2004 National Communications System Annual Report

Ensuring Essential Communications for the Homeland

Prepared by the Office of the Manager,
National Communications System

FOREWORD

For over 40 years the National Communications System (NCS) has served the Nation by providing for steadfast national security and emergency preparedness (NS/EP) communications. During this time, the NCS evolved and adjusted to a constantly changing telecommunications and national security landscape, keeping true to its mission to provide essential communications for the Federal Government under all conditions and to coordinate Federal planning for NS/EP communications.

Over the past year, the NCS leveraged its long established telecommunications policy expertise to assist the Department of Homeland Security (DHS) in meeting its mission to build the capacity to prevent a terrorist attack, to reduce the Nation's vulnerability to attack, and to enhance the capacity to respond to an attack. In December, President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which established a national policy for Federal departments and agencies to identify and prioritize the country's critical infrastructures and key resources and to protect them from terrorist attacks. The NCS has played a central role in the Government's efforts to implement HSPD-7, drafting the National Infrastructure Protection Plan's (NIPP) Telecommunications Sector Specific Plan and providing strategic advice based on telecommunications best practices to the DHS Office of Infrastructure Protection.

In addition, as a member of the Committee on Foreign Investments in the United States, DHS relied extensively on the NCS' authoritative knowledge on security issues related to foreign acquisitions and mergers in the communications realm to establish its formal position on foreign ownership related communications cases brought before the Committee. Also, the NCS assumed the lead on revising Emergency Support Function #2, which ensures the provision of Federal telecommunications support to Federal, State, and local response efforts following a presidentially declared major disaster, emergency, or extraordinary situation under the National Response Plan (NRP).

The NCS continued to grow and foster its relationship with industry and other Government entities through work on a variety of critical telecommunications issues. The NCS Committee of Principals (COP) extensively investigated the routing of telecommunications services to critical Government facilities to ensure the reliability of the Federal Government's access to the telecommunications network via redundant and diverse network architectures. The COP also examined the need to establish a Federal Government wide continuity communications enterprise architecture to support the performance of Federal Executive Branch minimum essential functions and continued its review of priority telecommunications service programs.

The President's National Security Telecommunications Advisory Committee (NSTAC) considered a number of important NS/EP related issues including enhancing the security of the commercial satellite infrastructure, trusted access to key telecommunications facilities, the adoption of a baseline security standard for the management plane, and existing barriers to

information sharing under the Critical Infrastructure Information Act of 2002.

Furthermore, the NCS placed significant emphasis on maturing its technology based programs a key asset in the Department's efforts to meet its mission to protect the homeland. The NCS considerably enhanced its Wireless Priority Service (WPS), announcing extended coverage for users in the western and northeastern regions of the United States. The NCS also continued to implement Government Emergency Telecommunications Service (GETS) features throughout the public switched telephone network, and maintained its commitment to work with the telecommunications industry to ensure NS/EP priority communications services will be available as networks evolve to packet-based technologies.

To enhance user access to both WPS and GETS, as well as the Telecommunications Service Priority (TSP) program and the Shared Resources (SHARES) High Frequency Radio programs, the NCS implemented the NS/EP Priority Communications One-Stop Shop Service, which allows customers to acquire information on NCS priority communications services, programs, and operations from a single source. The organization continues to embrace the use of new technologies to support emergency communications including the use of free space optics, wireless broadband, and Worldwide Interoperability for Microwave Access as back-up dial tone possibilities.

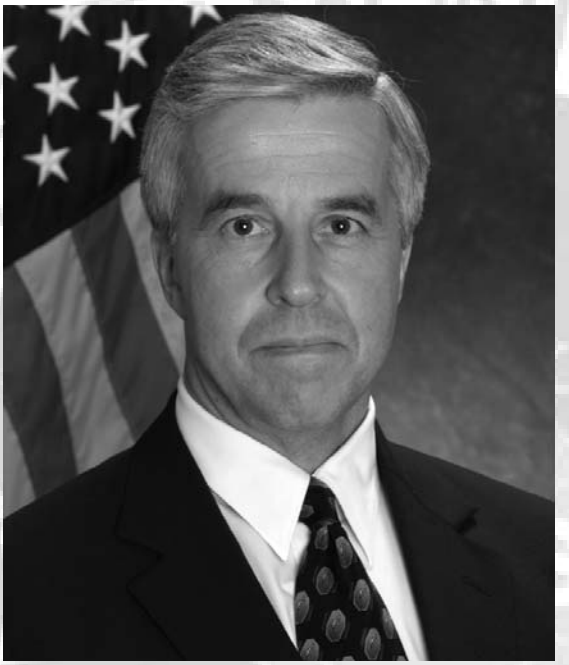
The NCS conducted a Commercial Satellite Feasibility Study to explore the viability of using satellites for NS/EP telecommunications and participated in a unique cross sector infrastructure analysis exercise with the Financial Services sector to assess systemic infrastructure issues in an area of high concentration of critical financial services functions. Finally, the NCS deployed its Individual Mobilization Augmentee's to disaster field offices in partnership with State and local Government personnel and emergency responders during Hurricanes Charley, Ivan, and Frances.

Over the past four decades, the NCS mission has been to coordinate emergency communications for the protection of our country and citizens, and as a result, the Nation has been better able to anticipate, prepare for, and respond to emergency incidents. As the Manager of the NCS, I am proud to see the NCS adapt quickly to its new environment, welcoming the opportunity to lend its expertise beyond NS/EP communications to include critical homeland security and critical infrastructure protection concerns. I applaud the NCS for its depth and breadth of work in this critical area, and I look forward to continuing to work in partnership with industry and other Government entities to ensure our Nation's telecommunications infrastructure remains robust and resilient so that decision makers and emergency workers are able to communicate during times of crisis and emergency situations.

Robert P. Liscouski
Manager


NATIONAL COMMUNICATIONS SYSTEM
NCS

NCS Leadership

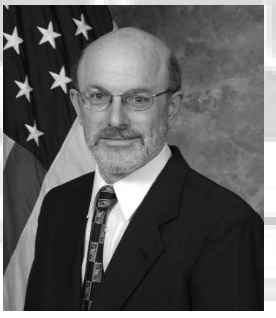


Mr. Robert P. Liscouski
Manager

Dr. Peter M. Fonash
Deputy Manager

Col. Sheron Bellizan
Chief of Staff USAF

Mr. John Graves
Acting Chief
Technology and
Programs Division



Mr. Jeffrey Glick
Chief
Critical Infrastructure
Protection Division

Mr. James Bittner
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. Harry Hixon

