plans.

The Tradeshow Outreach Program is proving to be an effective way for the NCS to reach out to its current and future customers. The information booth will continue to travel nationwide, providing critical information to NS/EP audiences about the NCS and priority telecommunications programs and services. Identified below are the tradeshow events where the booth was displayed during 2003.

- Orlando, Florida, March 30–April 2: Disaster Recovery Journal
- Arlington, Virginia, April 23–24: NCS Regional Managers and IMA Conference
- Anaheim, California, April 3–May 2: National Academies of Emergency Dispatch (CIP-telecom)
- Arlington, Virginia, May 14–16: Homeland Security Summit and Exposition

- Atlantic City, New Jersey, May 20–23: Emergency Management Association, Maryland—Directors Meeting

- Atlanta, Georgia, June 17: NCS ERT Seminar

- Washington, DC, July 23–25: Government Security Expo and Conference

- Dallas, Texas, August 22–25: International Fire and EMS Convention 2003

- Gaithersburg, Maryland, September 9–10: Securing the Homeland

- San Diego, California, September 21–24: Disaster Recovery Journal.

One-Stop Shop Service

The NS/EP Priority Communications OSSS enables NCS customers to acquire NCS NS/EP priority communications information, services, programs, and operations from a single source. The goal of OSSS, illustrated in the graphic, is to provide an efficient and effective means of managing and supporting the consolidated operations/user support missions and functions of the NCS for priority communications services under any circumstance. The OSSS consolidation began its implementation in September 2002 and includes user and operational support for the following programs:

- GETS

- WPS

- TSP Program

- ENS Pilot Program

- SHARES-HF Radio Program.

FY 2003 accomplishments include implementation of—

- The OSSS Call Center as a single number for all NCS customers to call for priority communications services. The OSSS Call Center can be reached at 1-866-NCS-CALL (866-627-2255), or in the Washington metropolitan area at 703-676-CALL (703-676-2255), Fax: 703-607-4984.

- A consolidated Web-based approach for NS/EP priority communications services using a Web portal to maximize the overall benefits of one-stop service. The NCS home page, www.ncs.gov, will serve as the portal with users being automatically linked to the appropriate Web pages for specific services.

- An architecture utilizing Web-based technology and a Web-based information delivery service that provides the foundation for the NS/EP communications services information and processes. Consolidating the support and technical information process for all NS/EP communications services under a single organizational environment provides continuity and integrity of management for the services/programs.

To support this effort, an initial concept of operations was developed and various standard operating procedures are now under development and/or consolidation. A roadmap for the future is also under development.

- An intensive marketing and outreach program to expand the user base for the OSSS programs/services that is supported by a marketing strategy plan as well as development of various marketing tools using both Web-based technology and other media as appropriate.

Operational Analysis

The OA Branch of the CIP Division serves as the focal point for developing analytical assessments of physical and cyber threats to, and vulnerabilities of, the public network affecting NS/EP telecommunications. Analytical initiatives conducted during FY 2003 include—

DOE SS7 Analysis

The Department of Energy (DOE) Office of Energy Assurance asked the OA Branch to provide assistance in assessing the physical security and vulnerabilities of the Signaling System 7 (SS7) network in the Manhattan area. For this study, the OA Branch identified the major characteristics of signaling assets in the area, including physical location, logical connectivity, operating carriers, and equipment manufacturers. This information was then used to determine if any single points of failure existed in the signaling network.

Cellular User Information Exchange Vulnerability Study

The NCS established the WPS Program to provide NS/EP users with priority access to U.S. cellular networks during times of emergency or crisis. One aspect of a wireless call not addressed by WPS involves the process of exchanging cellular user information, which occurs whenever a cellular user turns on their phone or operates in a different network or service area. The OA Branch has initiated a study to identify potential vulnerabilities associated with the cellular user information exchange process and to determine the effects of various network scenarios on the exchange process. Results from this study will allow the NCS to make recommendations for improving the ability of WPS to handle the needs of priority users.

Joint Telecommunications/Financial Services Pilot Recoverability Assessment

The OA Branch worked in conjunction with the NCC telecommunication carriers and the BITS Financial Services Roundtable to plan and conduct a Joint Telecommunications/ Financial Services Sector Pilot Recoverability Assessment. The assessment examined possible telecommunications network resiliency and diversity issues in a major metropolitan area that could affect core financial service processes. Participants representing both sectors developed a set of lessons learned and best practices designed to enhance network resiliency and diversity in support of the core processes.

TOPOFF2

The OA Branch participated in this year's TOPOFF2 exercise, a counterterrorism drill involving both Federal and local government agencies. OA Branch analysts responded to numerous ad hoc analysis requests

during the 5-day exercise. Telecommunications impact analyses were conducted to address various scenarios, including a dirty bomb attack in Seattle, Washington, quarantines over large populated areas in Chicago, Illinois, and nonspecific threats against New York City, New York.

Public Safety Wireless Network Program Support

The NCS recently established an alliance with the Public Safety Wireless Network (PSWN) Program in part to develop and enhance communications interoperability solutions for the NS/EP and public safety communities. In support of this alliance, the OA Branch supported efforts to evaluate the interdependencies between the public switched telephone network and a statewide land mobile radio communications system.

Wireless Messaging Network Vulnerability Study

During the events of September 11, 2001, users of two-way pagers and Blackberry-like devices were able to transmit messages successfully when other means of communications, such as cell phones failed. The capabilities of these wireless messaging devices and their nationwide coverage make wireless messaging a good medium for emergency communications that may provide benefit to the NS/EP community and first responders. However, the wireless messaging networks supporting these devices have not been fully explored. The OA Branch initiated a study to examine the robustness of the wireless messaging network architecture, its dependence on the wire line network, and its potential vulnerabilities and mitigation options. The study will allow the OA Branch to make recommendations for improving the use of wireless messaging devices during emergencies.

Infrastructure Interdependency Analysis

The increasingly interdependent nature of our Nation's infrastructures has the potential to create new and hidden vulnerabilities that could be exploited to cause widespread damage to our Nation's infrastructures, economy, and national security. To uncover and mitigate these vulnerabilities, the OA Branch initiated the development of an operational approach for analyzing and assessing the interdependencies of the Nation's critical infrastructures. A series of case studies were initiated to exercise the approach and validate the applicability across all infrastructures. This approach will enable the OA Branch to conduct an interdependency analysis at an operational level and produce actionable results in a short timeframe when an actual outage occurs or when a threat against a critical infrastructure is imminent.

Information Technology Support

The IT Branch is responsible for ensuring that secure information systems enhance the performance and operational readiness of OMNCS personnel. These information systems encompass a range of capabilities, from DISA local access networks (LAN) to laptops, and are distributed over a variety of locations, including headquarters, alternate facilities, and mobile users.

As IT security has gained additional public scrutiny over the past year, the IT Branch has continued to work toward a secure environment and has assisted in efforts for the certification and accreditation of various systems. During the past year, the Branch has assisted in the reaccreditations of the TSP system, the NCS homepage server, the NSIE server, and the Emergency Response Link

(ERLink). The IT Branch assisted in the initial accreditation of the Watch Daily Analysis (WDA) system. Ongoing efforts include technical and security review of the GEWIS and CWIN in advance of certification. Additionally, the IT Branch ensured that NCS systems and practices are maintained within evolving security guidelines.

In support of NCS users, the IT Branch collected requirements and is working with the DHS to migrate users onto DHS assets while maintaining a secure and functioning environment. As the DISA Local Area Network (LAN) liaison, the IT Branch represented OMNCS interests in such areas as proposed DISA network enhancements, the migration of desktops to Win2000, and the implementation of Common Access Cards. The IT Branch assessed impacts to operations resulting from the implementation of new, or the modification to, existing DOD and DISA policy, including the impact of shutting down ports and protocols to the network and the migration of equipment into a demilitarized zone subnet.

PLANS AND RESOURCES DIVISION

The Plans and Resources Division provides centralized management and oversight to the Office of the Manager, National Communications System (OMNCS) for acquisition matters, financial matters, strategic and performance management planning activities, staffing allocations, and other personnel-related matters. The Plans and Resources Division exercises authority and ensures accountability over all resources allocated to NCS programs.

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

PLANNING

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

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

FINANCIAL MANAGEMENT

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

program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits.

The Financial Team also leads in the development, coordination, and implementation of funding procedures as directed and provides guidance and assistance to all NCS agencies to ensure that their requirements are met. In addition, the Financial Team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

Acquisition Management

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

CUSTOMER SERVICE DIVISION

The Customer Service Division serves as the primary forum for coordination and collaboration among the Federal members of the NCS,other governmental entities, and private industries involved in critical infrastructure protection (CIP) and national security and emergency preparedness (NS/EP) programs and activities.

The division supports the NCS Committee of Principals (COP), the Council of Representatives (COR), and related working groups; the President's National Security and Telecommunications Advisory Committee (NSTAC) and its subordinate bodies; as well as public affairs and outreach activities for the NCS and the aforementioned committees. The following sections describe the Customer Service Division activities for Fiscal Year (FY) 2003.

NCS Committee Of Principals/Council Of Representatives

The COP is a Presidentially designated interagency group through which the President receives advice and recommendations on NS/EP telecommunications issues. The COP is the forum where senior Federal Government officials meet to exchange ideas and form recommendations that go directly to the Manager of the NCS, the Secretary of Homeland Security, and the President. This unique group that provides advice and recommendations on national security and emergency preparedness issues includes representatives from 23 Federal Departments and Agencies. The Department of Homeland Security (DHS) became a memeber of the interagency NCS and Committee of Principals when the President established the new department in March.

In October 2001, the COP was renamed as the Committee for National Security and Emergency Preparedness Communications by E.O. 13231. The same Executive Order (E.O.) created the President's CIP Board. However, with the creation of the DHS and the elimination of the CIP Board, the committee was renamed the Committee of Principals.

At the January 2003 COP meeting, Lt Gen Harry Raduege, Jr., Manager, NCS, discussed the pending move of the NCS into the DHS. He also noted that the NCS would be part of the new Directorate for Information Analysis and Infrastructure Protection (IAIP). During the meeting, the COP received updates on the Government Emergency Telecommunications Services (GETS), Wireless Priority Service (WPS), and Critical infrastructure Warning Information Network (CWIN). The COP also agreed to have NCS member organizations submit critical facilities information in accordance with a request from the Joint Telecommunications Resources Board.

The COR, a subordinate working group of the COP, met four times in FY 2003. The COR established the Critical Facilities Working Group (CFWG) to develop a template that a Government agency could use to identify the agency's critical NS/EP functions for which telecommunications services were essential; to identify the critical telecommunications facilities that were used to provide the agency's access to the Public Switched Network (PSN); to determine whether those facilities contained sufficient diversity and redundancy to ensure the agency could support its NS/EP functions over the PSN at all times; to ensure such facilities continued to contain adequate diversity and redundancy. Some of the CFWG's findings included the increasing importance and necessity of diverse telecommunications and the need to implement information security best practices. The COR also discussed the possibility of creating additional working groups to review the National Level Telecommunications Programs and NS/EP services and review agency security best practices.

The President's National Security Telecommunications Advisory Committee

The President's NSTAC highlighted key telecommunications issues at its NSTAC XXVI meeting held on April 30, 2003, in Washington, DC. During the Executive Session of the meeting, the NSTAC Principals and senior Administration officials reviewed the efforts of the last year and identified several issues for consideration for NSTAC XXVII. In FY 2003, the President's NSTAC celebrated its 20th anniversary and continued to provide industry-based advice and expertise on issues related to the implementation of NS/EP communications policy. The NSTAC members and the entities they represent are committed to this partnership in support of NS/EP on behalf of the United States.

NSTAC's Industry Executive Subcommittee Activities

During FY 2003, the NSTAC's Industry Executive Subcommittee (IES) continued to identify and develop communications issues critical to our national security and emergency preparedness for consideration and to direct the activities of its seven subgroups. The NSTAC addressed a variety of issues, including Internet security and architecture, vulnerabilities in telecom hotels and peering points, wireless security and communications, a research and development exchange, and legislative and regulatory issues. Specific subgroup activities and the results of their analyses, work, and recommendations to the President are discussed below.

NSTAC's Internet Security/Architecture Task Force

At the NSTAC XXV meeting, the Special Advisor to the President for Cyberspace Security discussed the serious threats to the Nation's telecommunications infrastructure posed by vulnerabilities within the Domain Name Servers and the Border Gateway Protocol. In response to these concerns, the IES, during the NSTAC XXVI cycle, created the Internet Security/Architecture Task Force (ISATF) to provide recommendations to the President on how to identify and remediate vulnerabilities in pervasive software/protocols and define the "edge" elements of the Internet to protect the "edges" of the Internet against attack or exploitation.

The ISATF, in its *First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software/Protocols* report, analyzed five stages relevant to identifying and remediating vulnerabilities in pervasive software and protocols: prevention, detection, information sharing, analysis, and correction. In the area of prevention, the task force advocated aggressive public-private research and development activities and cited the need to develop adequate alerting and warning systems to continue to support the operations of information sharing and analysis centers. The task force identified barriers to the effective detection of vulnerabilities, such as the myriad number of forums devoted to detection and the lack of standardization in reporting procedures. Third, the task force emphasized that there were significant barriers to information sharing, such as the Freedom of Information Act (FOIA) and liability concerns, and advocated the creation of legislation that would ease the sharing of critical information. The ISATF also concluded that the analysis functions within industry that detected and published vulnerabilities appeared to be adequate, but the Government might find some benefit in better leveraging available synergies by consolidating Government-funded analysis centers, where appropriate. Finally, the task force observed that although many organizations are successfully correcting and remediating vulnerabilities, a streamlined method for disseminating expeditiously corrective information to the telecommunications and ISP communities was not being utilized.

On the basis of the ISATF's analysis, the NSTAC made a variety of recommendations to the President. These recommendations included consolidating the Government-funded watch center operations of Federal agencies dedicated to the detection and dissemination of information related to Internet vulnerabilities into one organization. Further, the ISATF recommended establishing a lead organization within the DHS to coordinate a process with industry for warnings, notification, coordination, and remediation of widespread problems during a national emergency. The NSTAC also advocated funding efforts to identify and mitigate vulnerabilities in the most critical protocols or software relied upon within key sectors of the Nation's infrastructure.

In further efforts to better secure the Internet, the ISATF conducted an analysis of the edge elements of the Internet and determined that the Internet was not a single network, but a network of interconnected networks. As such, the concept of a single edge is "impractical" and could not be defined. The ISATF agreed that there was no single definition of the edge and that protective measures should focus on defending the Internet as a whole. In its

second report, *Edge Elements of the Internet*, the NSTAC advocated the continuation of Government efforts to identify the critical NS/EP missions and related functions that relied on the Internet and encouraged the parties responsible for those missions to ensure that they were adequately protected through redundancy and alternate capabilities. Furthermore, the NSTAC recommended ensuring that all products and services that composed the Internet had built-in baseline security features and that those capabilities were appropriately configured and kept up to date. The report also supported the development of a standard set of "key warnings and indicators" by Government, Internet security experts, and standards bodies for service providers to use as a baseline to measure security threats.

NSTAC'S VULNERABILITIES TASK FORCE

The IES chartered the Vulnerabilities Task Force (VTF) to examine possible risks associated with the concentration of critical telecommunications assets in telecom hotels and Internet peering points, as well as vulnerabilities involving equipment chain of control and trusted access procedures to telecommunications facilities.