Department of Defense (DOD)
Dr. Linton Wells

Department of Justice (DOJ)
Ms. Karen Beard

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

Department of Agriculture (USDA)
Ms. Janice Lilja

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

Department of Health and Human Services (HHS)
Mr. Robert Blitzer

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

Department of Energy (DOE)
Mr. Gordon Errington

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

Department of Homeland Security (DHS)
Mr. Steven Cooper

Federal Emergency Management Agency (FEMA)
Mr. Barry West

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)
Col. Randall Conway, USA

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

Department of the Interior (DOI)
Mr. Timothy Quinn

Department of Agriculture (USDA)
Mr. Roy Allums

Department of Commerce (DOC)
Mr. Benjamin Chisolm

Department of Health and Human Services (DHHS)
Mr. Robert Lavender

Department of Transportation (DOT)
Ms. Hollace Twining

Department of Energy (DOE)
Mr. Gordon Errington

Department of Veterans Affairs (VA)
Mr. David Cheplick

Department of Homeland Security (DHS)
Mr. Julio Murphy

Federal Emergency Management Agency (FEMA)
Mr. Barry West

The Joint Staff (JS)
Col Robert Gearhart, USMC

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

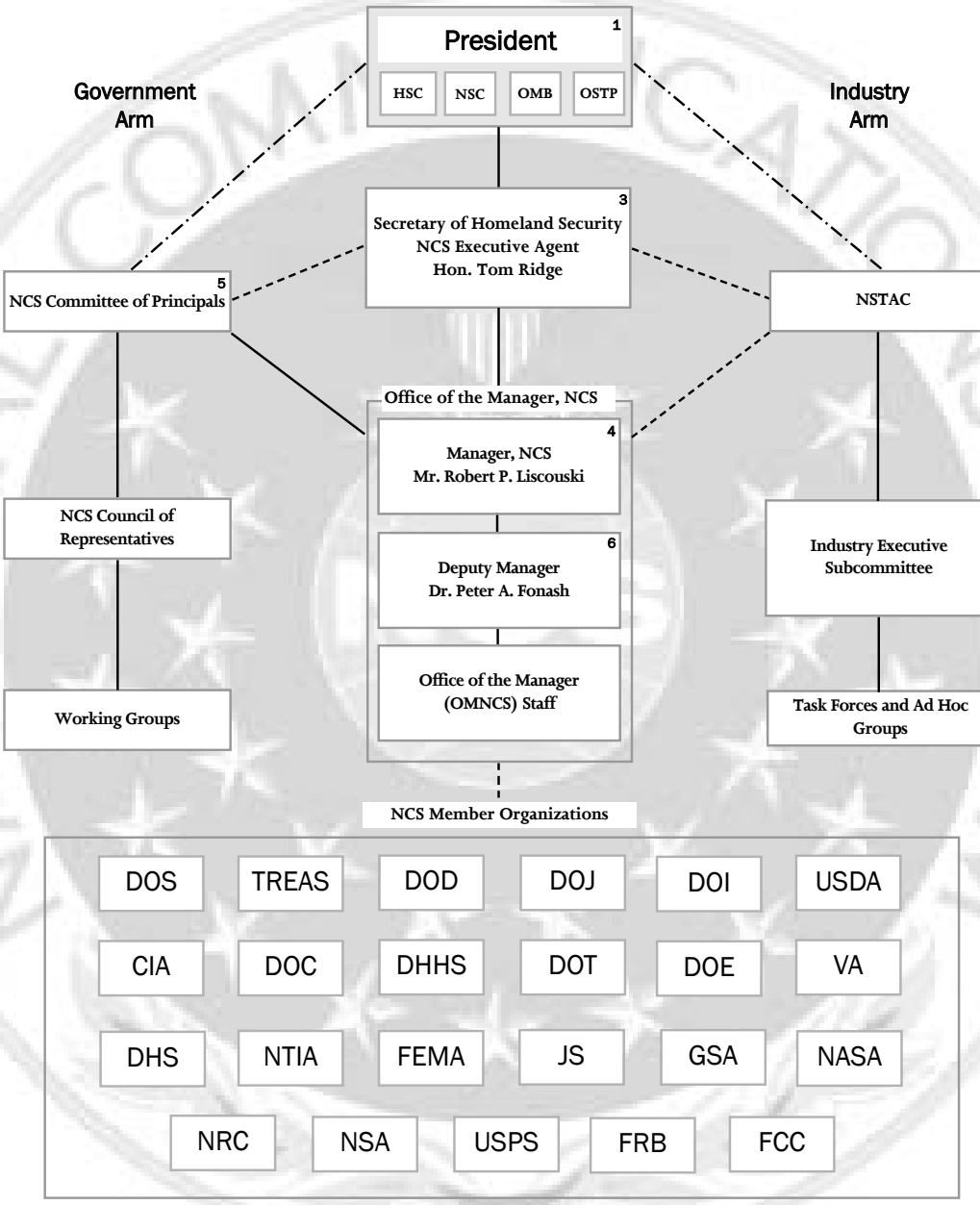
National Security Agency (NSA)
Ms. Carol Higgins

United States Postal Service (USPS)
Mr. Warren Schwartz

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

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

BACKGROUND

This document, prepared by the Office of the Manager, National Communications System (OMNCS), reports on national security and emergency preparedness (NS/EP) telecommunications activities and events, and highlights the agency's innovations, programs, and achievements during fiscal year 2004 (FY 04).

President John F. Kennedy established the National Communications System (NCS) by authority of Presidential memo, on August 21, 1963, as a result of communications shortfalls discovered during the 1962 Cuban Missile Crisis. During the crisis, the Federal Government experienced difficulty establishing and maintaining communications between the United States, the Union of the Soviet Socialist Republics, the North Atlantic Treaty Organization, and other foreign heads of state, which proved to be a hindrance to the swift and peaceful resolution of the conflict. Following the crisis, President Kennedy mandated that the National Security Council (NSC) conduct an investigation regarding national security communications. Following the investigation, the NSC established an interdepartmental committee to evaluate critical communications networks and recommend improvements as needed.

To best serve the needs of the President, the Department of Defense (DOD), 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 times of crisis. From these activities, the NCS was born. The original mission of the NCS was to "provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack." Today, the NCS continues to address NS/EP communications challenges, however many of the challenges have evolved due to changes in technology, the marketplace, and national security threats.

Over the years, the role of communications in supporting the Nation's NS/EP functions has expanded. By the 1970s, Government policy formally recognized that the communications infrastructure was an essential component of deterrence and recovery in the face of an attack. NS/EP communications remained at the forefront of Presidential concern in the Nation's defense, when 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. Today, the E.O. directs the NCS to advise the President, the NSC, the Homeland Security Council, the Director, Office of Science and Technology Policy, and the Director, Office of Management and Budget on these matters.

The role of the NCS in national and homeland security efforts was further defined when, as a response to the September 11, 2001, attacks on the World Trade Center in New York City and the Pentagon in Washington, D.C., 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.

A year later, on November 25, 2002, President Bush 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. On February 28, 2003, the President signed omnibus E.O. 13286, *Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, which transferred the NCS executive agent from the DOD to DHS. The following day, on March 1, 2003, the NCS officially became a part of DHS.

NCS ENVIRONMENT: THE EVOLVING HOMELAND SECURITY LANDSCAPE

As the homeland security policy and technology landscape dynamically evolves, so too does the NCS mission to ensure NS/EP communications to an ever broadening array of domestic and international partners. The addition of critical infrastructure protection (CIP) responsibilities to its traditional NS/EP communications focus makes the NCS a crucial component in the Department's efforts to thwart threats against the Nation's critical assets and to ensure continued national and economic security and public health and safety.

The introduction of two important policies during FY04 continued to shape the Government's response to its homeland security objectives. On December 17, 2003, President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, which established a national policy for Federal departments and agencies to

identify and prioritize U.S. critical infrastructures and key resources (CI/KR) and to protect them from terrorist attacks, with an emphasis on defending against catastrophic public health consequences and mass casualties. To assist in the implementation of HSPD-7, the NCS supported the production of the National Infrastructure Protection Plan (NIPP), providing lessons learned and best practices from the telecommunications sector perspective. The NIPP establishes a roadmap and delineates roles and responsibilities for identifying and prioritizing CI/KR, assessing vulnerabilities, and determining the protective actions that need to be taken within and across CI/KR. In addition, as the Sector Specific Agency for Telecommunications, the NCS worked in consultation with the private sector and the NCS Committee of Principals (COP) to draft the Telecommunications Sector-Specific Plan a further implementation requirement of the NIPP.

The President also issued HSPD-8, *National Preparedness*, on December 17, 2003, to establish policies that strengthen the preparedness of the United States in order to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. HSPD-8 requires a national domestic all-hazards preparedness goal**,** establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlined actions to strengthen preparedness capabilities of Federal, State, and local entities. This directive provides further critical context on the homeland security environment for the industry and Government members of the NCS National Coordinating Center (NCC).

Within this evolving legislative landscape, and as a result of the Government's increasing emphasis on protecting the Nation's vital resources and infrastructures, the NCS focused its attention on several areas of key interest in meeting the Department's CIP goals. In response to lessons learned both from the September 11, 2001, terrorist attacks and the devastating hurricane season along the southeastern coast of the United States, the NCS invested significant resources to work in concert with the financial services sector to better understand the interdependencies between the two sectors' infrastructures, which are indelibly linked for the conduct of day-to-day operations. Specifically, a group of financial services and telecommunications companies conducted the Joint Telecommunications/Financial Services Sectors Pilot Recoverability Assessment Information Exchange, to assess systemic infrastructure issues in an area of high concentration of critical financial services functions. Officials from the NCS, NCC, and BITS, a nonprofit consortium of the Nation's largest financial services companies, developed and facilitated these discussions. In addition, the President's National Security Telecommunications Advisory Committee (NSTAC) is addressing these interdependencies through its Financial Services Task Force.

Another key focus area for the NCS is the creation of a Federal Enterprise Architecture for continuity communications (CC) across the Federal Executive Branch of the United States Government. Under the guidance of the White House's Continuity of Operations Communications Plan—and through the authority of E.O. 12472—the NCS established the Continuity Communications Working Group (CCWG) to begin the creation of the CC enterprise architecture (CC EA). The CC EA will allow for the documentation and

standardization of communications capabilities across the Federal Executive Branch, ensuring that, during times of crisis, key Departments and Agencies will be able to communicate properly and fulfill their Mission Essential Functions. The CCWG is a subordinate group to the NCS COP and therefore is comprised of representatives from the COP member agencies. The CCWG will continue its efforts through FY04 and into FY05.

The NCS also addressed vulnerability concerns regarding commercial satellite communication (SATCOM) systems. SATCOM services are typically used during hurricane response, national security events, and military operations, and were leveraged extensively in response to the September 11, 2001, attacks. The NCS examined this key issue through the *Commercial Satellite Feasibility Study*, which examined the state of the industry and studied how satellite systems can be employed to ensure robust and reliable communications. The NSTAC also established a Satellite Task Force to review and assess policies, practices, and procedures for the applications of infrastructure protection measures to commercial SATCOM networks used for NS/EP communications.

The NCS continues to examine key technological solutions to NS/EP communications requirements. In the aftermath of the September 11, 2001, attacks, reports indicated that communication assets near the impacted areas were either congested or incapacitated, causing users to experience intermittent or a total lack of voice service. The reports generated concerns that key Federal departments and agencies in Washington, DC, might be at risk for losing critical wire line communications services if the supporting infrastructure were damaged or destroyed. The NCS, tasked by NSC, addressed this concern by establishing the Backup Dial-Tone (BDT) project to evaluate the need for a BDT capability for Federal departments and agencies in the Washington, DC area, and to determine whether such a capability would have been helpful in the New York City and Washington, DC area on September 11, 2001. During FY04 the NCS compiled and revised a list of technical solutions to address these vulnerabilities, relying on interviews with Government agencies to supply real-world data.

Fostering relationships with domestic and international stakeholders in order to better meet the NS/EP needs of the President and the Federal Government at large remains an essential element of the NCS' mission. The NCS has developed a close partnership with the National Cyber Security Division with which it coordinates the conduct and operation of cyber-based programs and activities to meet their respective NS/EP goals. In addition, the NCS has grown its relationship with both the Mexican and Canadian Governments with whom it exchanges information regarding best-practices for ensuring that critical infrastructures are protected across North America. Specifically, the NCS has attended bilateral meetings to discuss emergency calling services as well as emergency telecommunications planning agreements.

While the changing environment presents a new set of challenges, the NCS remains committed to evolving to meet the changing policy, technology, and threat landscape, demonstrating that it will 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 Communications System (NCS), through its Critical Infrastructure Protection Division, plays a vital role in ensuring that Federal, State, and local responders receive national security and emergency preparedness (NS/EP) communications assistance during and after man made and natural disasters. Specifically, the National Coordinating Center (NCC) assists in the initiation of national coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities under all circumstances. The NCS, on behalf of the Federal Emergency Management Agency (FEMA), was also designated the primary agency for implementing and coordinating the Federal Response Plan's Emergency Support Function #2 (ESF #2), which ensures the provision of Federal telecommunications support to Federal, State, and local response efforts following a presidentially declared major disaster, emergency, or extraordinary situation. The NCS also provides valuable analyses which examine the impacts of certain events on the telecommunications infrastructure, allowing for improved preparation in anticipation of an attack or disaster.

Furthermore, the NCS established the Individual Mobilization Augmentee (IMA) Program in 1988 to fulfill responsibilities assigned under Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. The IMA Program is staffed by civilian and military reservists, who work to enhance the efforts of the Office of the Manager, National Communications System (OMNCS), the NCC, and NCS Regional Managers during significant events such as floods, wildfires, hurricanes, ice storms, earthquakes, and other emergency events. The NCS IMA personnel supplement the assigned NCS staff support to national and regional crises and emergencies.

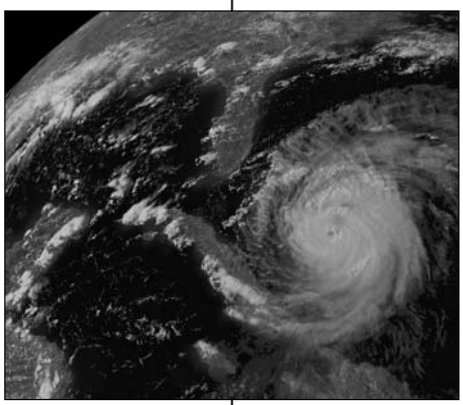
During Fiscal Year 2004 (FY04), the NCS leveraged its extensive emergency response expertise and its mature priority services programs to provide support to response efforts related to the devastating hurricane season that battered the southern portion of the United States and threats levied against the Nation's critical financial institutions.

HURRICANE RESPONSE

During the fall of 2004, three devastating hurricanes struck the coast of Florida in swift succession causing billions of dollars worth of damage to local infrastructures and significant loss of life. Charley, a Category 4 hurricane, struck the west coast of Florida on August 13, 2004; Hurricane Frances struck the east coast of Florida on September 3, 2004; and Hurricane Ivan made landfall on the Gulf Coast on

September 16, 2004. Presidential declarations were issued after each hurricane, pronouncing parts of Florida a Federal disaster area.

In support to the Federal Government's hurricane response activities, the NCS deployed its IMAs to disaster field offices in affected areas in Florida to assist FEMA responders. In addition, the NCS administered the use of its priority services programs. Between August 13, 2004, and August 15, 2004, 610 Government Emergency Telecommunications Service (GETS) calls were placed following Hurricane Charley. Furthermore, following Hurricane Frances, 1,033 GETS calls were made, while 922 GETS calls were made following Hurricane Ivan. The primary organizations originating GETS calls were the OMNCS, the Department of Defense (DOD), the Department of Treasury (TREAS), the Department of Homeland Security (DHS), and the Florida State Government. In the aftermath of Hurricane Charley, the NCS noted an increase in GETS card requests by Federal and State responders, which continued during the preparation for Hurricanes Frances and Ivan as well. Following the three hurricanes, an additional 3,259 GETS cards were requested by various different entities.



The Wireless Priority Service (WPS) also proved a great success during response efforts for Hurricane Charley. T-Mobile reported the completion of 13 WPS calls via the Orlando, Florida, Mobile Switching Center (MSC), while Nextel reported 111 successful WPS calls between the period of August 13 to August 14, 2004, a 96 percent success rate. Anticipating the likelihood of network outages, Nextel accelerated access to WPS in certain portions of Florida prior to the arrival of the hurricane. Indeed, general wireless services were affected by the storm, with many carriers reporting the loss of a number of cell sites including the loss of T-1 line connections from cell sites to MSCs, even after power to the cell sites was restored. Recognizing the value of the WPS capability, the Florida Division of Emergency Management requested 39 additional WPS phones from Nextel on August 18, 2004. In response, the Nextel Emergency Response Team (ERT) loaned 2,300 handsets with WPS Priority 5 to state emergency personnel during Hurricane Charley and 1,632 headsets of varying priorities during Hurricane Frances. While there were no reports received from Nextel or T-Mobile on the number of WPS calls during Hurricane Frances or Ivan, all MSCs remained operational.

In addition, the NCS responded to numerous Telecommunications Service Priority (TSP) requests from FEMA during this same period. As a result of the three hurricanes, 69 TSP provisioning requests were made from Government agencies and private sector entities.

THREATS TO FINANCIAL INSTITUTIONS

In August 2004, Secretary of Homeland Security Thomas Ridge raised the terrorism threat level from yellow to orange for financial institutions in New York, New Jersey, and Washington, D.C. in response to threats against specific financial targets in those areas. The targets included Citigroup buildings, the New York Stock Exchange, Prudential Financial, as well as the International Monetary Fund, and the World Bank.

In response to these threats and in an effort to reduce the response time for telecommunications impact analysis requests during this incident, which examined impacts to banking and finance users based on collateral loss of telecommunications, the NCS implemented a streamlined analysis process to provide quick support to DHS. In addition, the NCS streamlined, standardized, enhanced, and documented its processes for producing its analysis products to improve the response time for future analysis requests. Standardized report formats were developed and specific data sets and methodologies were identified for each type of analysis. This effort enhanced the capability of the NCS to provide consistent and timely analysis results—in as little as 30 minutes—during crises, disasters, and other national security events. This new procedure was also implemented to support the National Republican Convention, which was held in August 2004, in New York City.

III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

SECTION III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS) and the national security and emergency preparedness (NS/EP) community during fiscal year (FY) 2004.

NCS Leadership Changes

July 2004 was a major transition month for the National Communications System (NCS) leadership. Dr. Peter M. Fonash, Chief of the NCS Technology and Programs Division, became the Acting NCS Director, replacing Mr. Brenton C. Greene. Mr. Greene, who led the day-to-day operations as the NCS Deputy Manager since April 2001, resigned in July 2004 and returned to the private sector as Vice President, Government Relations with Lucent Technologies. Mr. John Graves, the NCS Program Director for the Government Emergency Telecommunications Service (GETS), became the Acting Chief of Technology and Programs.