The VTF, in its *Concentration of Assets: Telecom Hotels* report, stated that based on previous analyses, it was unlikely that the loss of assets located in a telecom hotel would cause a nationwide disruption of the critical telecommunications infrastructure. However, the VTF did note that analyses provided by the Department of the Navy's Joint Program Office for Special Technology Countermeasures revealed that loss of service of specific telecommunications nodes could adversely affect certain Government entities and their corresponding missions. As a result of the VTF deliberations, the NSTAC recommended the President (1) complete site-by-site risk analyses of mission-critical facilities to identify possible vulnerabilities that could affect the critical functions supporting those missions, providing adequate funding and resources to mitigate and remediate such vulnerabilities if they were found, (2) create a central mechanism to coordinate all Government infrastructure data requests to ensure timely and synchronized replies from the information and communications sector(s), (3) work with industry to protect assets from known threats by implementing a cross-functional warning system that had well-defined parameters and was consistently applied by both entities, and (4) adopt telecommunications services procurement security policy guidelines that would provide incentives to companies that followed Network Reliability and Interoperability Council (NRIC) best practices, high levels of security standards, and other recognized business contingency principles.

In its *Internet Peering Security* report, the VTF described how centralized locations were created to facilitate the exchange of Internet traffic among the various operators' interconnected networks. Those centralized locations became known as the first public peering points, or network access points (NAP), and later led to the development of direct or private peering points between network operators. The task force found that if a physical attack targeted multiple NAPs, traffic flow across the Internet could be impacted but not completely disrupted because of the multiple routing options. At the same time, the loss of a private peering point would most likely affect only Internet traffic flow for customers of those Internet Service Provider (ISPs) exchanging traffic at

that peering point and only for customers' facilities located within the immediate area of the peering point. The VTF did not present any new recommendations for that issue, but reiterated the recommendations presented in the *Telecom Hotels* report.

...loss of service of specific telecommunications nodes could adversely affect certain Government entities and their corresponding missions.

In its *Trusted Access* report, the VTF stated that the nationwide web of telecommunications assets was far too extensive to ensure full access control to prevent tampering. The VTF concluded that primary factors influencing the efficacy of access control procedures included individuals with malicious intent, the omnipresent insider threat, the lack of standard personal identification and background check capabilities, and a lack of universally applied access control procedures and best practices. To help mitigate potential threats, the task force recommended that the Government, at the Federal, State, and local levels, in cooperation with industry, develop guidance for the creation of national standards for national security background checks and identity verification procedures for key personnel.

Additionally, the VTF noted that voluntary best practices regarding the physical security of, and access to, critical telecommunications assets had not been universally promulgated and employed. Therefore, the VTF encouraged industry's voluntary implementation of NRIC best practices for access control, which could provide a framework for companies to reduce access vulnerabilities. The task force concluded that during emergencies, while the controlling authority should be responsible for allowing access, industry should be responsible for ensuring the identity of its employees who needed access to a particular site during disaster response activities. Therefore, the task force recommended that employees' identification be enhanced through the use of "tamper-proof" certificate-based picture identifications.

The VTF also focused its efforts on understanding the security of hardware and software materials as they transited from the vendor to the service providers. The VTF emphasized in its *Chain of Control Issues* report that overall risks to the security of hardware and software while in transit remained low because public network service providers and their vendors maintained an extensive, controlled delivery system. The complexity of the custom-designed equipment and the unique operating conditions, absence of support software programs and databases in the shipped gear, and limited time to act, made the successful modification of the system exceedingly difficult. Furthermore, upon receipt, the service provider was responsible for verifying the integrity of, and closely controlling the equipment and maintaining the inventory of, spare parts and components. The report also noted that the major risk the public network service providers and their vendors faced was physical damage to, and/or loss of, the equipment as each shipment was worth a great deal of money and represented a significant time investment. Since the economic worth of the materials drove the use of protective measures (such as bonded or vendor-owned trucking, air ride suspension trailers, and complex way bills), the task force agreed that no policy actions were deemed necessary at this time.

NSTAC'S Research And Development Exchange Task Force

On March 13–14, 2003, the President's NSTAC conducted its fifth Research & Development (R&D) Exchange titled, *R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness*.

The event, co-sponsored by the White House Office of Science and Technology Policy (OSTP) and the Georgia Tech Information Security Center at the Georgia Institute of Technology (Georgia Tech), was held at Georgia Tech in Atlanta, Georgia. The purpose of the R&D Exchange was to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding the trustworthiness of NS/EP telecommunications systems and the supporting network information systems.

Dr. John H. Marburger, Director of the White House OSTP, presented the keynote address during the opening plenary of the Exchange. Dr. Marburger noted the importance of increasing the trustworthiness of telecommunications and information systems that supported NS/EP activities and providing guidance to the Government on steps that should be taken. He further emphasized his reliance on the NSTAC's R&D Exchange to offer guidance on the need for specific funding or programs to enhance the trustworthiness of the Nation's NS/EP telecommunications.

During the 2-day event, participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, seven findings or themes regarding the trustworthiness of NS/EP telecommunications and information systems emerged. They are—

- A strong sense of frustration that many R&D information sharing events, such as the NSTAC R&D Exchange, produce similar results and recommendations, but action and implementation are short-lived
- A need to clarify the definition of NS/EP telecommunications in the post-September 11, 2001, world
- A need to address major challenges on driving technology innovation into NS/EP systems and functions
- A need to utilize partnerships in R&D integration efforts
- A need to influence business drivers for security
- A need to improve threat definition and analysis and, equally important, identify methods to share and analyze that information to influence R&D
- A need to strike a better balance between better engineering of software and hardware with efforts to improve human factors.

In August 2003, the RDXTF was renamed the Research and Development Task Force (RDTF) and was established as a standing NSTAC committee.

NSTAC'S Wireless Task Force

At the President's NSTAC XXV meeting, participants discussed the topic of security vulnerabilities in wireless communications

devices and networks. The IES, after an initial scoping of wireless security and other related wireless issues, formed the Wireless Task Force (WTF) to determine how the NS/EP user could operate in a secure environment and to provide conclusions and recommendations to the President regarding wireless security.

The WTF concluded in its report, *Wireless Security*, that there was a range of wireless security in use in the current telecommunications network, with security levels varying from effective, practical security on commercial wireless networks to significantly less security on the public wireless networks. As such, the WTF reported that an NS/EP agency must ensure that its NS/EP communications were secured appropriately for its mission. The WTF also agreed that the extent to which those vulnerabilities had been or could be addressed would be a function of the degree to which organizations with experience in security issues managed the network. Finally, the WTF recommended that the President establish policies regarding limits on the public availability and dissemination of Federal critical infrastructure information (such as the Federal Aviation Administration databases listing tower locations).

The IES also tasked the WTF to (1) study issues relating to the ubiquitous rollout of WPS, (2) determine how WPS could be promoted publicly, and (3) explore non-device specific and secure solutions for deploying WPS. As part of its study, the WTF closely monitored WPS deployment and task force members noted that the ubiquitous deployment of the program had not been achieved for a variety of operational, technical, financial, and regulatory reasons. The WTF also cited inadequate Government funding, a lack of liability protection for carriers, and technological limitations as additional impediments to ubiquitous rollout of WPS. However, they agreed that ubiquitous, nationwide deployment of WPS would be achieved if the Government included all wireless technologies in the solution set, used satellite back-up capabilities, and encouraged the participation of large and small wireless carriers.

In its report to the President, *Wireless Priority Service*, the NSTAC recommended that the President encourage the development and deployment of WPS solutions for all wireless technologies to maximize WPS coverage, increase ubiquity, and give NS/EP users the flexibility to handle a variety of emergencies and disasters. The NSTAC also recommended that the President reaffirm the Federal Communications Commission (FCC)'s Second Report and Order (R&O) on Priority Access Service (PAS) to extend liability protection to wireless priority solution providers that would be equivalent to the liability protection found in wireline priority communications programs. In addition, the NSTAC recommended that the President encourage and support adequate funding for the development and deployment of a multitechnology and multi-carrier WPS program, including a satellite backup capability. Finally, the NSTAC recommended that the President direct appropriate departments and agencies to conduct outreach and educational campaigns regarding WPS and its role in homeland security, specifically targeting State and local governments, small carriers, private sector critical infrastructure providers, and the general public.

NSTAC'S LEGISLATIVE AND REGULATORY TASK FORCE

During the NSTAC XXVI cycle, the Legislative and Regulatory Task Force (LRTF) examined existing legal penalties for those committing Internet attacks to determine whether the penalties should be strengthened or whether additional penalties were needed. The LRTF drafted a report, *Penalties for Internet Attacks and Cyber Crime*, in which the NSTAC concluded sufficient legal authority exists to penalize and deter those who commit cyber crimes. The NSTAC also made recommendations based on the report for pursuing a well-rounded and proactive approach to combating cyber crime. The NSTAC recommended that the President increase prosecution of cyber crime at the State level and allot additional funds to the States to better train personnel to combat cyber crime. The NSTAC also encouraged Congress to ratify the Council of Europe's *Convention on Cyber Crime* and implement legislation to reimburse communications service providers of costs incurred from responding to data preservation requests. The NSTAC also recommended that the President encourage other nations to adopt policies and procedures to better mitigate and respond to cyber crimes and companies to implement cyber security best practices.

The LRTF also continued to examine information sharing in the NSTAC XXVI cycle, during which the Government passed a law, the *Critical Infrastructure Information Act of 2002* (CIIA), which provided additional Freedom of Information Act (FOIA) and liability protections for companies that voluntarily share critical infrastructure information with the DHS. After the CIIA was enacted, the LRTF examined other legal and non-legal barriers to information sharing for the purposes of homeland security.

The NSTAC sent a letter to the NSTAC Principals' General Counsels encouraging them to provide their interpretations of the CIIA's FOIA and liability provisions. It also examined barriers to information sharing that may remain after the passage of the CIIA. The LRTF will continue to examine information sharing issues in the NSTAC XXVII cycle by drafting a report that will examine the information sharing environment since passage of the CIIA.

During the NSTAC XXVI cycle, the WTF tasked the LRTF to assess the legal and regulatory aspects of the FCC R&O on PAS. The LRTF reviewed the R&O and after careful consideration to the merits of reopening the PAS rulemaking, the LRTF concluded revisiting the rules would be a lengthy process and could consequently slow the WPS deployment. As a result, the NSTAC sent a letter to the President offering recommendations on PAS. In the letter, the NSTAC commended the FCC for adopting a Second R&O for PAS that indicated carriers providing PAS shall have liability immunity from Section 202 of the Communications Act, stated that the FCC and the National Telecommunications and Information Administration (NTIA) should accelerate ongoing efforts to improve interoperability between Federal, State, and local public safety communications agencies, and encouraged the Administration to support full and adequate Federal funding for PAS.

NSTAC'S FINANCIAL SERVICES TASK FORCE

Mr. Steve Malphrus, Federal Reserve Board (FRB), and Ms. Catherine Allen, BITS, briefed the IES in November 2002, and the FRB recommended that the NSTAC analyze the financial services sectors' concerns regarding network resiliency, redundancy, and diversity in support of critical financial services sector

processes. Subsequently, the IES created the Financial Services Task Force (FSTF) to examine, from an NS/EP perspective, vulnerabilities related to infrastructure interdependencies between the telecommunications and financial services industries and analyze issues regarding network redundancy and diversity (focusing on resilience instead of reliability) that could impact the financial services sector and, consequently, the U.S. economy. The task force is currently exploring these issues and will publish its results in the fall 2003.

NSTAC'S OUTREACH TASK FORCE

The IES formed the NSTAC Outreach Task Force (NOTF) due to the increasing importance of NS/EP issues and the creation of DHS. The NSTAC recognized its work was poised to provide policy recommendations that could help ensure NS/EP communications and enhance efforts to protect the Nation. The NOTF began FY 2002 as the Outreach Ad Hoc Group, but on February 20, 2003, the IES voted to form a task force to focus additional time, energy, and resources on NSTAC outreach initiatives. The NOTF was tasked to raise the awareness of NSTAC across the Federal Government, industry, and academic and research communities, solicit feedback and input on NSTAC products and outreach initiatives from critical stakeholders, such as representatives in the above-noted organizations, and promote the adoption of NSTAC recommendations to representatives in the above-noted organizations.

During the NSTAC XXVI cycle, the NOTF formulated an NSTAC outreach plan that focused on raising awareness of NSTAC among its stakeholders. During the NSTAC XXVII cycle, the NOTF will begin presenting NSTAC informational briefings to external stakeholders and create an NSTAC outreach packet, including an NSTAC orientation briefing and other useful background information for those unfamiliar with the NSTAC.

"NATIONAL STRATEGY TO SECURE CYBERSPACE" RESPONSE AD HOC GROUP

The White House Office of Cyberspace Security (OCS) drafted the "National Strategy to Secure Cyberspace" (National Strategy) in response to the growing threats to the cyberspace infrastructure. The National Strategy was made available to the public for comment for a 2-month period, between September 18, 2002, and November 18, 2002. The OCS specifically requested the NSTAC comment on the National Strategy and presented the NSTAC with a series of questions to address. Given this initial direction, the NSTAC formed the "National Strategy to Secure Cyberspace" Response Ad Hoc Group to provide comments on the draft National Strategy.

As part of its analysis, the ad hoc group reviewed previous NSTAC recommendations, recognizing that the NSTAC's cumulative work could provide valuable information related to cybersecurity policy. In partnership with the OMNCS, the NSTAC developed a matrix to compare previous NSTAC recommendations with those in the draft National Strategy. Previous NSTAC cybersecurity recommendations were provided to OCS as well as several additional comments on the strategy. On November 18, 2002, the NSTAC's "National Strategy to Secure Cyberspace" Response Ad Hoc Group submitted its final comments to the OCS. Several of these comments were incorporated into the final *National Strategy to Secure Cyberspace*, released in February 2003.

NSTAC XXVII Activities

As NSTAC task forces proceed with their work in FY 2004, the Presidential committee will continue to provide industry expertise on a range of subjects. Building on its prior work, NSTAC will address information sharing, national policies and/or regulatory issues affecting telecommunications, critical facilities vulnerabilities, trusted access to communications facilities, and the commercial satellite industry and security. The FSTF will continue to address the charge given to it by the IES in NSTAC XXVI through close coordination between the telecommunications and financial services sector as well as collaborating on Presidential recommendations. The NSTAC will also co-sponsor its sixth R&D Exchange in 2004.

Public Affairs

The NCS received numerous inquiries from the news media concerning emergency telecommunications. These inquiries have come from national media outlets such as the major television networks, national wire services, leading national newspapers, government focused telecommunications magazines, and specialized telecommunications periodicals. Inquiries have focused on the NCS transition into DHS, and its role within the Department's IAIP Directorate. Inquiries have also focused on the Telecom Information Sharing and Analysis Center (ISAC), WPS, GETS, Telecommunication Service Priority (TSP) Program, and the NCS mission to work with industry in support of emergency communications.

In addition to fielding press inquiries, the NCS has also distributed a variety of publications, reports, fact sheets, and brochures on NCS programs and the President's NSTAC. The publications are provided to the media, telecommunications companies, potential NSTAC membership applicants, and senior Government officials to provide background information on NCS programs and activities.

The NCS published its FY 2002 Report in late August 2003. The NSTAC Reports for the NSTAC XXVI cycle were published in early March 2003 and distributed soon after the NSTAC XXVI meeting held April 30, 2003. The NSTAC XXVI Issue Review is scheduled for publication in early FY 2004, as are two documents recognizing the 40th Anniversary of the NCS.

Outreach

The Deputy Manager, NCS, continued to spearhead an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences and supported OMNCS Division leaders and program managers in doing the same.
NCS representatives attend Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and critical infrastructure protection. Since the transfer of NCS assets to DHS, there have been numerous opportunities for NCS leaders to participate in panel discussions and other public events to promote and describe the NCS, DHS and its critical role in homeland security and NS/EP communications.

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. In spring 2003, the *NS/EP Telecom News* printed its first, full-color newsletter, followed by a 32-page special edition marking the 20th anniversary of NSTAC. The summer edition will be released before the end of the FY 2003, and two additional editions are planned for release in early FY 2004.

NCS Home Page

The NCS home page (http://www.ncs.gov) provides information on the NCS and NSTAC. The home page contains NCS and NSTAC history, information about NCS and NSTAC programs and activities, and online versions of NCS and NSTAC publications.

IV

NS/EP Telecommunications Support and Activities of Member Organizations

DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

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

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

TELECOMMUNICATIONS STAFF ORGANIZATION

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

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Information Technology Facilities Consolidation

DOS continues to progress on consolidating and standardizing its enterprise server operations. This project was started in mid-fiscal year (FY) 2001 and focuses on developing and implementing a plan for a comprehensive "server farm" concept which will establish the infrastructure for consolidating information technology (IT) facilities and processing resources, such as servers, databases, and applications into centrally managed facilities and systems. The benefits are savings in manpower and facilities throughout the Department, improved security, data integrity, operational reliability, technical support, and availability.

Interagency Collaboration

As previously reported, the Department conducted a pilot program known as Foreign Affairs Systems Integration (FASI) to enhance communication and collaboration among foreign affairs agencies overseas. At the conclusion of the FASI pilot program in January 2003, the Department refocused program objectives to enhance inter-agency communications and collaboration through the acceleration of a modern messaging system and expanded use of the Open Source Information System (OSIS) and Secure Internet Protocol Router Network (SIPRNET). The pilot program also demonstrated the value of e-mail connectivity between all embassy elements via a direct connection at post rather than through Washington, DC, headquarters agencies. The Department is now moving forward to provide direct e-mail connectivity among agencies represented at embassies.

The Department is also moving ahead to improve communications and collaboration among agencies via the OSIS. The OSIS is a Virtual Private Network (VPN) for securely transmitting unclassified information between agencies. The Department is increasing the amount of information it makes accessible through its site on the OSIS network, including consular data, administrative data, and information on State Department regulations and administration of embassy activities. DOS is also encouraging other foreign affairs agencies to use OSIS for communication and collaboration and welcome that the U.S. Agency for International Development recently joined OSIS.

Secure Voice Program

The Department is actively transitioning its legacy secure voice system to the new National Secure Voice Standard, the Secure Terminal Equipment (STE) system. Funding was designated for this project and STE systems are being received from the National Security Agency (NSA). The replacement process of the legacy secure voice system with this new technology is proceeding smoothly. STE units are being deployed both domestically and at posts overseas. Current projections show a complete legacy secure voice replacement will be accomplished by the end of calendar year (CY) 2003.

Communication Security

All (181) eligible posts have been converted to over-the-air-rekeying (OTAR), the focus will now be placed on domestic customers. The implementation of OTAR has enabled the Department to significantly reduce the physical cryptographic keying material at OTAR posts. Communications Security (ComSec) is dramatically enhanced by this reduction in cryptographic holdings.

DEPARTMENT OF STATE (DOS) *continued*

The Department created a Public Key Infrastructure (PKI) Program Office to implement PKI, providing users secure Internet and Intranet web application and e-mail services previously unavailable. The Department started to implement PKI during Fiscal Year (FY) 2001. In addition to providing public key technology to State users domestically and overseas, the Department is providing this "smartcard"-based access technology to users from the Department of Justice's (DOJ) Immigration and Naturalization Service (INS) to access visa information resources and to all Federal agencies with requirements to access the Interagency Collaboration Zone (ICZ) at overseas posts. This technology will have a profound impact on the overall level of information security for the State Department and the conduct of its business in the future.

Messaging Systems

On April 4, 2002, the Under Secretary for Management approved a recommendation to accelerate the implementation of a modern messaging system for the State Department. This project, originally scheduled for FY 2006, has been accelerated, with a pilot implementation planned for FY 2004 and full deployment to follow in FY 2005. This new system will replace the outmoded cable system and will integrate all of the current processes for messaging including cables, memoranda and e-mail, resulting in the preservation of the complete record of foreign affairs data information.

Enterprise Network Management

The Enterprise Network Management (ENM) Program is modernizing the Department's data communications capabilities, thereby enhancing the diplomatic readiness of the Department. ENM is currently augmenting the availability of this connectivity by using commercially available options including VPN technology to create network "tunnels" through the global Internet infrastructure. These tunnels provide an added route capability that is independent of the existing telecommunications infrastructure, thus increasing overall network availability. ENM has implemented about 115 alternate routes using this technology, with plans to implement at all posts by FY 2005. The current average VPN network availability is above 98%, with a goal of 99.7% by FY 2007.

Classified Connectivity Program

The Classified Connectivity Program (CCP), created in 1999 to modernize the Department's classified infrastructure, provides authorized employees posted overseas with desktop access to classified e-mail and telegram services, as well as to SIPRNET, a Web-based tool that allows users access to certain Intelligence Community Web pages. This capability will facilitate closer collaboration among agencies working together to serve and protect the U.S., its citizens, and its interests worldwide. In addition, CCP will replace obsolete IT and communications hardware and software currently in use by some posts to process classified foreign affairs information. CCP also provides for a consistent architecture across classified and unclassified systems, resulting in greater efficiencies with reduced cost through standardization and an improved administrative toolset, allowing Web-enabled configuration management. The system also aligns with e-government initiatives and the President's management agenda. The project is ahead of schedule and will end in September 2003, completing three months ahead of schedule. At this time, 226 eligible overseas posts will have a modernized classified infrastructure fully capable of supporting foreign affairs functions.

OpenNet Plus

IRM, with the strong support and assistance of our colleagues, is proud to announce that as of May 29, 2003, DOS has Internet access on desktops throughout the world. Secretary of State Colin Powell was quick to push for resources for DOS IT needs when he assumed his office. He has since delivered to the Department and now DOS has reciprocated. Because of OpenNet Plus, 43,570 users in 321 posts and bureaus now have Internet access.

DEPARTMENT OF THE TREASURY (TREAS)

The U.S. Department of the Treasury (TREAS) is the financial manager for the U.S. Government and a World leader in formulating and shaping economic policies and financial practices for the U.S. as a member of the World stage. The essential functions of the Treasury Department requiring NS/EP and Telecommunications Service Priority (TSP) program service are summarized as follows:

- Promote prosperous U.S. and World economics
- Promote a stable U.S. and World economy
- Manage the U.S. Government's finances effectively
- Maintain, manage and preserve the economic and financial management institutions of the United States, including all monetary, credit, and financial systems
- Serve as one of the principal economic advisors to the President
- Perform international economic and monetary control as it pertains to the well-being of the Nation
- Manufacture currency, coins, and stamps
- Establish, monitor and track methods of currency exchange and financial transactions.

TELECOMMUNICATIONS STAFF ORGANIZATION

Department of the Treasury manages its telecommunications services through the Office of Chief Information Officer (CIO), a component of the Office of the Assistant Secretary for Management and Chief Financial Officer. The Treasury CIO provides oversight and management of NS/EP support activities and National Communications System (NCS) liaison. The CIO is responsible for ensuring, through the exercise of program management authority, that Treasury bureaus have access to a cost-effective, technologically sound, telecommunications infrastructure for executing and carrying out their respective financial support missions.

In addition, the Treasury CIO is also a member of the Federal CIO Council for ensuring the deployment of an enduring telecommunications capability and associated e-government applications services for maximizing cross-functional department integration between and among the Federal Departments of the U.S. Government. In this role, the Treasury CIO is responsible for guiding, directing and developing IT management policies, standards, practices and procedures for enabling the financial business functions of the U.S. Government. The Federal CIO Council is the lead interagency forum for improving these practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Treasury Communications System

The Treasury Communications System (TCS), the Treasury Department's nation-wide business communications networking infrastructure, continues to provide critical telecommunications services to Treasury Department Headquarters and its associated bureaus. The TCS is one of the largest secure and encrypted networks within the Federal Government today. It routinely distributes and handles over 900 gigabytes of data each day and is the model being used by the Department of Homeland Security (DHS) in establishing their initial secure networking infrastructure. The cyber security protection mechanisms were significantly enhanced in FY 2003 by expanding its internal network detection devices from 10 to 18 and adding a security and threat management capability for evaluating potential cyber activity from a "security in depth" perspective. This resulted in a ten fold strengthening of the cyber security countermeasures of these telecommunications services.

Furthermore, the TCS Continuity of Operations (COOP) continues to evolve toward completing its connectivity to the Treasury Bureau alternate operating facilities. The TCS facility backup center (FBC) was completed and tested in late October 2002 at the Treasury Alternate Operating Facility (AOF). The final phase will be achieved after connectivity to the Bureaus' AOF is completed. This phase is forecasted for completion by December 2003. In addition, the Treasury Headquarters'

DEPARTMENT OF THE TREASURY (TREAS) *continued*

Departmental Offices continue to backup vital Treasury electronic mail along with appropriate IT application infrastructure platforms for access to Treasury Headquarters' vital records, files, and information to include critical Treasury mission applications for managing critical Treasury missions during national emergencies, disasters, and contingencies from this Treasury AOF facility.

Additionally, Treasury Headquarters and associated Bureaus have designated which circuits and locations are to be supported through the NCS TSP Program. The TSP Program provides for enhanced service restoration by the telecommunications service providers based upon circuits designated as either Command and Control (TSP Level 1) or Critical Operations (TSP Level 2). Telecommunications service providers are required to restore service in priority order according to the TSP level indicator and before any non-TSP circuits are restored in case of a national emergency or disaster. This capability was utilized when Bureau locations were affected by the September 11 terrorist attacks in New York City. Therefore, by the end of FY 2003, TREAS designated 2710 telecommunications circuits as either TSP Level 1 or Level 2, a 130 fold increase over the previous reporting period.

Treasury Emergency Management Center Capability

In October 2002 through January 2003, the Treasury COOP was revised around the legislation associated with the establishment of DHS. As an aftermath of this plan, Treasury Headquarters established interim Emergency Management Centers for responding and reacting to crises, disasters and emergencies. These centers are currently integrated with the Treasury telecommunications enterprise network operations facilities for ensuring continuous operations of TREAS in a crisis or emergency. Currently, these centers are being improved and modernized around changes in TREAS' operating principles and practices and the associated IT systems for enhancing their business management information systems.

Treasury Computer Security Incident Response Capability

In October 2002, TREAS partnered with a managed security services provider to enhance the TREAS' Computer Security Incident Response Center (TCSIRC) capabilities. As a result, TREAS has currently been approved through Defense Security Services the authority to store and process information and data up to the Secret Collateral level. Treasury CSIRC also hosts a Critical infrastructure Warning Information Network (CWIN) terminal in their Network Security Operations Center (NSOC) for providing the TCSIRC with advanced threat information.

In FY 2003, Treasury leveraged its TCSIRC's visibility across numerous government and commercial networks, their capital investment in facilities, technology and processes, and their relationships with FedCIRC and other law enforcement agencies to provide comprehensive incident response and vulnerability management capabilities to the Treasury Department and associated mission bureaus. By centralizing the information at the TCSIRC service provider and utilizing their secure web portal, TREAS and its associated mission bureaus can now effectively share information regarding network and system vulnerabilities, resulting in an increased awareness of emerging threats and a corresponding decrease in costs and resources.

During recent outbreaks of worms and viruses across the Internet, the TCSIRC played a crucial role and provided incident response assistance and mitigation strategies to the Department and each of the subordinate bureaus. The advanced notifications and mitigation strategies deployed during this period by the TCSIRC greatly reduced the potential impact to the entire Treasury Department and resulted in minimal loss of computing capabilities in FY 2003.

Certification and Accreditation

In the last three years, the TCS Security Assurance Program has made great strides in keeping its systems, and those of other bureaus, compliant with Federal and Treasury certification and accreditation (C&A) policies and procedures. By maintaining an assurance that its infrastructure and networks will be secure and protected, TCS continues to provide and enhance its protective environment with a security posture conducive to processing sensitive-but-unclassified information.

In FY 2003, the TCS Security Assurance Program certified and accredited not only its own environment and associated IT infrastructure systems, but those of other bureaus and agencies; such as the Office of Thrift Supervision (OTS), Treasury Inspector General for Tax Administration (TIGTA), and the Office of DC Pension that is responsible for processing pension annuity payments for the District of Columbia's retired workers.

DEPARTMENT OF THE TREASURY (TREAS) *continued*

The TCS continued to maintain its C&A in FY 2003 by ensuring that new services added to the General Support System go through the same process as the original C&A. Some of the additions to the TCS Systems that have been processed in FY 2003 include the internal PKI, the external PKI certificate authority (ECA), and the Foreign Credit Reporting System (FCRS). Currently, TCS Network Security is in the process of certifying and accrediting the newly created Treasury external network (Extranet). The TCS Network Security is also in the process of re-certifying and accrediting the entire TCS as part of the proscribed three-year recertification process and practice.

The Department is working with the Bureaus on numerous endeavors to improve the state of security on mission critical systems and major business applications. In addition, specialized IT security training and emphasis on security is being addressed in the Department's capital investment planning process. The Treasury Department continues to make progress in improving security of its IT systems supporting the Department's financial and terrorist asset tracking missions.

Support for the Federal PKI Development

The Treasury Department continues to provide technical, operational, and leadership support in the development and use of an interoperable government-wide PKI to permit electronic transactions over the Internet in a trusted environment. In late FY 2002, TREAS deployed an enterprise PKI system for use by all Treasury Bureaus. The system is capable of issuing PKI certificates to Treasury's 150,000 users. The Department is one of four Federal agencies (Treasury, Defense, Agriculture, and NASA) that have been cross-certified with the Federal PKI Bridge. This effort will allow Treasury to strengthen its secure communications processes in conjunction and alignment with its development of a common infrastructure landscape.

To date, ten Treasury Bureaus have completed implementation and three are planning their implementation within the next year.

Critical Infrastructure Protection

In October 2002, the Treasury Department identified Security, Privacy and Critical Infrastructure Protection (CIP) as a key initiative. Treasury has established a CIP Working Group consisting of representatives from all its Bureaus. A Project Matrix review to identify Treasury critical assets has been completed and a Treasury-wide CIP policy and a CIP Plan with an associated Treasury CIP Implementation Plan are being developed. Treasury is in the process of prioritizing our cyber critical assets and conducting interdependency analyses on those identified as supporting national critical functions and services.

Public Safety/Law Enforcement Wireless Activities

During 2002, TREAS led significant activities in addressing interoperable wireless communications for public safety and law enforcement officials. However, the Treasury program office was transferred to DHS in March 2003. During 2003, and in light of the organization's transfer to DHS, Treasury continues to partner with DOJ, as well as DHS, to implement a joint law enforcement land mobile radio system that will meet the requirements of involved Federal Departments. This initiative will provide cost and operational efficiencies across TREAS and also will enhance interoperable communications among the various law enforcement agencies. This initiative will also assist Federal Departments in addressing a long standing issue relative to frequency spectrum management by providing a "one-stop-shop" function within a single Federal Department.

Wireless technologies continue to expand in number and complexity. As such, these rapidly evolving technologies and wireless standards have created a unique challenge to the Treasury Department, as well as the U.S. Government, to keep pace with new wireless platforms and devices. Therefore, Treasury continues to coordinate its wireless requirements with DOJ and DHS in a joint radio system venture for the future.