Also in July 2004, Air Force Colonel Sheron Bellizan assumed duties as the NCS Chief of Staff, replacing Navy Captain J. Katherine Burton, who served as the NCS Assistant Deputy Manager from September 2001 until her retirement in June 2004. Mr. James G. Bittner became the Chief, NCS Plans and Resources Division, formally replacing Larry Wheeler—now with the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection (IAIP) Directorate. Finally, Mr. Jeffrey Glick assumed duties as Chief, NCS Critical Infrastructure Protection Division, replacing Mr. Frederick W. Herr, who retired from the Federal Government.

TECHNOLOGY AND PROGRAMS DIVISION

The Technology and Programs Division implements evolutionary NS/EP telecommunications capabilities to enable a reliable and effective infrastructure. The division develops programs, technical studies, modeling capabilities and analyses, and standards that promote the reliability, security, interoperability, and priority treatment of NS/EP telecommunications.

Division objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs and evaluating emerging technologies to alleviate impediments to interoperability. This information is brought to 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 FY 2004.

Government Emergency Telecommunications Service

Background

The OMNCS established 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 receive a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters. GETS reached full operational capability on September 30, 2001.

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient, 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. This 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 WorldCom, 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) Network and Telecommunications Integrated Solutions Division (formerly GTE Government Systems Division) 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 technology provided the basis for the first phase of GETS LEC feature deployment, which was 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. By full operational capability, 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 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.

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.

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. In case the access control system is inoperative, a fail open feature will allow users to complete their GETS calls. The utility of this feature was demonstrated during the September 11, 2001, attacks on America.

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

In 1996, ANSI modified the SS7 standards so that NS/EP traffic would have a higher signaling priority level than regular or non-priority telephone traffic. The GETS PMO worked closely with the Network Interconnection Interoperability Forum (NIIF) to facilitate industry migration to the standard related to SS7 message priority. GETS representatives worked with the GETS IXCs and LECs as well as the switch vendors to reach consensus on a migration plan and schedule. Their work resulted in the adoption of the Initial Address Message (IAM) Implementation Plan, which was brought to the NIIF.

In December 1997, NIIF accepted Issue No. 0095, Implementing Plain Old Telephone Service IAM Priority Level 0. Based on the resolution, all participants submitted plans, providing specific dates indicating when they would comply with the standard. Switches that comply with the standard serve more than 90 percent of the access lines in the nation.

Interoperability

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

Like other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the Telecommunications Act of 1996. In some areas, this environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin telephones and PBXs. Previous testing shows these problems to be particularly prevalent for coin telephones owned and operated by small businesses and PBXs operated by the hospitality industry (such as 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.

Currently, 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 of September 11, 2001. Despite the heavy telephone congestion occurring immediately following the attacks and during the first week afterward, 95 percent of the 4,000 GETS calls to and from Manhattan were successfully processed. During the same period, another 3,000 GETS calls were made in Arlington, Virginia, area with similar success rates. From the date of the attack until September 28, over 1,000 GETS cards were issued to qualified emergency personnel. During that 17-day span more than 1,500 people made GETS calls.

In the past year, the GETS program has continued to make significant progress in its outreach efforts to all levels of Government (Federal, state, and local) and other qualified NS/EP industrial and nonprofit organizations. As of July 2004, there were 89,941 active GETS cards—an increase of 11,076 cards during the past year—categorized as follows: Federal: 60,908; State: 8,402; local: 10,222; industry: 9,065; and other NS/EP organizations: 1,334.

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.

In response to an October 1995 petition from the NCS, the 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 made PAS voluntary, found it to be in the public interest, and defined five priority levels for NS/EP calls.

The days following the tragic events of 9/11 saw widespread wireless network congestion. 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 Oct 5, 2001, Meeting on Selected NS/EP Telecommunications Projects, Oct 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, D.C., 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 one year

In response to this guidance, OMNCS initiated the following solutions:

- Immediate—a solution using a single carrier with commercially available and readily deployed technology in Washington, D.C., New York City 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, helping to return the Government as well as 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 United States, 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 2004, there were over 9,000 WPS users. It is the objective of OMNCS to provide the WPS capability to an estimated NS/EP 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, D.C., New York City, and Salt Lake City (site for the 2002 Winter Olympics) had cellular telephony 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, D.C., and New York City.

T-Mobile 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 because I-WPS did not conform to the Federal Communications Commission (FCC) Report and Order (FCC-00-242, 13 July 2000) requirement to invoke the priority service on a call-by-call basis. T-Mobile 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, D.C. 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 FOC. Subscriptions and usage costs for continued use of this service have been transitioned from the OMNCS directly to the user agency.

Nationwide WPS

Due to the requirement for nationwide WPS coverage, multiple carriers and multiple access technologies are needed. Nationwide WPS, a more comprehensive wireless priority capability, will be available in the two dominant access technologies deployed by U.S. carriers, GSM (i.e., T-Mobile, Cingular Wireless, AT&T Wireless, and Nextel) and CDMA (i.e., Verizon Wireless and Sprint PCS). Nationwide WPS is provided in two major phases, initial operating capability (IOC) and FOC. IOC is a GSM-based solution only, consisting of priority radio channel access at call origination. IOC began December 31, 2002, and it satisfied the requirements of the FCC Second R&O for invocation of the service on a call-by-call basis by dialing the WPS prefix (#272) at the start of each NS/EP call. FOC provides a full, end-to-end capability, beginning with the NS/EP wireless caller, through the wireless networks, through the IXC and/or LEC wireline networks, and to the wireless or wireline called party. T-Mobile began deploying WPS FOC in December 2003. Cingular. AT&T Wireless, and Nextel began deploying WPS FOC in July 2004.

Nationwide Industry Requirements

Nationwide WPS is made possible by strong industry partnerships with Government during the development of Industry Requirements (IR). 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 four months after direction was received from the NSC. The FOC requirements for both GSM and CDMA are also completed. These documents are used as a basis to issue Requests for Proposals (RFP) for the Nationwide WPS. The final revisions to the CDMA home location register (HLR) IR documents were completed in June 2004. Verizon Wireless and Sprint PCS are expected to begin offering WPS in 2006.

The NCS has taken steps to ensure that the IR documents provide a method for use of the nation's cellular telecommunication networks by NS/EP personnel that does not hinder public use during emergency events. As a result, the IR documents stipulate that 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 NS/EP leadership and key personnel who require reliable communications services in times of disaster or emergency, WPS and GETS are powerful emergency communications assets and important national resources.

National Security and Emergency Preparedness Standards

Standards Development

Presidential Executive Order (E.O.) 12472 of April 1984 calls for NCS consideration of evolving international and national standards with respect to NS/EP telecommunications. In addition, Office of Management and Budget Circular A-119, presents rationale for Government to: (1) participate in; and (2) adapt for Government acquisitions, the work and products of voluntary (commercial/industry) standards committees.

Traditional NS/EP telecommunications services have been designed around the circuit-switched infrastructure of the Public Switched Telephone Network (PSTN). However, evolving converged and public next generation networks (NGN) are emerging with packet-switched design infrastructures. As this evolution continues to mature, priority telecommunications services will be guided and implemented by commercial standards that stem from emerging technologies based on packet-switched infrastructures, such as the Internet and Internet Protocol (IP) based Cablecom networks.

In concert with this evolution, third generation and beyond wireless public networks are becoming increasingly more vital to the NS/EP community. Therefore, work is ongoing with a number of national and international telecommunications industry standards organizations to ensure that evolving commercial standards address requirements of the NS/EP community of users.

Ongoing standards development initiatives for NS/EP users encompass prime functionalities of: signaling, access, management, transport, interoperability, mobility, and associated architectures.

Because Internet and wireless communications have become increasing vital

to national security during NS/EP events, the current focus is on these two telecommunications media. Proactive efforts with industry in standards development organizations include:

- Telecommunications Committee (T1)
- Telecommunications Industry Association (TIA)
- International Telecommunication Union, Telecommunications Sector (ITU-T)
- Internet Engineering Task Force (IETF)
- TeleManagement Forum
- Third Generation Partnership Project (3GPP)
- Third Generation Partnership Project 2 (3GPP2)

Department of State Support

Direct support is provided to the U.S. State Department by Chairing the International Telecommunications Advisory Committee Study Group 'B' along with serving as senior Government advisors and leaders (such as, head of delegations) to a variety of international and national meetings on telecommunications.