Summary

The COOP requirements for the TCS have been fully coordinated and synchronized with the plans and programs operating under the Treasury Department's Office of Emergency Preparedness (OEP). Notwithstanding the devolution of the Treasury law enforcement organizations to DHS, the issuance of Government Emergency Telecommunications Services (GETS) cards more than doubled in FY 2002 and continued to increase in FY 2003. In February and March 2003, Treasury established a Treasury Emergency Management/Operations

DEPARTMENT OF THE TREASURY (TREAS) *continued*

Center within the greater Washington DC/metropolitan area for further strengthening of Treasury emergency preparedness posture. Key operational functions and capabilities enabled in FY 2003 are:

- Additional Department of the Treasury Emergency Management Centers (EMC) with associated system monitoring and management tools
- Office space for senior Treasury Department leadership and their core emergency staff
- Communications connectivity to other Bureau Alternate Operating Facilities (via the TCS W2 Site) and associated emergency preparedness staffs
- Local Treasury Headquarters connectivity to Treasury enterprise services, such as e-mail, business applications and other information services.

These enhancements and modernization initiatives in FY 2003 will allow TREAS to respond, operate, and function in a crisis, emergency or national disaster once completed.

DEPARTMENT OF DEFENSE (DOD)

NS/EP TELECOMMUNICATIONS MISSION

Under the provisions of Executive Order (E.O.) 12472, the Department of Defense (DOD) maintains 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 by E.O. 12333, "U.S. Intelligence Activities," December 4, 1981
- Ensure that the Director, 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(1) of E.O. 12472.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOD includes the Office of the Secretary of Defense (OSD), the military departments and services within them, the combatant commands, and other agencies established to meet spetcific U.S. military requirements. The Defense Information Systems Agency is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense for Networks and Information Integration [ASD (NII)].

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense, and the ASD (NII). Command, control, and communications requirements are the concern of the Joint Staff Director for Command, Control, Communications and Computer (C4) Systems (J6).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Critical Infrastructure Protection

The Deputy Secretary of Defense signed a Memorandum September 8, 2003 realigning CIP Oversight to the Assistant Secretary of Defense for Homeland Defense (ASD [HD]). The ASD (HD) will focus on the planning and execution of DOD activities and the use of resources in preventing and responding to threats to infrastructures and assets critical to DOD missions. The ASD (HD) will also represent the DOD on all CIP related matters with designated Lead Federal Agencies, the Executive Office of the President, DHS, other Executive Departments and Federal Agencies, and State and local entities.

Horizontal Fusion

In August 2003, the ASD (NII) announced the successful completion of Quantum Leap I. The exercise demonstrated a concept of net-centric operations called "horizontal fusion" —the ability to integrate data from several sources for rapid and effective decision making. The Horizontal Fusion Portfolio Initiative is a direct response to integrate and optimize technology and operations to achieve "Power to the Edge" in the new battlespace. It uses a joint suite of military communication and intelligence capabilities in development by the armed services with multiple Web-enabled portlets, on-line foreign language translation, and leading edge computing services to provide a dynamic look at tactical operations for real-time collaboration, situational awareness and sense-making.

Horizontal Fusion Net-Centricity is made possible by the new technology context that includes:

- The Bandwidth Expansion program, or GIG BE, which provides a secure, robust, optical Internet protocol (IP) terrestrial network
- Joint Tactical Radio System, which offers a family of software reprogrammable radios based on an open-communication architecture that will provide interoperable tactical wideband IP communications capabilities
- Wide-band satellite communications, which provides ubiquitous communications with optical quality bandwidth
- Net-Centric Enterprise Services, which supplies the infrastructure and services to support the broad range of applications and data used in a Net-Centric enterprise
- Information Assurance (IA), which is vital to support all efforts to ensure that the Net is robust, reliable, and trusted

DEPARTMENT OF DEFENSE (DOD) *continued*

- Horizontal Fusion, which provides Net-Centric applications and content needed to assure analysts and warfighters with the ability to make sense of complex and ambiguous situations across the battlespace.

Implications of these capabilities provide leaps in potential for battlefield operations, access to real-time critical knowledge and situational awareness, informed command decision-making, and operational and tactical response.

This year's Horizontal Fusion Portfolio is made up of 13 initiatives designed to provide improved intelligence and operations support for joint task forces and tactical units engaged in hostile action. Moving beyond former concepts of "plug and play" wiring diagrams, "one-to-one" interfaces, or "push" technology, Horizontal Fusion is built on a foundation of transforming the ways in which knowledge is available to the battlespace.

DEPARTMENT OF JUSTICE (DOJ)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission for 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 (TS) operates and manages DOJs' consolidated data transport network, law enforcement message processing systems and Telecommunications Services Center. TS also provides networking and technical assistance to DOJs'offices, boards, divisions, and bureaus. Secure interagency message transmission is offered through separate facilities (Automatic Digital Information Network, and Justice Automated Message System).

The Information Security Policy Group (ISPG), Security and Emergency Planning Staff is responsible for security oversight of all national security communications systems within the Department. The ISPG is the central office of record for all national security information key material for the department. The Drug Enforcement Administration, FBI, and U.S. Marshals Service continue to administer their own communications security programs. The Bureau of Alcohol, Tobacco, Firearms, and Explosives has moved to DOJ and INS has moved to DHS.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

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

- Telecommunications Services (TSS) provides representation for DOJ on the NCS Committee of Principals (COP) and Council of Representatives (COR)
- A TSS representative serves on the TSP Oversight Committee
- DOJ continues its active participation in the NCS activities of the COP and participated in NCS NS/EP telecommunications support, activities, and programs
- DOJ continues its vigorous support of the activities of NCS NS/EP planning, program, and contingency programs, and emerging NS/EP telecommunications programs. DOJ has sponsored full access to TSP services for five commercial companies which are either departmental component contractors or engaged in national security and emergency preparedness support in their normal duties (remote security alarm sensing; 911 and enhanced 911 services in several Midwestern states; and for environmental and emergency response services for cleanup of waste at clandestine drug laboratories)
- Additionally, DOJ is an active participant in the GETS Program, the Wireless Priority Service (WPS), the TSP Program, and the Shared Resources (SHARES) High Frequency (HF) Radio Program.

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 Interior (DOI) and the U.S. Department of Agriculture (USDA) co-manage the National Interagency Fire Center in Boise, Idaho. It is the Nation's primary emergency support facility for forest fire suppression. They provide emergency transportable land mobile radio (LMR) systems from multiple radio caches strategically located throughout the U.S. to support wildland fire fighting and other national emergency activities. Forest fire suppression operations are conducted in close cooperation with state and local government emergency support activities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOI mission critical long distance voice and data communications is primarily provided by WorldCom via the General Services Administration (GSA) Federal Telecommunications System 2001 (FTS2001) contract. Due to WorldCom's Chapter 11 bankruptcy, the DOI has reviewed it's contingency plans and service alternatives, and is closely monitoring WorldCom service status, particularly relative to GSA's proposed debarment. DOI is planning the consolidation of the Departments' bureau backbone data communications networks to a single Department wide IP based architecture with enhanced network security functionality. DOI is also consolidating Internet service provider access throughout the Department.

Conversion of DOI's wideband LMR systems to narrowband digital operation is a high priority activity. We continue to investigate sharing opportunities with the USDA and other cooperators to improve interoperability and reduce costs. We have a multi-vendor multi-year contract to supply digital narrowband radios and systems in response to the National Telecommunications and Information Administration (NTIA) mandated transition to narrowband LMR operations. This contract, available to all Federal agencies, provides lower-cost standardized interoperable digital radios. We are a participating partner in the e-Gov Wireless Public Safety Interoperable Communications Program (SAFECOM) program which will improve interoperability of public safety radio systems.

Key officials, emergency coordinators, and telecommunications managers throughout the Department have GETS Cards for long distance emergency telephone communications and WPS. Cellular phones have been provided to key officials in Washington, DC. Secure telephone units-third generation are used to support DOI national security programs and HF backup radio links are used to augment DOI emergency relocation site communications.

DOI SIGNIFICANT ACCOMPLISHMENTS

- Additional DOI Digital Narrowband Contracts were awarded.
- Pilot implementations of Microsoft Active Directory were completed.
- A secure TrustNet network was implemented to protect individual Indian trust data. Planning has been completed for implementation of the Department's consolidated Enterprise Services Network.

U.S. DEPARTMENT OF AGRICULTURE (USDA)

NS/EP TELECOMMUNICATIONS MISSION

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

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

USDA has been granted originating classification authority and has awarded a contract to clearly define Department wide requirements for classified communications infrastructure. The Department plans to explore options for sharing existing Federal infrastructure where feasible.

USDA has replaced over 50% of the original Secure Telephone Units, Third Generation (STU III) with STE, and has installed and/or ordered additional STE's to meet the growing requirements of homeland security, COOP relocation sites, and mission areas. In addition, USDA participates in the Cellular Priority Access Service (CPAS) and is in the process of installing a secure video conferencing system to support homeland security requirements. USDA also supports the GETS program and in an ongoing effort, ensures all persons in NS/EP leadership positions have GETS cards.

The COOP Planning Staff within the USDA Office of Procurement and Property Management continues to utilize the information obtained from the intelligence community as a key component in COOP, Continuity of Government, and other national security program planning.

NS/EP PARTNERSHIP ACTIVITIES

The USDA Forest Service participated in the recent update to the National Response Plan (NRP). The Forest Service has responded to emergencies and major disasters under the NRP for many years. These responses have increased in recent years and the level of involvement is expected to remain high. As a follow on to the NRP, the USDA Forest Service also participated in the recent update to the National Incident Management System (NIMS) - Initial system (July 1, 2003). These documents establish an updated national approach to domestic incident management.

USDA entered into a Memorandum of Agreement with DHS to support the SAFECOM E-Government initiative. SAFECOM's mission is to enable public safety personnel nationwide (across local, tribal, State and Federal organizations) to improve public safety response through more effective and efficient interoperable radio communications. Contributions include the six-month assignment of an interim USDA representative to serve as Program Manager during the transition of SAFECOM for the Federal Emergency Management Agency (FEMA) to DHS and funding in the amount of $1.4 million.

USDA and the Federal Communications Commission (FCC) cooperate under an agreement to investigate and resolve domestic and international radio interference. This cooperation enables rapid identification and resolution of harmful cases of radio interference nationwide. The USDA Frequency manager participated in the mixed commission meetings between Mexico and the U.S. to address radio frequency interference (RFI) cases. Specific cases were reviewed and remediation negotiated. RFI along the Mexican border poses a significant risk to general law enforcement, border security, wild land firefighting, and drug interdiction efforts for multiple federal agencies.

USDA and DOI updated a nationwide agreement for the sharing of common radio frequencies for aircraft operations. This agreement reserves seven radio frequencies used in providing emergency communications, air tactical operations, and flight tracking of government aircraft.

Due to expertise in incident command, the Forest Service is providing incident command training to the Fire Department of the City of New York.

DEPARTMENT OF COMMERCE (DOC)

NS/EP TELECOMMUNICATIONS MISSION

The Department of Commerce (DOC) promotes job creation, economic growth, sustainable development, and improved living standards for all Americans by working in partnership with businesses, universities, communities, and workers to:

- Build for the future and promote U.S. competitiveness in the global marketplace by strengthening and safeguarding the nation's economic infrastructure
- Keep the U.S. competitive with cutting-edge science and technology and an unrivaled information base
- Provide effective management and stewardship of the nation's resources and assets to ensure sustainable economic opportunities.

The DOC touches the daily lives of Americans in many ways. The Department makes possible the weather reports heard every morning and facilitates technology that Americans use in the workplace and home every day. DOC also supports the development, gathering, and transmitting of information essential to competitive business and makes possible the diversity of companies and goods found in America's (and the world's) marketplaces. Lastly, DOC supports environmental and economic health for the communities in which Americans live and it conducts the constitutionally mandated decennial census, which is the basis of representative democracy.

These missions are ongoing and sustained during national level NS/EP activities in case of emergencies, including stress periods during peacetime, crisis, and mobilization activities, periods of disaster recovery, as well as during wartime crises such as the events on September 11, 2001, and the aftermath of that event in support of homeland security.

TELECOMMUNICATIONS STAFF ORGANIZATION

The DOC manages its telecommunications through the Office of the CIO.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

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

- The DOC is actively involved in homeland security initiatives and efforts to enhance preparedness in the post September 11 environment with the necessary IT equipment, software, and hardware upgrades. DOC's headquarters in Washington, DC, is implementing a new, state-of-the-art public address system in the Herbert C. Hoover Building common areas. This new system will integrate with the Voice over Internet Protocol (VoIP) telephone system's Emergency Broadcast System. In case of any emergency, the same alert can go to DOC offices and the common areas of the building such as the White House Visitors' Center.
- The DOC has enhanced and successfully exercised its COOP Plans, including telecommunications support, in various emergent scenarios. The exercises included DOC essential personnel and implemented the architecture for alternate site processing of management data, communications, and operations.

The DOC serves as a lead government agency implementing alternative communications technology with an emphasis on the Internet and electronic-commerce and methods for protecting government networks. The DOC continues to increase their use of NCS services and programs, especially in light of the tragic terrorist attacks and post September 11 security programs.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

To respond to the roles and responsibilities assigned to the U.S. Department of Health and Human Services (DHHS) in an emergency coordination and response effort, five basic elements were considered in the development of the "Functional Statement" and the strategies necessary to provide a technically sound and viable plan. Those elements are:

- Develop an integrated system of information and communications technology that will provide the necessary assets essential to the DHHS, for the Office of the Secretary, and the Office of the Assistant Secretary for Public Health Emergency Preparedness (OASPHEP), in the coordinated effort to protect against, respond to, and recover from all acts of bio-terrorism and other public health emergencies that affect the civilian population.

- Integrate a comprehensive architecture of proven technology that can be replicated in multiple form factors to address the operational issues defined in the "Functional Statement."

- Insure that the method and mode of communications technology is compatible with the systems of the Centers for Disease Control (CDC) Emergency Operations Center (EOC) in Atlanta, Georgia, Food and Drug Administration (FDA) EOC in Rockville, Maryland, Office of Emergency Response (OER) EOC in Rockville, Maryland, DHHS COOP facilities, and the field assets of OASPHEP and OER.

- Develop primary, secondary, and tertiary conduits and pathways of communications to achieve the redundancy necessary for "fail safe" operations in the following five areas of technology:

  - *Computer and Data Systems*
  - *Telephone and Voice Communications Systems*
  - *Radio Communications Systems*
  - *Satellite Communications Systems*
  - *Visual Display Systems.*

The Secretary's Command Center (SCC) began operations in the newly constructed permanent facility located adjacent to the office of the Secretary of Health and Human Services on December 2, 2002, and has been in continuous operation since opening. Constructed in 59 days at a cost of $3.7 million (26% under budget), the Command Center has become a model of technology and program for the federal emergency management sector. The success of the SCC has extended beyond the command and control aspects of the Department's assets and has become an example of the progressive thinking and attention to preparedness. The SCC has been responsible both directly and indirectly in conveying the public health messages of DHHS through the public and government population.

To extend the program of the SCC beyond DHHS, several governmental and non-governmental working groups have developed to increase the collaboration between partners engaged in public health related issues. The "E-Managers Working Group" has brought together center managers and IT personnel from ten federal agencies in an effort to create a more efficient exchange and peer evaluation of pertinent incident information. From this collaboration four important operational issues have been addressed and interim systems have been constructed to facilitate better government cooperation. They are:

- Common Incident Management Software system, DHHS will sponsor a Government Event Management Software

- Video teleconference (VTC) Portal and weekly Command Center VTC, the Department of Energy (DOE) will sponsor

- Geographic Information System Data Base, DHHS will collect an inventory of GIS.

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 U.S. 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." Since the tragic events on September 11, 2001, the entire Department has been engaged in the evaluation and implementation of enhancements to the safety and security of the Nation's transportation systems. With the recognition of new threats and vulnerabilities of the transportation systems and the U.S. way of life, the Department is developing new strategies and contingencies to deal with these threats and vulnerabilities. The recognition of the vital role that telecommunications plays in providing for the safety and security that the traveling public has come to expect from the Nation's transportation systems, has enabled the Department to further enhance its ability to respond to and counteract new threats as they arise.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The Department participates in several ongoing NS/EP telecommunications activities to include:

Support of NCS Activities

The Department continues its active participation on the NCS COP/COR, the President's National Security Telecommunications Advisory Committee (NSTAC), and actively supports NCS NS/EP activities and programs. The Department has designated a member of the CIO's staff to be an on-site liaison at the NCS headquarters. This DOT liaison is working to further ensure that the Department is taking maximum advantage of the various NS/EP programs and services offered by the NCS.

GETS

The Department is involved with the NCS GETS program and has been since its inception. GETS cards are assigned to Regional Emergency Transportation Coordinators and Representatives across the U.S. and overseas for use during natural disasters and other emergency situations and exercises. The Department provides GETS usage sponsorship for State and local government transportation system officials, as well as key private sector transportation officials. This year, the Federal Highway Administration substantially increased its involvement in the GETS program by issuing cards to all of its 52 field division offices and its mid-level and senior leadership in Headquarters.

Wireless Priority Service

The Department is also participating in the WPS program to further enhance its emergency communications capabilities. Both the T-Mobile cellular and Globalstar satellite handsets were acquired and issued to departmental individuals who perform NS/EP roles and functions. In conjunction with the GETS cards, these two NCS programs help to further ensure that the Department is able to better communicate in the event of an emergency.

Telecommunications Service Priority

The Department is actively sponsoring NCS programs to those transportation sector industries who partner with Federal, State, and local Transportation Departments in response to NS/EP events. All DOT Operating Administrations review their telecommunications network to ensure that TSP is implemented on critical communication links.

Other NS/EP Programs

DOT continues to participate in the Federal Telecommunications Standards Committee (FTSC), the SHARES HF Radio Program, and the Communications Resource Information Sharing (CRIS) Initiative.

DEPARTMENT OF TRANSPORTATION (DOT) *continued*

DOT SIGNIFICANT ACCOMPLISHMENTS

- Participated in the Top Officials 2 (TOPOFF2) exercise co-sponsored by DOJ and DOS.
- Developed some specific scenarios of its own that were enacted during the course of the federal event and the feedback from the participating DOT players was invaluable towards better preparing the Department to respond during emergency situations.

DEPARTMENT OF ENERGY (DOE)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Emergency Communications Network

The DOE Emergency Communications Network (ECN) is a multi-faceted communications network used to exchange classified and unclassified voice, data, and video information during emergency situations. The ECN connects eight field offices, four national laboratories, selected DOE/National Nuclear Security Administration (NNSA) support facilities, the FBI Critical Incident Response Group and Threat Assessment Division, the National Infrastructure Protection Center (NIPC), and an undisclosed FEMA location. The ECN also has a dedicated connection to the Russian Federation's Ministry of Atomic Energy in Moscow.

The ECN's configuration is an asynchronous transfer mode (ATM) network with multiple paths among six primary network hubs. Major features of the ECN include: a wide area network (WAN); local area networks (LAN) at selected sites; access to the Internet and World-Wide Web; videoconferencing between sites; and access to commercial videoconferencing systems. During FY 2003, over 320 unclassified and classified videoconferences were conducted on the ECN to support the Department's mission. Significant ECN enhancements in FY 2003 include installation of ECN equipment at the DOE West site, relocation of the Los Alamos Laboratory ECN system to a new Operations Center, and relocation of the FBI ECN system from Quantico, Virginia, to Stafford, Virginia.

The Department evaluated ECN equipment requirements for new node sites at Brookhaven National Laboratory. The Bonneville Power Administration (BPA) tested a new operating system for classified/unclassified computers to replace outdated SUN workstations at DOE Headquarters (HQ) and all ECN field sites. BPA partnered with the Office of Intelligence to upgrade data and video communication links between DOE HQ, the Remote Sensing Laboratory in Las Vegas, Nevada, and Albuquerque, New Mexico.

The vision of the ECN Program is to provide the DOE/NNSA emergency response community a world-class, state-of-the-art, high-speed, global emergency communications network. The ECN will support the international exchange of classified and unclassified voice, data, and video information. The ECN staff envisions the ECN as a U.S. based emergency communications system platform that is expandable to provide emergency response and emergency management communications capabilities across the globe.

DOE/NCS

The NCS and DOE successfully completed the first test of an initiative designed to study "Backup Dial Tone" capabilities in and around the National Capital Region. The first tests, conducted with the DOE and Terabeam Corporation of Kirkland, Washington, involved deploying Free Space Optics (FSO) as a wireless transmission medium to connect two of their buildings using VoIP technology. FSO is a technology where voice and data signals are sent via an invisible beam of light through the air, rather than through underground fiber optic cables. The light, using the same wavelength of a fiber optic cable light, is beamed directly through office windows or to building rooftops and provides an improved capacity for transferring large amounts of data. This is the first phase in a multi-phase plan to incorporate FSO technology at the Department. Later phases include implementing a video conferencing service over the FSO link and using the FSO link to provide a diverse route between two private branch exchanges (PBX).

Terabeam's FSO metropolitan area network in Seattle, Washington, provides a model for the effort being pursued in the Washington, DC, metropolitan area. The Seattle network contains 11 hub sites which transmit free space optics wireless signals throughout the downtown area.

Metropolitan Area Network Upgrade

During FY 2003, HQ began upgrading the DOE Washington, DC, Metropolitan Area Network (MAN), between the Germantown and Forrestal facilities from OC-3 and DS-3 ATM circuits to an OC-12 Synchronous Optical Network Ring. This upgrade will increase network performance, availability, and enable future services to be delivered over the fault-tolerant ring at reduced costs. The VoIP pilot was also completed and in 2004, HQ will deploy VoIP technologies.

DOE Corporate Network

Improvements and additions were made to the DOE Corporate Network (DOEnet) during FY 2003. Permanent virtual circuits (PVCs) were ordered to provide continued service to DOEnet field locations in the event of a loss of

DEPARTMENT OF ENERGY (DOE) *continued*

connectivity at either of the DOEnet hub locations (currently at DOE HQ, Forrestal and at the Nevada Operations Office in Las Vegas, Nevada). This reduces the possibility of a catastrophic loss of network availability due to the failure of a single site or router. Network changes were made to accommodate the consolidation of the Ohio Field Office circuit into the Fernald circuit in concert with staff relocations.

Idaho National Engineering And Environmental Laboratory/Idaho Operations Office

The Idaho National Engineering and Environmental Laboratory (INEEL) began transitioning from wideband to the federally mandated narrowband-capable trunked LMR system technology. Completion, testing and acceptance of this project are planned by the end of CY 2003. Installation of the two-mountain top repeater infrastructure consoles and the majority of the mobile radios are complete. The strategic placement of antenna equipment within operational areas greatly improved signal strength for optimal signal saturation and system efficiency. The redundancy built into the new system, minimizes the probability of a single event leading to the failure of the entire system. It also provides improved means of emergency, safety, and security communications throughout the INEEL complex.

The INEEL built a comprehensive Next Generation Communications Test Bed as part of a Critical Infrastructure Assurance Test Range. The Communications Test Bed offers large-scale, independent, end-to-end testing of next generation wired and wireless communications infrastructures including third and fourth generation cellular, LMRs, and wireless LAN systems. Also included in the Critical Infrastructure Assurance Test Range are Supervisory Control and Data Acquisition, Cyber Security, Transportation, and Physical Security Test Beds. Efforts are underway to address NS/EP uses of the Test Range in the event of an occurrence.

A Network Scanning Security Identifier was developed to verify security configurations on individual workstations and servers. It is a customized wrapper for a commercial vulnerability scanner (Internet Security Scanner) that uses a web interface to provide the results to individual end-users and is capable of scanning UNIX, Linux, Windows servers, and workstations. This software identifies vulnerabilities in systems (internal and external/Demilitarized Zone) so they can be mitigated. This capability will provide a stronger cyber security posture within the INEEL.

Nevada Operations Office

The Nevada Operations Office (NV), in cooperation with the Nevada Test Site (NTS) Power Department, completed the implementation of the data network Synchronous Optical Network (SON) ring and transition circuitry. The SON encircles the NTS with fiber cables, eliminates a single point of failure, and provides enhanced bandwidth capability.

NV is in the process of completing an alternate service route for the DOE portion of the Web Link Wireless Nationwide Advanced Messaging Network. This service provides a diverse route that does not utilize the existing services to move the signal from the server in Nevada to the satellite up-link in Atlanta, Georgia. The expected availability of this service is September 2004.

Oak Ridge Operations Office

Oak Ridge Operations Office continued to implement a wide area radio system that will resolve known safety, emergency preparedness, and mutual aid issues. The CD-1, Project Acquisition Execution Plan, Preliminary Hazards Assessment, Systems Requirements Document, Work Breakdown Structure, Project Execution Plan, and Government Cost Estimates are all complete. Oak Ridge requested HQ funding for the new trunked capable narrowband ultra HF mobile radio system to replace the analog wideband radio system. Oak Ridge PKI implementation to support encrypted network traffic continues and presently supports the National Weather Service as a retransmission site for the Emergency Manager's Weather Information Network.

Richland Operations Office, Hanford Site

The Hanford Site (HS) Narrowband Radio Upgrade Project (Project L 347) is approximately 50% complete and on schedule. System functional requirements are developed. The conceptual system design is approved and the detailed designs were issued to the field. Richland Operations Office (RL) field crews are fully engaged with installation activities. RL and the contractor working with HS's radio integration team have retro-fitted two repeater sites with new narrowband equipment. The new repeater site is operational and producing 30%

DEPARTMENT OF ENERGY (DOE) *continued*

increase in radio coverage versus the old systems. One-half of the new narrowband radio systems have been deployed. The balance of narrowband systems are scheduled to be fully deployed and operational by the end of FY 2003. Full system feature activation is expected by the third quarter of FY 2004. The new system allows dynamic communication capabilities for site emergency functions with automated interfaces to local, regional, and Federal safety agencies.

HS implemented enhanced PBX security measures to disable the system maintenance modem circuits and document these as operational circuits disabled for security purposes. These modem circuits can be temporarily activated by maintenance personnel and then immediately disabled upon completion of the maintenance activities. HS also implemented a personal computer based war dialing system to call every phone number (within all number ranges) on a quarterly basis to determine if any unauthorized modems are connected to the Integrated Voice Data Telecommunications System. If unauthorized modems are found, the modem will be disconnected and a determination made if additional measures are required.

Savannah River

The Savannah River Site Operations Center (SRSOC) now has radio communications capability with Aiken County's Fire and Emergency Medical Service personnel for drills and emergencies. This also gives Site ambulances more radio coverage.

Integration of the Remote Control-Control Stations (RCCS) to support the Savannah River Site (SRS) Operations Center is complete. These control stations provide the SRSOC an alternate path of access into the SRS trunking system in the event of a failure of the T1 circuits between SRSOC and the radio trunking site. This RCCS configuration permits continued radio communications with the SRS security and public safety talk groups via the SRSOC's CentraCom Elite communications consoles.

Savannah River has completed the installation of a video downlink for its helicopter forward-looking-infrared (FLIR) system. This downlink allows helicopter FLIR images to be distributed to Savannah River's Emergency Operations Center and other key locations.

DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Wide Area Networking

The Department of Veterans Affairs (VA) is optimizing its corporate WAN under the Telecommunications Modernization Project (TMP). Each TMP phase will facilitate the evolution of the VA WAN into a national resource capable of meeting VA corporate business applications and operational processes. Two phases have been completed. The remaining TMP phases are scheduled for completion by the end of FY 2004.

VA Nationwide Teleconferencing System

The VA Nationwide Teleconferencing System (VANTS) provides 24x7 audio and video teleconferencing services for business meetings, program planning sessions, distance learning, interviews, and hearings. VANTS customers include VA employees, emergency personnel, State officials, hospitals, universities, and other Federal government agencies, including DOD. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 Kilobit per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 960 audio ports for voice teleconferencing.

Frequency Management Automation

To expedite the engineering of new radio frequencies, VA uses the latest frequency management software, Spectrum XXI. Additionally, VA has joined the NTIA in pioneering a Government-wide, classified data exchange beta test that will make the Government Master File (GMF) of radio frequency authorizations available, in real time over the Internet. The initial database used for testing and debugging the system, will contain VA's unclassified radio frequency authorizations, except the law enforcement records.

Enhanced Mobile Satellite Services

VA coordinates with Defense Information Systems Agency to provide agency customers with Enhanced Mobile Satellite Services via the Iridium low earth orbit satellite constellation. In addition to the handsets assigned to hundreds of emergency responders in the field, VA has installed multi-exchange units at geographically dispersed locations to allow the handsets to dial directly into VA facilities via the satellite network. Many of the handsets are also equipped with approved Type I communications security devices to support secure voice communications.

VA California Emergency Communications System

The VA California Emergency Communications System ultra HF radio system is under engineering review for conversion from the existing analog, shared frequency radio system to a wide-area, digital trunking system capable of providing service to a widely expanded area with a vastly increased capacity for voice, secure voice, and data communications. This VA Trunking System will be integrated with the Federal, State, and local emergency communications systems to provide a high degree of interoperability for first responders, law enforcement, Special Operations, and day-to-day VA operations.

Office Of The Inspector General 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 very HF digital 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 radio system provides the highest degree of security in communications available today for IG field operations.

CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP TELECOMMUNICATIONS MISSION

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

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

TELECOMMUNICATIONS STAFF ORGANIZATION

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

The agency also provides telecommunications support to other U.S. government departments, agencies, and the military services as required to support intelligence requirements.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following CIA activities support NS/EP objectives:

- Active participation in the NCS activities of the COP/COR
- Continued support of the GETS, the FTSC, the TSP Program, and the SHARES HF 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 support to Defense Message System objectives and architecture.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP TELECOMMUNICATIONS MISSION

As a major component of the Department of Homeland Security (DHS), the Emergency Preparedness and Response Directorate (EP&R) inherited FEMA's mission of reducing the loss of life and property and protecting the Nation's critical infrastructure from all types of man-made and natural hazards through a comprehensive, risk-based, emergency management program of mitigation, preparedness, response, and recovery. In addition, the Directorate will continue to help prepare the nation to address the consequences of terrorism and to serve as the nation's portal for emergency management information and expertise. In this regard, EP&R evaluates new and existing technologies and telecommunications resources to ensure that the department has the capability to accomplish its mission.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

EP&R is seeking to improve the development and coordination of its all-hazards disaster programs among Federal departments and agencies, State and local governments, and other public and private sector organizations while responding to Presidential disaster declarations. EP&R actively directs its approach to disasters toward homeland security issues. EP&R helps communities to face the threat of terrorism, and its Office of National Preparedness endeavors to ensure that the nation's first responders are trained and equipped to deal with weapons of mass destruction. To benefit from their experience and to help first responders to be better prepared, EP&R reaches out and establishes working relationships with State and local first responder and public safety communications associations.