Technical Analyses and Studies

Technical approaches employed for development of priority services in the above organizations include:

- Conducting studies, performing analyses, sponsoring industry/academia research and development of new technologies for potential NS/EP applications
- Firmly establishing NS/EP technical requirements in work programs, in cooperation with industry and academia
- Developing and providing detailed technical proposals (i.e., NS/EP contributions) within industry standards programs, encouraging industry participants in these programs to make technical proposals to augment NCS proposals
- Integrating NS/EP technical service agreements into operational systems as an inherent part of the underlying packet-based infrastructure rather than a retrofitted fix in deployed systems, investigating new features emerging in packet-based networks to enhance NS/EP operations such as E-mail, instant messaging, multicast video, web access, tunneling, mobility, and more
- Performing and promoting independent testing and implementations of proposed technical solutions
- Participating in the development of contemporary telecommunications industry acquisition tools, such as service level agreements (SLAs) and associated application notes, to better specify criteria for availability, reliability and quality performance of delivered NS/EP telecommunications services

Federal Wireless Users' Forum

Background
The Federal Wireless Users' Forum (FWUF) is an association of individual Federal Government wireless users. In 1992, the OMNCS established the FWUF as a mechanism for interaction and exchange of information among wireless communications service vendors and users to establish industry-wide standards for emerging wireless digital technologies. The objectives of the FWUF are:

- Educating Government users about wireless telecommunications
- Identifying the telecommunication needs of Government users
- Facilitating information exchange with other user groups, standards organizations, manufacturers, and service providers to ensure that Government user needs are met
- Supporting the interoperability of emerging wireless services and equipment through increased participation in the formulation of Federal policy, support of standardization efforts, and other appropriate activities

The Forum is co-chaired by the OMNCS and the National Security Agency (NSA) and is directed by a steering committee consisting of members from the Department of Defense (DOD), the Department of Commerce, the Department of Treasury, the National Institute of Standards and Technology (NIST), and the Federal law enforcement community. FWUF holds biannual forums for members to bring together people from the Federal Government and from the wireless telecom industry. Activities of the Forum include:

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

20th FWUF Workshop Highlights
The 20th FWUF Workshop took place from October 21-23, 2003, in Las Vegas, Nevada. On the first day of the workshop, participants discussed the power blackout of August 2003 and its effects on wireless networks. In addition, NIST introduced a test bed that uses a commercial-off-the-shelf (COTS) platform to provide wireless communications for first responders, resulting in a self-configuring ad hoc network architecture that will support voice, data, location, and tracking services, among others. Secured Mobile Environment was also mentioned, stressing that the need for Public Key Infrastructure (PKI) on wireless networks is greater now than ever before and that the DHS First Responder requirements should include:

- Interoperability between multiple agencies
- Effort coordination
- Commercial network use, when available
- Satellite-based or otherwise independent emergency infrastructure

Another highlight of the workshop was GSA Federal Technology Program (FTP) Wireless

Program Office offering a "One Stop Shop" for wireless that covers satellite service, cellular, Land Mobile Radio (LMR), wireless Local Area Networks (LANs), and other technologies. The goals of this office include:

- Integrating communications
- Command and control solutions needed for DOD, DHS, law enforcement and the public safety community
- Enhancing productivity for the mobile worker
- Remote access to office applications
- E-mail and Instant Messaging (IM)

The Workshop was held in conjunction with the Cellular Telecommunications and Internet Association (CTIA) Wireless Information Technology (IT) and Internet 2003 convention. This gave participants an opportunity to gain more exposure among commercial wireless service providers and developers. The Workshop participants benefited from demonstrations of the latest in wireless data services and technologies and the future direction of the wireless industry. Participants were also able to hear keynote addresses given by various wireless industry representatives. One key point addressed during the Workshop was that in the first six months of the year 2003, $700 million of revenue was made in the wireless data business.

21st FWUF Workshop Highlights

The 21st FWUF Workshop took place from April 6-8, 2004, in Seattle, Washington. Security was the main topic of discussion during the workshop, stressing that the events of 9/11 led to the need for data exchange beyond voice over a reliable network. The increased reliance on the Internet and databases has affected business models in all industry and Government sectors. Mobile technologies are extending communications services beyond the edge of the wired infrastructure and significantly increasing the complexity of enterprise networks. The explosive growth of wireless and mobility-enabled devices are having a direct effect on IP, with 80 percent of all organizations forecasted to have access to wireless LAN technology by 2008. In the future, there will be more bandwidth requirements, rapid protocol evolution, potential compatibility issues, a greater awareness among users and enterprises, a greater need for vendors to create secure wireless products, and more involvement from the academic community as general purpose wireless research increases.

The Workshop also provided participants an update of WPS, with GSM being the selected technology over CDMA. WPS has two phases, with Phase 1 being available by the fourth quarter of the year 2005. Phase 1 provides for radio access queuing at the origination side only, with only one priority level for all WPS calls. The queue time is 12 seconds, and calls are on a first-in, first-out basis. Phase 2, which gives end-to-end queuing, has five priority levels, and a queue time of 28 seconds, will be available sometime between late 2006 and early 2007. WPS will begin development for CDMA in 2005.

Modeling, Analysis, and Technology Assessment

As directed by Executive Order 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.

Internet Disruption Impact Analysis
The NCS is investigating whether the Internet could be "taken down," in what scenarios a widespread disruption would be possible, and how to measure the impact of each scenario as it relates to other critical infrastructures (CIs). To answer these questions, the NCS brought together a panel of experts from industry and the research community and asked them to review potential disruption scenarios for their likelihood and impact—and to recommend methods to quantify disruption impact while looking for possible improvements. Although many groups outside of the NCS are evaluating technical and policy issues to address and prevent Internet disruptions; the IDIA effort is complementary to these other efforts by:

- Identifying Internet disruption scenarios
- Quantifying impact of each scenario

The first three CIs to be analyzed were Government, energy, and finance; analysis of the remaining CIs is planned for FY 2005.

Backup Dial Tone/Route Diversity Analyses
The Backup Dial Tone (BDT) study uses the 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, D.C., area.

Next Generation Networks
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. Since 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 in order 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 Providers
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 Internet Service Providers (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.

Internet Protocol (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 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 Telecommunications Infrastructures
An analysis capability is being developed to identify the most critical government locations and the most critical telecommunication provider's locations necessary to ensure government connectivity during a crisis. NCS is coordinating with GSA FTS 2001 personnel to share FTS2001 traffic data, particularly for agencies recently merged with the Department of Homeland Security.

Supervisory Control and Data Acquisition Modeling
A capability is being developed to model the interaction and dependency between telecommunications and Supervisory Control and Data Acquisition (SCADA) systems to enable detailed analyses of SCADA communications vulnerabilities. Combining the modeling and analysis capabilities of the NDAC with the Idaho National Environmental and Engineering Lab (INEEL) SCADA test bed provides the ability to test variants of SCADA equipment, software, protocols, and configurations. This collaboration, using real SCADA systems and their communications interfaces, will enable calibration of the NDAC SCADA communications dependency and vulnerability models—and will enable the development of technology, procedures, and recommended best practices for mitigating SCADA communications vulnerabilities.

Internet Priority Services
Due to the ever-increasing use of the Internet for transmission, the NCS is looking at ways to assure priority NS/EP communications, similar to that provided by WPS and GETS, for data, voice and video applications using IP technology. In November 2003, the NCS issued a Request for Information (RFI) on IP-based assured communications, including Voice over Internet Protocol (VoIP). Responses enabled the NCS to make a broad assessment of IP emerging technologies, developing major findings and recommendations in support of deploying the service. Moreover, RFI responses support the following NCS goals:

- Identify emerging IP technologies
- Undertake prototype and proof of concept projects
- Support standardization efforts
- Formulate modeling and simulation projects
- Specify commercial priority service capabilities

The RFI requested information from contractors and vendors on their current IP technology capabilities and their plans for supporting an Internet Priority Services (IPS). The NCS received 47 responses from industry in the following business categories: 1) GETS carriers; 2) ISPs; 3) equipment and software vendors; 4) research organizations; and 5) consultants/integrators/engineers.

The IPS RFI assessment revealed that there is no overall priority or end-to-end Quality of Service (QoS) architecture in place on the Internet today. Service providers are deploying QoS and priority techniques only within their individual IP networks and only for limited applications and users. Required IP technology research and development activities include:

- Study new features to mitigate congestion and network outages, maintaining NS/EP priority services during significant network overload
- Develop new and updated standards to provide end-to-end priority and QoS
- Study IP technology security issues that address authentication, authorization and accounting (AAA), connection admission control (CAC), and security protection of the users' traffic and network resources

Technology Assessment Labratory
The NCS has established a fully accredited Technology Assessment Laboratory (TAL), which 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 COTS and Government off-the-shelf (GOTS) that may satisfy specific NS/EP requirements, often obviating development contracts
- Host Applications & 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:

- NDAC. 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

- Internet Modeling Framework (IMF). 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. Internet community projects—such as The Honeynet Project—provide an excellent opportunity to increase the respect and recognition of the NCS within research and development circles. It will also enhance our in-house expertise in critical areas. The TAL supports this activity

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

Advanced Technology

The NCS Advanced Technology (AT) Branch ensures new and emerging technologies are available to Government during national emergencies or crises. Over the past year, they researched a range of NS/EP communications topics such as Telecommunications Electromagnetic Disruptive Effects (TEDE); conducted a vulnerability study on Short Message Service (SMS) increased traffic trends; and, as directed by the White House, concluded a SATCOM feasibility study in support of NS/EP communications.

Hybrid Networks

The AT Branch analyzes emerging wireless and wireline communications technologies, vulnerabilities to TEDE, and their implications on NS/EP telecommunications services.

Next Generation Networks

During the past year, the AT Branch analyzed:

- Emerging Open System Interconnection (OSI) Layer 1 technologies and services, in addition to layer 2 where applicable

- Emerging PSTN as it evolves to packet-based technologies, architectures, and services

- Next Generation Optical Internet and Cable technologies—the underlying technology for

telecommunications networks for the foreseeable future

Wireless Networks
Wireless spans a wide range of technologies, including cellular, satellite, wireless LAN, and other technologies. Many of these areas are experiencing rapid growth and technological innovations that are sure to change the burgeoning landscape of wireless communications. The AT Branch made an initial analysis with a focus on future cellular technologies and other advanced wireless technologies supporting voice and data. Moreover, the AT Branch analyzed the different user location technologies that support different mobile communications technologies.

Commercial Satellite Feasibility Study
In July 2002, as directed by the White House, the AT Branch commenced a satellite study to determine the feasibility of using satellites for NS/EP. The objectives of the study were to:

- Develop a comprehensive view of the commercial satellite industry as it relates to non-DoD and Intel communities
- Delineate 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 examined: the baseline capabilities of existing commercial satellite infrastructures; identified and made an initial assessment of key satellite system vulnerabilities; analyzed Federal agencies' satellite communications use vis-à-vis NS/EP functional requirements; and postulated candidate commercial NS/EP SATCOM programs. Finally, based on the study findings a smaller set of NS/EP commercial SATCOM programs were recommended.

The AT Branch, along with other Federal entities and satellite industry participants, was invited to participate and brief to the National Security Telecommunications Advisory Committee (NSTAC) Satellite Task Force (STF) on the Commercial Satellite Feasibility Studyfindings. The NSTAC STF embarked on a study to review and assess policies, practices, and procedures for the application of infrastructure protection measures to commercial SATCOM networks used for NS/EP communications. The study was triggered by a request of the Director of the National Security Space Architect.

Priority Text Messaging
With the preponderance of cell phones today, the use of pagers has declined and many manufacturers have announced plans to discontinue these devices. Short text messaging to mobile devices is increasingly important to NS/EP users who previously relied on pagers for data/text communications. The AT Branch studied SMS technology, the trend in traffic growth, and, most importantly, the impact of that trend on mass NS/EP messages on this channel of communications. The NCS study findings will be the basis by which managers of emergency mass notification applications will be able to assure message delivery with the major U.S. wireless carriers.

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 AT Branch, coordinates and approves these tests and studies, and keeps the National Security Advisor informed of them. The AT Branch has also published documents delineating telecommunications vulnerabilities due to EMP, Magneto Hydro Dynamics, High Power Microwave, Directive Energy Systems, High Radiation Environments, Solar Flares, and the effects of lightning.

The AT Branch 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

TEDE susceptibility tests of the telecommunications infrastructure include:

- PSTN switching systems and infrastructure
- Terrestrial/satellite transmission and power systems
- Equipment level tests and network level modeling
- Congressional "live fire" high-power microwave vulnerability tests of SCADA systems, PSTN switching systems, LANs and computer systems

Participating in the work of the Congressional EMP Commission, the AT Branch provided a briefing of current efforts and made legacy TEDE studies available. The briefing focused on vulnerabilities to the total national infrastructure, with telecommunications being a critical part of that infrastructure.

The AT Branch is currently investigating:

- Solar mass emission effects on the power grids, which could disrupt the electric power distribution systems, and SCADA systems connected to telecommunications systems
- Vulnerabilities of Internet and telecommunications hotels due to malicious high-power microwave injections

CRITICAL INFRASTRUCTURE PROTECTION DIVISION

The Critical Infrastructure Protection (CIP) Division includes five branches: the Operations Branch, the Planning, Training, and Exercise (PT&E) Branch, the Operational Analysis (OA) Branch, the Priority Telecommunications Services (PTS) Branch,

and the 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, administrative oversight and project management.

The Operations Branch is responsible for emergency response operations, information sharing activities, and administering priority telecommunications. The emergency response activities include activating and staffing Emergency Operations Teams (EOTs), producing and maintaining standard operating procedures, developing and maintaining flyaway kits for use during response operations, and maintaining the readiness of the NCC Watch Center and the NCC and OMNCS relocation sites. The branch is also responsible for the day-to-day operations of the NCC, the Telecom Information Sharing and Analysis Center (ISAC), and the 24x7 Watch Analysis Operations.

The PT&E Branch is responsible for developing, conducting, and participating in 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 branch supports several interagency working groups focused on emergency response, continuity of operations (COOP), and continuity of Government (COG) planning. The Branch also administers the NCS Individual Mobilization Augmentee 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 threats to and vulnerabilities of the public network affecting NS/EP telecommunications. These assessments are intended to facilitate assurance 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.

The Office of Priority Telecommunications (OPT) is the operational arm of the National Communications System priority telecommunications programs to include associated outreach. OPT manages the administration of the GETS, WPS, and TSP programs which allow NS/EP personnel to queue ahead of the public for telecommunication needs during crises on the public telecommunications infrastructure.

National Coordinating Center

DHS/NCS manages the National Coordinating Center (NCC), an industry-Government collaborative body, established in 1984. The NCC mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications service or facilities under all conditions, crises or emergencies. The operational arm of the NCC is the 24x7 watch and analysis operation, the "NCC Watch." Senior level information assurance analysts are located on site in the NCC Operations Center,

continuously fostering technical working relationships with external liaison partners, both industry and Government. Their technical expertise and collaboration efforts, coupled with evolving analysis capabilities, are key in adding value to the information sharing process.

Major NCC activities in FY 2004 included:

- Enhanced procedures to ensure effective information sharing, especially within Department of Homeland Security to include National Cyber Security Division (NCSD) and U.S. Computer Emergency Readiness Team (U.S. CERT), the Infrastructure Coordination Division and National Infrastructure Coordination Center, and the Homeland Security Operations Center Infrastructure Protection NICC Desk

- Provided evaluation and analysis on multiple hardware and software vulnerabilities and exploits including Bagle, Netsky, MyDoom, Mimail, Welchia, PhatBot, and Netsky

- Conducted testing and analysis on Transmission Control Protocol vulnerability in regards to specific Border Gateway Protocol (BGP) sessions. This included a test lab environment setup; download and installation on exploit tools, and test scenarios exploring three different possible attack options

- 24x7 NCS Watch Desk representation in the DOD's Global Network and Security Operations Center, fostering information sharing with industry and coordinating information sharing among Government Network Operations Centers

- Maintained an effective working relationship with both the Canadian Government and the telecommunications industry in Canada. Personnel from Industry Canada and the Public Safety and Emergency Preparedness Canada deploy 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 U.S and Mexico, and eventually a tri-lateral body to work critical telecommunications infrastructure cross border issues

Telecommunications Information Sharing and Analysis Center

The NCC Telecom-ISAC is a function of the NCC and builds on the history of cooperation and established trust among the NCC members. Currently there are 32 industry member companies and associations with membership open to companies that provide telecommunications or network services, equipment or software, select Competitive Local Exchange Carriers (CLECs), Internet Service providers, telecom professional organizations/associations, and companies with participation/ presence in the communications and information sector. The 24x7 NCC Watch performs triage for all NCC functions, manages the NCC Telecom-ISAC information sharing process, and provides an analysis function for the NCC Telecom-ISAC.