EP&R is moving the Disaster Management Program, an e-government initiative, forward in cooperation with DHS leadership and the Office of Management and Budget (OMB) to provide this critical service. The Disaster Management program consists of three synergistic services: (1) an interoperability service targeted at enabling responders to share incident information; (2) a responder "tool kit" that provides a basic suite of digital applications for responder organizations; and (3) an enterprise portal that provides disaster information and unstructured collaboration services to citizens and responders. The use of these services among responders and citizens continues to grow rapidly. The interagency Wireless Public SAFECOM is being transitioned to the DHS IA Infrastructure Protection Directorate.

FEMA SIGNIFICANT ACCOMPLISHMENTS

- As FY 2003 began, EP&R/FEMA was supporting 14 declared disasters. Since then, EP&R has responded to over 40 additional declared disasters and 15 declared emergencies. The support included the deployment of the disaster response teams to install telecommunication resources at disaster field offices (DFO); the processing of 89 TSP requests for provisioning new data and/or voice T-1s and 23 TSP requests for restoration priority of existing critical communication circuits; the reprocessing/recycling of 29,661 pieces of used IT equipment needed for DFO operations; and the billing of approximately $13 million new IT services in support of disaster operations.
- EP&R participates in GETS, WPS, and has added TSP restoration priority to most of EP&R's critical communication circuits.
- Designed and installed secure/non-secure video conferencing systems at the DHS Nebraska Avenue facility, other Federal locations, 54 State/Territorial emergency operations centers, and 25 governor's offices.
- Delivered secure telephone instruments to all State/Territorial governor's offices.

THE JOINT STAFF (JS)

NS/EP TELECOMMUNICATIONS MISSION

The J6 provides advice and recommendations on C4 matters to the Chairman of the Joint Chiefs of Staff (CJCS) and to the Joint Chiefs of Staff (JCS). J6 develops policy and plans, monitors programs of joint C4 systems, and ensures adequate C4 support to the NCS, Commander in Chiefs, and warfighters for joint and combined military operations. The J6 leads the C4 community, conceptualizes future C4 system architectures, and provides direction to improve joint C4 systems. The J6 oversees C4 support for the National Military Command System (NMCS).

TELECOMMUNICATIONS STAFF ORGANIZATION

The J6 Directorate is led by the Director and Vice Director.
The Director chairs the Military Communications-Electronics Board (MCEB) for the Secretary of Defense. The Director and Vice Director are general/flag officers from the Military Departments. The J6 Directorate includes functionally aligned Division, Programs and Budget sections, and a Director's Action Group.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

(Refer to DOD Section)

PENDING ISSUES

(Refer to DOD Section)

JS SIGNIFICANT ACCOMPLISHMENTS

(Refer to DOD Section)

GENERAL SERVICES ADMINISTRATION (GSA)

MISSION

The mission of GSA Federal Technology Service (FTS) organization is to provide information technology solutions and network services that deliver best value and innovations to support customers' missions worldwide. The FTS NS/EP mission ensures that federally owned or managed domestic communications facilities and services meet the NS/EP requirements of the Federal government.

CURRENT/ONGOING ACTIVITIES

The FTS provides a variety of network services and information technology solutions that meet and/or exceed the Federal government's current and future NS/EP needs. Telecommunication's offerings such as global voice, data and video services continually support both local and long distance coverage to the Federal community and continues to be utilized by tribal, State, and local governments through the sponsorship of various Federal departments and agencies.

GSA continually supports the NCS activities by dedicating a full-time FTS detailed employee to the NCS National Crisis Coordinating Center. Additionally, GSA FTS has identified 11 of its Regional Emergency Communications Planners (RECP) to provide expert telecommunications advice and services to the NCS as a NCS Regional Manager. These GSA personnel provide services as the Federal Emergency Communications Coordinator to FEMA and the Office of Science and Technology Policy during national security emergencies and/or Presidentially declared disasters.

During FY 2003, GSA FTS introduced a new contract vehicle called Connections. Connections is an eight-year multiple award, indefinite delivery, indefinite-quantity contract with a base period of three years and five, one-year options. Connections provides telecommunications equipment, support services, and solutions to Federal agencies, replacing multiple expiring, regional equipment and services contracts, and consists of three service categories: equipment and services, support services, and solutions. Equipment and services are comprised of voice, data and video equipment, microwave systems, wire and cable, and installation and maintenance. The support services category offers a variety of technical and professional labor skills. The solutions category includes infrastructure-related requirements using turnkey solutions, integration services, and managed services.

Additionally, FTS assembled Connections with an impressive array of industry partners with over 50% of the awards going to small business. Connections' wide range of telecommunications equipment and services, combined with flexible packaging options, enables FTS to better support the needs of its customers. This award gives customers a choice of industry partners, packaging options, and solutions designed to facilitate the convergence of voice, data, and video solutions in the federal workspace. Connections equipment and services are being offered throughout the U.S., District of Columbia, Virgin Islands, Puerto Rico, American Samoa, Guam, Saipan, and the Northern Mariana Islands.

The FTS provides contract vehicles for worldwide telecommunications services, international direct distance dialing, wireless voice and data, satellite services, internet access, technical services support, digital signature and managed PKI services, information security products and services, and IA services for CIP. Multi-Tiered Security Profiles is an initiative of the FTS that is designed to provide enhanced Network Service offerings by integrating various security layers into the current portfolio of contracts. The FTS Center for Information Security Services (CISS) developed the Safeguard and Access Certificates for Electronic Services (ACES) programs, and awarded contract vehicles to assist agencies with their security requirements and meet legislative mandates such as the Federal Information Security Management Act and the Government Paperwork Elimination Act.

The FTS Safeguard program provides services and products to assist agencies in meeting the mandates of the Federal Information Security Management Act of 2002, which requires that agencies conduct annual IG security evaluations; report to OMB annually on the state of security of their information systems; and requires an annual OMB report to Congress. Safeguard's solutions assist agencies in the assessment, protection and monitoring of their systems; and in the development of a strong security architecture for their enterprise that supports the vision of the *President's National Strategy for Homeland Security; The National Strategy to Secure Cyberspace; and the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.*

GENERAL SERVICES ADMINISTRATION (GSA) *continued*

The FTS ACES program provides digital certificates and managed PKI services to assist Federal agencies in meeting the requirements of the Government Paperwork Elimination Act, Presidential Directive on Electronic Government, Health Insurance Portability and Accountability Act, E-Government Act of 2002, and the Electronic Signatures in Global and National Commerce Act. The ACES program provides the infrastructure that allows agencies to meet their expanding electronic government initiatives without the burden and expense of building their own PKI. The ACES program also meets OMB's guidance on Streamlining Authentication and Identity management within the Federal Government. The ACES Program will be fully cross-certified with the Federal Bridge Certificate Authority by the end of FY 2003.

The FTS CISS is working closely with NSA and the Committee for National Security Systems (CNSS) Crypto Modernization Working Groups to assist customer agencies in modernization of legacy crypto systems. NSA has identified a list of legacy crypto equipment that will require replacement by modern technology equipment utilizing a more secure key. CISS has provided all customer agencies with options to modernize their secure systems.

The GSA FTS Federal Computer Incident Response Center (FedCIRC) became part of DHS on March 1, 2003. FedCIRC's new assignment will continue to support the Federal Government as a trusted focal point for computer security incident reporting and providing assistance with incident prevention and response. FTS continues to work very closely with the FedCIRC as a valued Federal partner, sharing developments, standards and trends for consistent, comprehensive/cost-effective ways to protect the nation's critical infrastructures.

GSA SIGNIFICANT ACCOMPLISHMENTS

- GSA FTS was recognized by the CNSS for its significant contributions, dedication, and commitment to shaping the goals for building a strong, viable national IA program.
- The FTS Safeguard program has awarded four task orders that have greatly enhanced the security posture of DHS Bureau of Customs and Border Protections (formerly part of the U.S. Customs Service). Through these task orders, Customs has established a well structured IA and CIP program which includes performing Business Impact Analysis, Certification and Accreditation, Data Recovery and Duplication Services, and Enterprise Security Services.
- The FTS Safeguard program awarded a task order that has provided the U.S. Army Reserve Command (USARC) with a means of assessing the Anti-Terrorism/Force Protection Vulnerabilities of all USARC units within a three year time frame. This task order has exceeded the expectations of the client by not only meeting the challenge of performing 1100 anti-terrorism/force protection vulnerability assessments, but also providing USARC with recommendations for enhanced security of their critical physical and electronic assets.
- The FTS Safeguard program is providing the CDC with a broad range of lifecycle IT support and security services needed to develop and maintain a variety of data-focused systems that are highly interactive in a collaborative environment with their stakeholders and are pivotal to their mission. The systems are associated with bio-terrorism preparedness and were used during the Severe Acute Respiratory Syndrome situation.
- The FTS ACES program is supporting DHHS in obtaining the services needed to implement and deploy the initial phase of an agency-wide PKI. DHHS is committed to the implementation of an enterprise wide PKI in support of the Department IT Strategic Plan. Specifically, this support will entail building the infrastructure needed to issue digital

GENERAL SERVICES ADMINISTRATION (GSA) *continued*

certificates to DHHS entities, implementing a Certificate Acceptance Infrastructure to validate certificates and provide interoperability with the Federal Bridge Certification Authority and the eAuthentication gateway, and acquiring a PKI-enabling toolkit to integrate digital signatures into the HHS business process. Additionally, ACES is supporting the Social Security Administration's (SSA) Prisoner Reporting Application. Specifically, FTS supported the development and deployment of a peer-to-peer secure transport mechanism using digital certificates to exchange data between the SSA and prisons. This application will be expanded to nearly 2500 prisons to allow the automatic exchange of data incorporating digital signatures, electronic postmarks and validation services provided by the eAuthentication Gateway.

- The FTS supported the FBI Trilogy Project. This is a WAN connecting different geographical LANs within the FBI nationwide using ATM and frame relay.

- The FTS supported the FBI's Satellite Diversity Project. This is the backup to the FBI's Trilogy Network.

- The FTS supported the DOJ, INS' backbone network. This is the telecommunication backbone installed for use by the newly formed DHS.

- The FTS supported the U.S. Custom Services' Managed Router Network which ties into the classified DHS network. Some of the services from the Treasury Communications System were moved over to FTS2001. Routers were placed at various 900 end locations, along with industry partner experts to manage the new network.

- The FTS supported the DOT, U.S. Coast Guard's Secure Frame Relay Services connecting 178 remote recruiting sites.

- Since 1999, FTS has awarded 50 Metropolitan Area Acquisition (MAA) contracts in 25 metropolitan areas across the nation. Three-fourths of the Federal workforce is now within reach of an MAA, with attractive prices and state-of-the-art service offerings. When Winstar Communications faced liquidation before the Bankruptcy Court of Delaware, GSA's FTS teamed with DOJ and the FCC to ensure that the Government's interests were fully represented. During this process, FTS updated its contingency plans to enable quick response should bankruptcy court decisions become unfavorable to the interests of our customers. Fortunately, Winstar was purchased by IDT and the crises were averted.

- The GSA FTS Northeast and Caribbean Region (Region 2) has provided regional support directly to the NCS, jointly cooperated on missions, and undertaken other activities for the purpose of improving the Region's security and survivability of communications in the event of a terrorist attack or natural disaster event. The FTS Regional Emergency Support Function Coordinator and other FTS personnel participated in Regional Interagency Steering Committee (RISC) planning activities in New England, Puerto Rico, the Virgin Islands, and New Jersey. This also included a briefing to share lessons learned during our response to the terrorist attacks on September 11, 2001. FTS has coordinated the distribution of key NCS services. WPS units, GETS accounts, and GlobalStar Satellite telephones have been distributed to key GSA Officials. Joint NCS/FTS briefings on these programs have been given to key municipal emergency workers at One Police Plaza in New York City, New York. GSA has completed the construction of two "hot" COOP sites in New York City and Newark, New Jersey to serve as Emergency Operations Centers in the event that a catastrophic event disables the Regional Headquarters at 26 Federal Plaza in New York City. These sites have fully redundant telecommunications and data capabilities. GSA is currently issuing Smart Cards to GSA employees, Federal tenants, and contractors at 26 Federal Plaza; installing Smart Card actuated building entrance portals (turnstiles); and will have a fully operational Smart Card entrance system by the end of the FY 2003. Federal Plaza is one of the largest multi-tenant Federal office buildings in the country.

GENERAL SERVICES ADMINISTRATION (GSA) *continued*

- GSA FTS Mid-Atlantic Region (Region 3) participated in a multi-agency exercise to represent and promote NCS Emergency Support Functions (ESF) -2 (telecommunication) requirements. Additionally, in the quest to establish redundant communications, GSA's FTS Mid-Atlantic Region set up a capability to accomplish diverse routing in their Regional Office Building and its alternate facility. Their installation of separate Centrex lines in addition to already established PBX/Primary Rate Interfaces and its future installation of a microwave link from their building to local service provider switches, will allow the Mid-Atlantic Region multiple utilization options when underground cables are affected by unforeseen circumstances.

- GSA, FTS Great Lakes and Northwest Artic Regions participated in a mock exercise to help combat terrorism. TOPOFF II was conducted by the governments of the U.S. and Canada. During this exercise FTS RECP provided ESF-2 communications support and illustrated the many reasons Federal, State, and local governments should establish redundant and diverse routing communication capabilities. They also stressed the need for an alternate means of communication when telecommunication systems become saturated or unusable.

- The GSA FTS Southeast Sunbelt Region (Region 4) represented the NCS at all FEMA's Region 4 RISC and Documentation Committee meetings. It hosted and addressed the NCS Telecommunications Seminar held in Atlanta, Georgia, as well as participated in the 2003 NCS Regional Manager/Individual Mobilization Augmentee (IMA) Program Conference. The Southeast Sunbelt Region provided ongoing telecommunications training to the NCS IMAs and hosted each IMA on their annual training and drill days in Atlanta. It should also be noted that the Region worked with the NCS to place TSP on all GSA Southeast Sunbelt Regional PBXs, and was successful in assuring that WPS was provided to the FTS Assistant Regional Administrator, Network Services Director, Regional, and Deputy Emergency Communications Planners to assure priority restoration of trunk circuits in the event of a catastrophic outage.

- The GSA, FTS Pacific Rim (Region 9) RECP was called upon to provide ESF-2 support for multiple disasters during FY 2003. This support included the disaster response and recovery efforts to the American Samoa floods, Guam/Rota Super Typhoon Pongsona, and the Arizona Wild Fires. Additionally, the Region 9 RECP coordinated and implemented the establishment of the Region 9 COOP Center's telecommunications infrastructure.

- The FTS continues to provide vendors and agencies information regarding all FTS services, including disaster support, contingency planning, and COOP services through the GSA home page (http://www.gsa.gov).

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP TELECOMMUNICATIONS MISSION

The National Aeronautics and Space Administration (NASA) shall (pursuant to an E.O. dated February 28, 2003) coordinate with the Secretary of Homeland Security 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 NCS process. The Associate Administrator for Space Flight assigned the Assistant Associate Administrator for Space Communications as NASA's COP member.

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 (NISN).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

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

NASA also continues to actively participate in the SHARES HF Radio Program, GETS, Interagency Committee on Search and Rescue, the Federal Wireless Users Forum, and the NCS Technology and Standards Accomplishments.

NASA NS/EP TELECOMMUNICATIONS ASSETS

- The NISN supports both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency, its contractor and research partners, and International Space Partners.
- NASA Space Network is a constellation of geostationary Tracking and Data Relay Satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft and other supported customer satellites.
- NASA Deep Space Network (DSN) supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.
- NASA Ground Network (GN) supports Low-Earth orbiting space flight missions. NASA obtains a significant portion of GN services from the commercial market.
- 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.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA) *continued*

NASA SIGNIFICANT ACCOMPLISHMENTS

- Upgraded NASA's mission support communications network.
- Provided additional connectivity to the world wide DSN complexes.
- Completed upgrades to the Russian services infrastructure which supports the International Space Station.
- Installed a very high speed backbone network service connection to support Earth Observing spacecraft data.
- Deployed an Integrated Financial Management Program Network to all NASA Centers.