Major NCC Telecom-ISAC activities in FY 2004 included:

- Formulated lessons learned from both the August 2003 Northeast Power Outage and Hurricane Isabel, both clearly illustrating the dependence of the telecommunications infrastructure on the electric power infrastructure. Successful coordination between the Energy ISAC and the NCC Telecom ISAC was used as a foundation to develop sound coordination efforts with other critical infrastructures and their corresponding ISACs

- Participated in several critical infrastructure protection exercises including Livewire, a scenario designed to examine DHS' roles and responsibilities in response to cyber threats and to establish information-sharing processes for an emergency situation

- Reorganized the NCC Telecom-ISAC organization, establishing both an industry and Government chair position to facilitate a better working relationship with the newly formed ISAC Council and the Multi-State ISAC

- Developed and implemented additional strategies to further encourage new membership to the NCC Telecom-ISAC, especially within the satellite industry

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 Watch Analysis Office (WAO), to develop and implement the GEWIS capability. GEWIS is envisioned to 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 2004 saw the transition of GEWIS program management from the NCS to NCSD to better align cyber tool development with respective directorate mission requirements. NCS and NCSD continue to collaborate on system functionality and further refinement of requirements as technologies advance in the telecommunications and cyber arenas. During FY 2004, the NCS led the system development of GEWIS to v2.0. The enhancements included the addition of data sources to provide a broader perspective on situational awareness and to provide validation and corroborate the analysis results from existing data streams. System interface was enhanced to provide the analysts improved visualization to detect anomalous activity and the ability to isolate the activity and drill down into the data.

Alerting and Coordination Network

The Alerting and Coordination Network (ACN) is a private telecommunications network independent of the PSN. The mission of ACN is to provide a stable emergency communications network connecting the telecommunications service provider's NOCs and/or emergency operation centers (EOCs) in order to support network restoration, coordination, transmission of telecommunications requirements and priorities, and incident reporting when the PSN is inoperable, stressed, or congested.

ACN implements a private IP backbone network in a seamless, server-based environment, providing several levels of fault tolerance and scalability. ACN continues to support the NCC as well as existing ACN participants, the NCC Telecom-ISAC and the CWIN.

The OMNCS continues to work with industry to establish procedures for maintaining and utilizing the ACN and expanding its availability within the telecommunications infrastructure. With the conversion to VoIP completed, ACN continues to evolve, providing cross-infrastructure coordination in the event of outages in the telecommunications infrastructure.

Cyber Warning Information Network

Established originally with a focus on protecting the Nation's cyber infrastructures, Cyber Warning Information Network (CWIN) was expanded to support critical infrastructure protection across all sectors. It provides a private, protected and reliable network, offering voice and data connectivity to industry and Government partners. Membership is distributed through all the critical infrastructure sectors and will include Information Sharing and Analysis Centers for each sector.

Deployment of CWIN to user sites began in mid-FY 2002 and has continued through FY 2004. CWIN participants now include Federal watch centers at geographically dispersed locations and other sites, including telecommunications and Internet service providers and critical infrastructure protection entities. With the NCS transition to DHS, the CWIN program participant prioritization and implementation schedule are being aligned with similar DHS systems, goals, and objectives.

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 2004, the CCPC met twice in plenary session: once at NATO headquarters in Brussels, Belgium, and the other in Tblisi, Republic of Georgia. Its telecommunications working group met four times and the postal working group met twice. A group of rapporteurs tasked to develop a paper on the impact of the information society on civil emergency planning and the impact of interdependencies on civil emergency planning met three times (Brussels, Washington, D.C., and London).

Major CCPC FY 2004 activities and accomplishments include:

- Approved the 2004 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 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 26 NATO nations

- 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

Civil Infrastructure Protection—International Outreach

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

- Mexico, January 29—30: The Director of the NCS and the Department of State representative travelled to Mexico City to finalize the installation of a Homeland Security Telephone Link between Secretary of Homeland Security Thomas Ridge and Secretary of Governance Santiago Creel. The appropriate diplomatic protocols and agreements were signed by the Director and officials of Centro de Inteligencia y Seguridad Nacional (CISEN)

- Washington, D.C., March 9—10: The Director of the NCS was a delegation member to the U.S.-Germany bilaterals held at the Deparment of Commerce under the auspices of the Department of State and the Department of Homeland Security. A presentation by the Director regarding ISACs and the government-industry partnership in place at the NCS was well received by our German colleagues

- Canada, April 6—7: The Director of the NCS and the Department of State representative travelled to Ottawa, Ontario to finalize the installation of a HSTL between Secretary of Homeland Security Thomas Ridge and Deputy Prime Minister Anne McLellan. The appropriate diplomatic protocols and agreements were signed by the Director and officials of the Office of the Privy Council

- Australia, April 21—23: The Director of the NCS was a delegation member to the U.S.-Australia bilaterals held in Canberra. Key activities as a result of the bilateral included capacity

building to better protect information systems, promotion of security education and the itendification of cooperative efforts on practical objectives to include Civil Infrastructure Protection modelling and threat assessment and joint research and development. The Director was accompanied by the current industry representative, a Qwest official, who presented information relative to government-industry partnerships

- The Netherlands, September 22—23: The Director of the NCS participated in a CCPC working group session held in Rotterdam. The Director toured the Port of Rotterdam to include the operations center where he was provided a briefing on the technology in place to provide security for the port. The Director was a speaker at the joint session of the Telecommunications and Postal working groups where he explained the mission of the NCS to delegations from 26 NATO nations

- Washington, D.C., September 28—29: Officials from NCS participated in the U.S.-Mexico bilaterals held at the Department of State. The bilaterals are a continuing process in support of the Smart Borders Agreement between our two nations

- Arlington, VA, October 5—6: The NCS hosted a visit of a delegation from the Netherlands composed of high-level government officials. The Netherlands has an interest in the activities of the National Coordinating Center and received briefings in that regard

- Washington, D.C., October 18—22: The Director of the NCS participated in the U.S.—Russia Technical Talks held at the Department of State. In his capacity as Chairman of the Standing Subcommittee on Upgrades, the Director has the responsibility for U.S. oversight of improvements to and modifications of the various "hotline" programs between the two nations. The Director negotiated preliminary plans and procedures for the installation and activation of a Homeland Security Telephone Link between Secretary Ridge and his Russian counterpart

- Belgium, November 24—25: The Director of the NCC attended orientation sessions in Brussels to become familiar with NATO operating procedures. The Director of the NCC has been named as the Telecommunications Liaison Officer to be contacted by NATO senior staff for technical assistance with international telecommunications issues during times of emergency, crisis and war

The Department of State 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 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
- 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

Critical Infrastructure Protection—International Activities

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 Department of State 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 meeting, the Manager, NCC, and the Department of State 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, D.C., 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. Department of State and comprised of members from industry and 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. Department of State, hosted an official CIP bilateral meeting comprised of members from 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 Department of State representative continues to attend NATO CCPC meetings in coordination with the U.S. telecommunications representative on behalf of the NCS.

Network Security Information Exchange Activities

The joint meetings of the NSTAC and 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 2004, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including peer-to-peer networks and spyware, patch and risk management, and offshore outsourcing. White papers were produced on Telecommunications Sector Cyber Security Guidelines for changes to the National Threat Condition; Spyware: Security Implications and Recommended Strategies for Combating the Threat; and Laptop Theft. In addition, in coordination with the Telecom ISAC, BGP guidelines were developed.

In FY 2004, the NSIEs worked closely with Industry Canada and Canadian Telecommunications companies to establish an NSIE-like entity in Canada similar to those already in existence in the United States and United Kingdom.

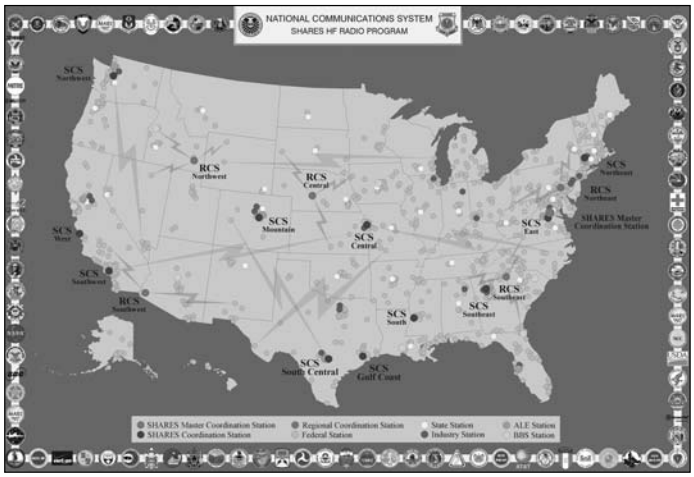
Shared Resources High Frequency Radio Program

The Shared Resources High Frequency Radio Program (SHARES) 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 high frequency radio resources of Federal and Federally affiliated organizations when normal communications are destroyed or unavailable. SHARES incorporates the resources of 1,115 HF radio stations located in all 50 states and overseas.