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 U.S. 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

The NRC Emergency Telecommunications System (ETS), which provides NS/EP communications from nuclear power plants and major fuel cycle facilities, consists of FTS 2001 Direct Access Lines at most locations. At twenty-three sites, ETS is provided using the utilities' corporate communications systems. GETS continues to be highly recommended by NRC as a means of enhancing access to long distance service. TSP coverage is assigned to at least one circuit at each FTS 2001 served ETS site. The NRC is working to add secure teleconferencing capability to the ETS. The NRC and NCS met to discuss the Emergency Notification Service Pilot Program. The NRC is currently considering whether to participate in that program.

NRC SIGNIFICANT ACCOMPLISHMENTS

- The NCS successfully upgraded NRC's existing Alerting and Coordination Network (ACN) service in February 2003. They disconnected the ring down circuit that existed between NCS and NRC and installed a new circuit with a VoIP telephone.
- NRC successfully used GETS access numbers during their response to the September 11th terrorist attacks.
- NRC continues to promote GETS as a means of improving emergency telecommunications at nuclear power plants.
- NRC continues to recommend to licensees that GETS be included in their contingency plans.
- NRC continues to encourage emergency response staff at NRC to place quarterly test calls through GETS and to include GETS in the agency contingency plans.
- The total number of active GETS card holders at NRC rose from 294 to 372 during the year.
- TSP coverage has been assigned to one primary FTS 2001 ETS circuit at each FTS 2001 served site.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP TELECOMMUNICATIONS MISSION

The NTIA NS/EP mission as tasked under E.O.s 12046, 12472, and 12656 include serving as the Executive Branch telecommunications policy adviser to the President, serving as the manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board. Thus, among other things, NTIA advises and assists the President in the administration of a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support NS/EP functions.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The NTIA/Office of Spectrum Management (OSM) continues to plan and implement, using a phased approach, a series of Federal spectrum management system improvements to include the capability for total electronic transfer and use of Federal spectrum management information and data. 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:

- Updated and implemented various planned outcomes and improvement goals in the NTIA Federal Spectrum Management System/IT Improvements Plan, e.g., provided the Federal spectrum management community with the capability to access and exchange electronic copies of all official, unclassified Interdepartment Radio Advisory Committee (IRAC) documentation via a Web-based server capability and updated search software and indexes for searching electronic files of IRAC documents.

- Implemented, for use by NTIA essential personnel, the architecture for alternate site processing of Federal spectrum management data, communications, and operations.

- Partnered with DOD's Joint Spectrum Center to develop and field: (1) SPECTRUM XXI Version 4.0 for use by all Federal spectrum managers; (2) for evaluation and testing, the initial operating capability (IOC) version of an icon-based, graphical user interface supported by sophisticated logic that will serve as the method used by Federal agencies to develop and submit spectrum certification requests to NTIA; and (3) the IOC version of the Statistical Database Viewer to display in several ways various spectrum information including allocation tables and associated spectrum-use statistics; and other automated capabilities.

In addition, the NTIA/OSM-

- Provided Co-Chair of the GETS/WPS User Council and participated in Council activities and endeavors as well as provided GETS user authorizations to all new NTIA emergency essential personnel

- Participated in various activities and endeavors relative to national emergency management and continuity of government as well as agency COOP

- Participated in various activities and endeavors of the President's NSTAC

- Participated in NCS COP/COR activities and endeavors

- Participated in NCS SHARES HF Coordination Network Interoperability Working Group activities and endeavors

- Completed Memorandum of Agreement between the Manager, NCS and the Administrator, NTIA in which the NTIA agreed to provide a person to support NCS missions and NS/EP telecommunications requirements to include serving as a non-resident member of the National Coordinating Center for Telecommunications

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) *continued*

- Began implementing a FY 2003 Budget Initiative, Paperless Spectrum Management Process, that will enhance technology development and commercialization by improving the use of spectrum through increased spectrum sharing and efficiency
- Began implementing a second FY 2003 Budget Initiative, National and International Spectrum Reform, that will overhaul and rebuild the international and domestic radio frequency spectrum management processes to be more responsive, effective, and efficient in various ways.

NTIA SIGNIFICANT ACCOMPLISHMENTS

- Conducted over 200 meetings of the IRAC and its Subcommittees and ad hoc groups.
- Processed over 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 various meetings of International Telecommunication Union working groups, study groups, etc. to include the 2003 World Radio Conference.
- Served as the lead agency for the Information and Communications (I&C) Sector of the nation's critical infrastructures; as such, chaired the I&C Sector Working Group and its Subcommittees to promote information sharing and coordinated action to mitigate CIP 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 NSA has an operational mission to support the critical intelligence needs of DOD and the national security community, and to provide the technical support necessary to develop and maintain the security and protection of NS/EP telecommunications. NSA's customers include a broad range of users of the National Information Infrastructure and the critical infrastructure communities. IA activities include a close working relationship with the National Institute of Standards and Technology (NIST).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Support To Counter-Terrorism And Operation Iraqi Freedom

- NSA continues to develop and make available IA solutions for the U.S. Government to support national and international activities.
- Provided quantities of security products, IA systems security, installation, training, and cryptographic keying material to protect voice and data communications in support of Operation Iraqi Freedom and other initiatives across the national security community.
- The NSA Interagency Operations Security (OPSEC) Support Staff continues to assist in improving the U.S.'s OPSEC posture by providing awareness, training and support.

National IA Support

- NSA continues to lead the activities of the CNSS.
- Strengthening the partnership with the NIST to grow and maintain the National Information Assurance Partnership's Common Criteria Evaluation and Validation Scheme, to enable the successful implementation of NSTISSP-11.

Coalition Interoperability

- NSA is leading the development of Cross Domain Solutions to ensure secure transfer of information between security domains, enabling Secure Coalition communications capabilities.
- Developing the Content-Based Information Security solution to provide secure bilateral and multi-lateral coalition information exchanges.

Information Assurance Technology Development And Roll-Out

- Continuing to develop high assurance IA products and technologies to address the needs of the U.S. Government.

Cross Domain Solutions

- Providing technical and risk analysis for secure network interconnection to system's certifiers and accreditors in DOD and the Intelligence Community.
- Developing a High Assurance Guarding solution to support Intelligence Community trusted interface initiatives.

Wireless

- Developing a secure BlackBerryTM wireless e-mail device that utilizes the DOD PKI via a Common Access Card interface.
- Developing a secure, dual mode, Code Division Multiple Access (CDMA) wireless phone that will provide secure voice and data over any CDMA network in the U.S.

Secure Telephony

- Developed and delivered next generation narrow band devices that provide desktop interoperability with secure wireless products without replacing a STU-III.
- Developing an STE capability to provide secure telephony over Internet Protocol (IP) networks.

High Assurance IP

- Leading an industry/Government team in developing a common High Assurance IP Interoperability Standard (HAIPIS) for future IP In-line encryptors including a foreign interoperability appendix to allow seamless interoperability with allied and coalition partner's HAIPIS compliant solutions.
- Developing a Gigabit Ethernet Encryptor that will provide secure data transfer at a minimal performance throughput of 1 Gigabit per second (Gbps) with a planned migration to 10 Gbps.

NATIONAL SECURITY AGENCY (NSA) *continued*

Crypto-Modernization Program

- The Crypto-Modernization Initiative continues to gain momentum toward the modernization of an aging cryptographic product inventory, meet increased interoperability requirements, and keep pace with information technology evolution.

- NSA IA products and supporting infrastructures, currently in development, have addressed enabling modern cryptography.

Support To National Critical Infrastructure Issues

- Provided services including threat, vulnerability, information regarding cyber incidents, and risk assessments.

- Provided security guidance for ongoing NS/EP programs, including the Global Early Warning Information System.

National Security Incident Response Center

- The National Security Incident Response Center (NSIRC), including a NSIRC Desk Officer 24/7 time-sensitive operations desk, provided expert assistance to the national security community regarding cyber incidents and computer network defense. NSIRC provided unique, tailored, time-critical, and term reporting based on NSIRC's ability to detect, react, warn, and respond to intrusions into U.S. Government cyber networks and provided all-source threat reporting on foreign threats to U.S. information systems and the effect on operations, exercises, information systems, and force protection.

The NSIRC partnered with other NSA offices, organizations within the DOD, the intelligence community, and other Federal agencies through DHS and its components: FedCirc, NIPC, and the NCS. NSIRC also partnered with the Network Security Information Exchange, industry, academia, and others to share information about and respond to, cyber events.

U.S. POSTAL SERVICE (USPS)

NS/EP TELECOMMUNICATIONS MISSION

The U.S. Postal Service (USPS) delivers to almost 138 million homes, businesses, and post office boxes. In support of that effort, the USPS maintains one of the largest computing infrastructures in the world. The infrastructure is comprised of more than 547,000 hardware components that support 170,000 users utilizing more than 1,100 business applications in over 14,000 locations. Every day the IT organization gets the job done-securely, efficiently, and economically.

The USPS has not been assigned any specific NS/EP telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs, engineers, and develops telecommunications systems, services, and solutions to support day-to-day organizational, administrative, and operational mission requirements.

FY 2003 Infrastructure Components	Quantity
Local Area Networks	14,000
Desktop PCs	130,000
Laptops	30,000
Retail Terminals	66,000
Business Partner Connections	700
Remote Dial-up Accounts	26,000
Virtual Private Network Connections (Cable/Broadband)	3,000
Satellite Connections	12,000
Handheld Scanners	330,000

USPS SIGNIFICANT ACCOMPLISHMENTS

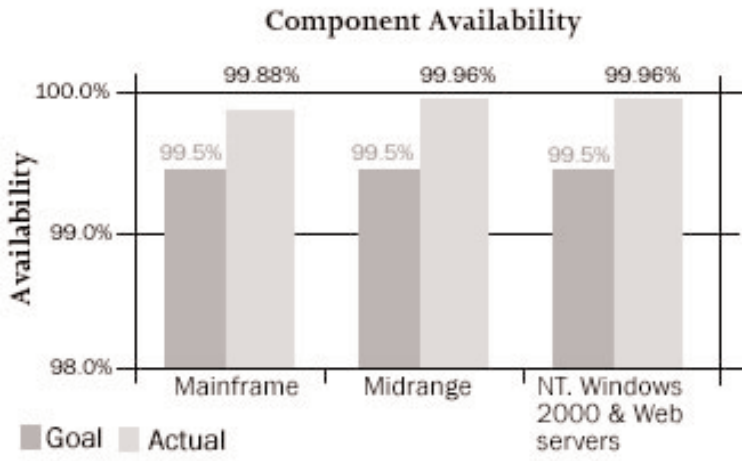
Implementing the Advanced Computing Environment

During FY 2003, the USPS has deployed an infrastructure plan for a uniform, distributed, computing environment within the Postal Service called the Advanced Computing Environment (ACE) and it is anticipated the initiative will save the Postal Service more than $100 million over 5 years.

In FY 2003, over 75,000 employees migrated to ACE and District help desk consolidation has been completed.

ACE deployment will include reducing:

- 270 standard software packages to 60
- 85 District help desks to one
- 13,000 servers to 1,500, but with increased capacity
- 11,000 support locations to 540.



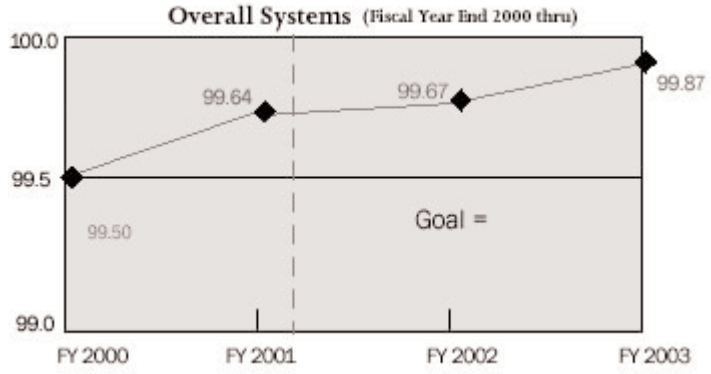
During FY 2003, the Postal Service also:

- Deployed an Active Directory infrastructure for a single sign-on capability
- Removed more than 3,700 servers from service-reducing redundancy, maintenance, and management costs
- Negotiated contracts for help desk consolidation, ACE deployment, and e-mail replacement, saving more than $10 million.

U.S. POSTAL SERVICE (USPS) *continued*

USPS SIGNIFICANT ACCOMPLISHMENTS

As of the end of the FY 2003, almost 1,400 Blackberry wireless communications devices had been deployed to Postal Service executives. This important tool allows USPS executives to be mobile without loss of critical communications.



Improving Service Standards
The IT Portfolio groups launched a comprehensive effort to improve systems availability through process management and development of systems availability performance metrics and indicators. The result of this effort was an improvement of systems availability overall to the point systems were operational an unprecedented 99.87% of the time during FY 2003, surpassing all Service Level Agreement requirements.

Enhancing Security
During FY 2003, the USPS IT Corporate Information Security Office (CISO) made significant progress in creating a climate where employees, customers, and partners understand security brings real business value to USPS products and services. The Postal Service had no significant security breaches or viruses that could have prevented USPS from serving customers or conducting day-to-day business functions.

Also during FY 2003, the Postal Service designed and put into operation the initial elements of a layered defense that includes strengthening firewalls, guarding the network perimeter, implementing initial baseline hardening standards, and enhancing access controls.

Supplementing the USPS layered defense initiative are:

- Enhanced intrusion detection software
- Scheduled infrastructure vulnerability assessment tests that include critical and high-risk sites as well as identified vulnerabilities
- Scheduled network scans to identify potential risk areas.

In addition, USPS established crisis management and incident response teams to identify, contain, and respond to security threats, including the development of COOP procedures and shadow infrastructure to assure the continuity of essential business functions in the event of a wide range of emergencies or threats.

U.S. POSTAL SERVICE (USPS) *continued*

USPS SIGNIFICANT ACCOMPLISHMENTS

Protecting Postal Service information resources from threats and ensuring the integrity of Postal Service applications and technologies covers a tremendous territory:

- Over 4 million e-mail messages scanned monthly for viruses
- Over 55 billion network data packets scanned monthly for evidence of intrusion
- Over 2,000 employees a month viewing the Postal Service security awareness video
- Over 2.3 million files a month being transferred securely using Assured File Transfer.

Working With DOD
The Postal Service has a long-standing relationship with DOD in facilitating the overseas delivery of mail to the men and women of the armed forces. The Military Postal Service Agency moves mail on aircraft and ships to more than one million service men and women in more than 160 countries and aboard Navy and Coast Guard ships.

- This past year the Postal Service and DOD continued to improve the Automated Military Postal System, which automates many military postal processes and provides detailed information on military post operations, transportation costs, and daily retail financial transactions. The system will reduce paperwork and labor costs and improve timing and accuracy of air carrier payments.
- USPS is also working with DOD to improve the electronic presentation of mailing addresses and to promote adherence to domestic and international mailing requirements. The project involves development of postal address information in an XML format that makes it easier to generate data and communicate internationally via the Web.
- USPS has also worked closely with DOD to assure that mail destined to U.S. troops Iraq and Afghanistan kept flowing from home.

Supporting LMRS Requirements
In order to support the federally mandated narrow-band conversion effort for LMRS, the Radio Frequency and Wireless Group utilize a Indefinite Delivery, Indefinite Quantity (IDIQ) contract for radio frequency analysis, engineering, hardware/software implementation, and maintenance contract. This contract vehicle was initially awarded in FY 2000 and continues to provide the most comprehensive handheld, base station, and repeater LMRS solution package within the civilian federal arena. Over 350 frequency assignments were converted to narrowband in FY 2003.

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 "operation and liquidity of banks," the "maintenance of national monetary, credit, and financial systems," and the "maintenance and restoration of stable and orderly markets." The FRB does not have telecommunications assets listed as 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 IT 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 COP.

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 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.

In December 2002, the FRB expanded its sponsorship criteria to include large-value clearing and settlement systems and major financial services exchanges and utilities. The FRB also continues to sponsor the GETS for essential Federal Reserve Bank services. In 2002, the FRB began sponsoring GETS for other key participants in the nation's payment systems as well as those foreign central banks that are critical to the maintenance of the nation's economic posture.

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 and expanded in 2002. The FRB continues to sponsor TSP assignments for the following:

- 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.
- Voice and data circuits supporting Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities.
- 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 the FRB's eligibility criteria.

In December 2002, the FRB began to sponsor TSP assignments for the following:

- Circuits used for large-dollar clearing and settlement services, including access circuits to the Federal Reserve's net settlement service, the networks of Automated Clearing House (ACH) operators, the Continuous Linked Settlement (CLS) bank, and the major clearing corporations and securities exchanges circuits used by ACH operators and the CLS bank that meet the FRB's eligibility criteria.
- Circuits connecting customers of Fedwire, SWIFT, and CHIPS that meet the FRB's eligibility criteria.

FEDERAL RESERVE BOARD (FRB) *continued*

By the end of FY 2003, the FRB will have sponsored approximately 3,000 active TSP assignments.

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. In December 2002, the FRB began sponsoring other key participants in the nation's payment systems. By the end of FY 2003, the FRB will have sponsored approximately 30 institutions.

During the FY 2002, the FRB participated in the WPS pilot for Washington, DC, and New York City, New York, and continues to use the service at these locations. In FY 2004, the FRB will implement a WPS program 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.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

NS/EP TELECOMMUNICATIONS MISSION

The FCC NS/EP responsibilities include:

- Evaluate and strengthen measures for protecting U.S. telecommunications, broadcast and other communications infrastructure and facilities
- Ensure rapid restoration of U.S. telecommunications, broadcast, and other communications infrastructure and facilities after disruption by a terrorist attack or natural disaster
- Ensure that public safety, public health, and other emergency and defense personnel have effective communications services available to them in the immediate aftermath of any terrorist attack or natural disaster within the U.S.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Much of what the FCC does either directly or indirectly affects the NS/EP telecommunications activities of other Government departments and agencies. In the wake of the September 11 attacks, the FCC created the Homeland Security Policy Council (HSPC) to further the agency's NS/EP Telecommunications Mission. The HSPC has worked with other government entities and with industry on homeland security matters and coordinated Commission actions to improve homeland security.
In July 2003, the FCC established an Office of Homeland Security to provide consolidated support for the homeland security and emergency preparedness responsibilities of the Commission, the FCC's Defense Commissioner, and the HSPC.

Some of the most relevant FCC actions in support of NS/EP Telecommunications are described below.

Rechartering The Network Reliability And Interoperability Council

The FCC rechartered the Network Reliability and Interoperability Council (NRIC), a Federal Advisory Committee, to emphasize the threats to network services and infrastructure caused by terrorist attacks and natural disasters. NRIC VI now consists of senior executives representing communications firms from all segments of the industry. NRIC VI has developed best practices to help prepare against such threats and hasten restoration of network services in their aftermath. Since making the best practices available in March 2003, the NRIC has been engaged in a vigorous outreach program to increase industry awareness of the new practices.

Chartering The Media Security And Reliability Council

The FCC chartered a "media counterpart" to NRIC, the Media Security and Reliability Council. This consortium of broadcast, cable and satellite companies met on May 28, 2003, and reviewed its initial 34 best practices ranging from encouraging media companies to conduct vulnerability assessments to seeking enhancement of public warning systems through a public/private partnership.

Promoting TSP

The FCC worked with the NCS to develop an outreach program designed to ensure that the nation's 911 centers (Public Safety Answering Points) are registered in the TSP program. The program includes TSP presentations at stakeholder conferences and workshops, articles endorsing the TSP program for their newsletters, development of best practices for 911 center participation, and development of detailed guidance to help 911 centers determine which services to enroll in the program. The FCC also announced for the first time that it will sponsor all 911 centers' participation in the program.
In addition, the FCC and NCS have developed expedited procedures to significantly reduce the time for enrollment.

Enhancing Public Safety Communications

The FCC adopted a Report and Order (R&O) in the 4.9-gigahertz proceeding, which established licensing and service rules for spectrum in the band. This item will open the door for the deployment of new broadband technologies and provide substantial flexibility to increase spectrum utilization and foster interoperability. Also, the FCC adopted an R&O that sets aside channels specifically for low power public safety operations.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

continued

Fostering Availability And Implementation Of Wireless E911

The FCC continues to work extensively with mobile wireless carriers, the public safety community and local exchange carriers to facilitate the deployment of 911 and E911 service. On April 29, 2003, the Commission hosted its first E911 Coordination Initiative which was attended by representatives from the Federal Government, the public safety community, wireless carriers, and local exchange carriers. The FCC completed the task of obtaining a Governors 911 designee from the remaining approximately 25 states, thereby fulfilling the requirement established in the Wireless Communications and Public Safety Act of 1999.

Exploring New Policy Options For Enhancing Public Safety Communication

The FCC formed the Spectrum Policy Task Force to assist the Commission in identifying and evaluating changes in spectrum policy that will increase the public benefits derived from the use of the radio spectrum. One of the Task Force's most important objectives was to assist the Commission in addressing ubiquitous spectrum issues, including, interference protection and effective public safety communications.


NATIONAL COMMUNICATIONS SYSTEM
NCS

A

Acronyms

A

NCS RELATED ACRONYMS

2

24x7	24 hours, 7 days a week

3

3G	Third Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2

A

ACE	Advanced Computing Environment
ACES	Access Certificates for Electronic Services
ACH	Automated Clearing House
ACN	Alerting and Coordination Network
ACR	Alternate Carrier Routing
AGCS	AG Communications Systems
AIN	Advanced Intelligent Network
ANSI	American National Standards Institute
AOF	Alternate Operating Facility
ASD (HD)	Assistant Secretary of Defense for Homeland Defense
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
ATG	Advanced Technology Group
ATM	Asynchronous Transfer Mode

B

BDT	Backup Dial Tone
BGP	Border Gateway Protocol
BPA	Bonneville Power Administration
BT	British Telecommunications

C

C4	Command, Control, Communications and Computer Systems
C&A	Certification and Accreditation
CCP	Classified Connectivity Program
CCPC	Civil Communications Planning Committee
CDC	Centers for Disease Control

CDMA	Code Division Multiple Access
CERT	Computer Emergency Response Team
C.F.R.	Code of Federal Regulations
CFWG	Critical Facilities Working Group
CHIPS	Clearing House Interbank Payments System
CIA	Central Intelligence Agency
CIIA	Critical Infrastructure Information Act of 2002
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Corporate Information Security Office
CISS	Center for Information Security Services
CJCS	Chairman of the Joint Chiefs of Staff
CLS	Continuous Linked Settlement
CMRS	Commercial Mobile Radio Service
CNSS	Committee for National Security Systems
COG	Continuity of Government
ComSec	Communications Security
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
COTS	Commercial Off-The-Shelf
CPAS	Cellular Priority Access Service
CRIS	Communications Resource Information Sharing
CTIA	Cellular Telecommunications and Internet Association
CWIN	Critical infrastructure Warning Information Network
CY	Calendar Year

D

DFO	Disaster Field Offices
DHS	Department of Homeland Security
DHHS	Department of Health and Human Services
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOEnet	DOE Corporate Network
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DSN	Deep Space Network
DWDN	Dense Wave Division Multiplexing

E

ECA	External PKI Certificate Authority
ECN	Emergency Communications Network
E-Mail	Electronic Mail
EMC	Emergency Management Centers
eMLPP	enhanced Multi-Level Precedence and Preemption
EMP	Electromagnetic Pulse
EMS	Emergency Medical Service
ENS	Emergency Notification System
ENM	Enterprise Network Management
E.O.	Executive Order
EOC	Emergency Operations Center
EOT	Emergency Operations Teams
EP&R	Emergency Preparedness and Response Directorate
ERLink	Emergency Response Link
ERT	Emergency Response Training
ESF	Emergency Support Function
ESF-2	Emergency Support Function -2
ETS	Emergency Telecommunications System
ETSI	European Telecommunications Standards Institute
Extranet	External Network

F

FASI	Foreign Affairs Systems Integration
FBC	Facility Backup Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCRS	Foreign Credit Reporting System
FDA	Food and Drug Administration
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FLIR	Forward-Looking-Infrared
FNBDT	Future Narrow Band Digital Terminal
FOC	Full Operational Capability
FOIA	Freedom of Information Act
FSO	Free Space Optics
FSTF	Financial Services Task Force
FTS	Federal Telecommunications System (Section IV)
FTS	Federal Technology Service (Section V)
FTS2001	Federal Telecommunications System 2001
FTSC	Federal Telecommunications Standards Committee
FRB	Federal Reserve Board
FWUF	Federal Wireless Users Forum
FY	Fiscal Year

G

Gbps	Gigabit per second
GETS	Government Emergency Telecommunications Service
GEWIS	Global Early Warning Information System
GMF	Government Master File
GN	Ground Network
GNSOC	Global Network and Security Operations Center
GOTS	Government Off-The-Shelf
GPRA	Government Performance and Results Act
GSA	General Services Administration
GSM	Global System for Mobile Communications

H

HAIPIS	High Assurance Internet Protocol Interoperability Standard
HF	High Frequency
HPC	High Probability of Completion
HQ	Headquarters
HS	Hanford Site
HSPC	Homeland Security Policy Council

I

I&C	Information and Communications
IA	Information Assurance
IAIP	Information Analysis and Infrastructure Protection
IAM	Initial Address Message
IC	Integration Contractor
ICZ	Interagency Collaboration Zone
IDIQ	Indefinite Delivery, Indefinite Quantity
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IG	Inspector General
IMA	Individual Mobilization Augmentee
IMAP	Integrated Mapping and Analysis Program
IMF	Internet Monitoring Framework
INEEL	Idaho National Engineering and Environmental Laboratory
INS	Immigration and Naturalization Service
IOC	Initial Operating Capability
IP	Internet Protocol
IR	Industry Requirements
IRAC	Interdepartment Radio Advisory Committee
ISAC	Information Sharing and Analysis Center
ISATF	Internet Security/Architecture Task Force

ISP	Internet Service Provider
ISPG	Information Security Policy Group
IT	Information Technology
ITU-T	International Telecommunication Union, Telecommunications Sector
IWG	Interoperability Working Group
I-WPS	Immediate Wireless Priority Service
IXC	Interexchange Carrier

J

JCS	Joint Chiefs of Staff
JS	Joint Staff

K

Kbps	Kilobit per second

L

LAN	Local Area Network
LEC	Local Exchange Carrier
LECMap	Local Exchange Mapping
LMR	Land Mobile Radio
LRTF	Legislative and Regulatory Task Force

M

MAA	Metropolitan Area Acquisition
MAN	Metropolitan Area Network
MCEB	Military Communications-Electronics Board

N

NAP	Network Access Points
NASA	National Aeronautics and Space Administration
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NDAC	Network Design and Analysis Capability
NGN	Next Generation Networks
NIIF	Network Interconnection Interoperability Forum
NIMS	National Incident Management System
NIPC	National Infrastructure Protection Center
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NMCS	National Military Command System
NNSA	National Nuclear Security Administration
NOC	Network Operations Center
NOTF	NSTAC Outreach Task Force
NATO	North Atlantic Treaty Organization
NRC	Nuclear Regulatory Commission
NRIC	Network Reliability and Interoperability Council

NRP	National Response Plan
NSA	National Security Agency
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSIRC	National Security Incident Response Center
NSIE	Network Security Information Exchanges
NSOC	Network Security Operations Center
NSTAC	President's National Security Telecommunications Advisory Committee
NTA	National Telecommunications Alliance
NTIA	National Telecommunications and Information Administration
NTS	Nevada Test Site
NV	Nevada Operations Office

O

OA	Operational Analysis
OAM&P	Operations, Administration, Maintenance, & Provisioning
OASPHEP	Office of the Assistant Secretary for Public Health Emergency Preparedness
OC	Oversight Committee
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
OCS	Office of Cyberspace Security
OEP	Office of Emergency Preparedness
OER	Office of Emergency Response
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSIS	Open Source Information System
OSM	Office of Spectrum Management
OSSS	One-Stop Shop Services
OSTP	Office of Science and Technology Policy
OTAR	Over-the-Air-Rekeying
OTS	Office of Thrift Supervision

P

PAS	Priority Access Service
PBX	Private Branch Exchanges
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
PN	Public Network

POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
Project L3417	Narrowband Radio Upgrade Project
PSAP	Public Safety Answering Points
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PSWN	Public Safety Wireless Network
PT&E	Planning, Training, and Exercise
PTS	Priority Telecommunications System
PVC	Permanent Virtual Circuits

R

R&D	Research and Development
R&O	Report and Order
RCCS	Remote Control-Control Stations
RDTF	Research and Development Task Force
RECP	Regional Emergency Communications Planners
RFI	Radio Frequency Interference
RISC	Regional Interagency Steering Committee
RL	Richland Operations Office

S

SAFECOM	Wireless Public Safety Interoperable Communications Program
SATCOM	Satellite Communications
S-BGP	Secure Border Gateway Protocol
SCC	Secretary's Command Center
SHARES	Shared Resources
SHARES-HF	Shared Resources High Frequency Radio Program
SIPRNET	Secure Internet Protocol Router Network
SON	Synchronous Optical Network
SRS	Savannah River Site
SRSOC	Savannah River Site Operations Center
SRWG	Security Requirements Working Group
SS7	Signaling System 7
SSA	Social Security Administration
SSU	Standing Subcommittee on Upgrades
STE	Secure Terminal Equipment System
STU III	Secure Telephone Units, Third Generation
SWIFT	Society for Worldwide Interbank Financial Telecommunications

T

TAL	Technology Assessment Laboratory
TCS	Treasury Communications System
TCSIRC	TREAS' Computer Security Incident Response Center
TEDE	Telecommunications Electromagnetic Disruptive Effects
Telecom-ISAC	Telecommunications-Information Sharing and Analysis Center
TIA	Telecommunications Industry Association
TIGTA	Treasury Inspector General for Tax Administration
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks
TMP	Telecommunications Modernization Project
TOPOFF2	Top Officials 2
TREAS	U.S. Department of the Treasury
TS	Telecommunications Services
TSP	Telecommunications Service Priority
TSS	Telecommunications Services Staff

U

UK	United Kingdom
USDA	U.S. Department of Agriculture
USARC	U.S. Army Reserve Command
USPS	U.S. Postal Service

V

VA	Department of Veterans Affairs
VANTS	VA Nationwide Teleconferencing System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference
VTF	Vulnerabilities Task Force

W

WAO	Watch and Analysis Operation
WAN	Wide Area Network
WDA	Watch Daily Analysis
WERT	Wireless Emergency Response Team
WPS	Wireless Priority Service
WTF	Wireless Task Force


NATIONAL COMMUNICATIONS SYSTEM
NCS