Emphasis continues to be placed on readiness by conducting nationwide SHARES exercises each year, as well as the SHARES Weekly Net which is conducted for a two-hour period every Wednesday. The SHARES Interoperability Working Group (IWG), a permanent body established under the NCS Committee of Principals (COP), continues to meet monthly to coordinate SHARES network activities and to address issues affecting interoperability of Federal HF radio systems. The IWG, composed of 109 members representing 72 Federal, state and industry organizations, continue 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 25 SHARES Outreach Program events.

During FY 2004, SHARES conducted 56 on-air operations. A total of 9,539 Station Availability Reports were submitted to the 15 SHARES Coordination Stations during these operations. This number includes 48 weekly SHARES nets as well as the eight SHARES events listed below that resulted in a SHARES Operational level change. One thousand one hundred and fifteen SHARES stations, representing 54 Federal, state, and industry organizations, located in all 50 states, Puerto Rico, Virgin Islands, and D.C., participated in the operations. The NCS



consistently saves the Department of Homeland Security millions of dollars annually in resources and manpower as a direct result of the SHARES emergency radio program.

SHARES conducted operations for the following events:

1. SHARES Weekly Net—48 Total for FY04
Average Weekly Station Participation: 160
Government: 155
Industry: 5
Entities: 20

2. Threat Advisory Level HIGH—
(22 DEC 03)
Stations Participating: 298
Government: 289
Industry: 9
Entities: 35

3. State of the Union Address—(20 JAN 04)
Stations Participating: 177
Government: 170
Industry: 7
Entities: 22

4. Super Bowl #38—(01 FEB 04)
Stations Participating: 206
Government: 203

Industry: 3
Entities: 21

5. Hurricane Charley—(13 AUG 04)
Stations Participating: 209
Government: 203
Industry: 6
Entities: 29

6. Republican National Convention—(30 AUG 04)
Stations Participating: 298
Government: 292
Industry: 6
Entities: 30

7. Hurricane Frances—(03 SEP 04)
Stations Participating: 290
Government: 283
Industry: 7
Entities: 26

8. Hurricane Ivan—(11 SEP 04)
Stations Participating: 314
Government: 308
Industry: 6
Entities: 32

9. Hurricane Jeanne—(25 SEP 04)
Stations Participating: 256
Government: 250
Industry: 6
Entities: 24

Planning, Training, and Exercise Support

The 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 2004, the Branch successfully coordinated and performed the following activities:

Emergency Response Training Seminars
Emergency Response Training (ERT) seminars are a highly visible and successful training program for the NCS. 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 mission and capabilities of the NCS; explain the NCS' role as the primary Federal agency for Emergency Support Function (ESF) #2 within the National Response Plan; and emphasize the best use of finite industry and Government resources. During FY 2004, seminars were presented to Federal, state and local government, and private industry emergency planners and operators in Federal Regions VI (Irving, TX), VIII (Denver, CO), IX (Oakland, CA), and the National Capital Region (NCR). This effective training outreach program reached a combined audience of approximately 355 attendees.

Emergency Operations Team Training
During FY 2004, internal training was provided to familiarize personnel with ESF #2 responsibilities during a disaster. In addition a COOP deployment was conducted with the NCC industry partners to familiarize the 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. Within the NCR, the NCS responded to a region-wide directive from the DHS to implement COOP

procedures and operate from the NCS Relocation Facility for 1½ days. In the Federal Regions, the NCS Regional Managers participated in regional exercises such as UNIFIED DEFENSE-04, pre-hurricane season exercises, and DETERMINED PROMISE-04.

OMNCS Individual Mobilization Augmentee Program

The OMNCS continues its Individual Mobilization Augmentee (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 deploy 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 myriad 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 NCS NS/EP mission at the national and regional levels.

During FY 2004, the NCS augmentees provided support for disaster relief operations in the Federated States of Micronesia after the Typhoon Lupit disaster. Additionally, the IMAs were on-call or on-site to support several national security special events, such as, the international G-8 Conference, and the two national political conventions.

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 COOP program that ensures its critical mission essential functions will be sustained throughout any emergency. The OMNCS continues to update contingency plans, procedures, and facilities to effectively ensure continuation of its critical missions and 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 insure the operational readiness of the OMNCS personnel that will respond to the emergency. Through its involvement in the Department of Homeland Security's COOP Working Group, the OMNCS participated in the planning and execution of the May 2004 National Capital Region deployed COOP training and exercise event, FORWARD CHALLENGE 04, for the Federal Executive branch.

Continuity of Government

As directed by E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, the OMNCS provides valuable staff and administrative support to the Executive Office of the President, Office of Science Technology Policy in the execution of its emergency functions.

One-Stop-Shop Service

The NS/EP Priority Communications One-Stop-Shop Service (OSSS) enables NCS customers to acquire NCS NS/EP priority communications information, services, programs, and operations from a single source. The goal of OSSS 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

FY 2004 accomplishments include:

- Expanded the hours and reach 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 metro Washington, D.C., area at 703-676-CALL (703-676-2255), Fax: 703-607-4984
- Completed 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 is available at: www.ncs.gov
- Completed a Concept of Operations to help define the roles, responsibilities and goals of the OSSS
- Implementation of an intensive marketing and outreach program to expand the user base for the OSSS programs/services which is supported by a marketing strategy plan as well as development of various marketing tools using both web technology and other media as appropriate

Telecommunications Service Priority Program

The TSP Program, established by a FCC Report and Order dated November 17, 1988, provides a regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications services. FCC authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments. FY 2004 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 over 62,000 total active TSP assignments in support of NS/EP communications. During FY 2004, the

OMNCS issued more than 300 provisioning TSPs to aid in the installation of critical circuits. The TSP user base increased by more than 65 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 accomplished the revalidation of all expired TSP assignments and initiated the vendor confirmation process.

TSP Information Technology Solutions

The OMNCS continues to utilize innovative IT solutions in support of TSP Program operations. During FY 2004, the NCS TSP Program Office 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, by exploring the development of a web-based application. These enhancements will result 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.

During FY 2004, the TSP website (http://tsp.ncs.gov) was redesigned to enhance its accessibility and improve its consistency with other NCS Priority Program websites. Among the information included on the site are frequently asked questions and 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 2004, the CIP Division and the TSP Program Office continued its ongoing outreach efforts 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 2004 TSP outreach activities, as various financial institutions, the Department of Transportation, and the United States Department of Agriculture 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 remain a high priority. For example, the OMNCS and TSP OC found that a low percentage of 911 Public Safety Answering Points (PSAPs) were currently enrolled in the TSP Program. To reach these PSAPs, the OMNCS implemented a targeted outreach campaign in FY 2004, utilizing regional workshops, published articles, and working relationships with major national public safety organizations.

Priority Telecommunications Outreach

The NCS CIP Division had over 40 trade show exhibits this year across diverse venues within the United States. 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, WPS, SHARES for HF Radio, and OSSS. CIP services support the initiation, coordination, and restoration of NS/EP telecommunications during national crises or emergencies, and regional disasters. The Outreach Program identifies the ways in which these services can benefit various emergency management organizations and the importance of incorporating the 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 around the country 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 2004:

- Minneapolis, MN, January 8: Finance & Banking Information Infrastructure Committee
- Orlando, FL, January 27—29: Armed Forces Communications & Electronics Association's TechNet
- Orlando, FL, January 27—29: Emergency Management Association
- Washington, D.C., February 25—26: AFCEA Homeland Security Information Technology
- Orlando, FL, February 29—March 3: Information Processing Interagency Council
- Salt Lake City, UT, March 2—6: Emergency Medical Service Today
- Orlando, FL, March 7—10: Disaster Recovery Journal
- Williamsburg, VA, March 16—19: Virginia Emergency Management Association
- Raleigh, NC, March 30—April 2: Homeland First Response
- Lake Buena Vista, FL, April 5—9: National Hurricane Conference
- San Antonio, TX, April 14—16: Energy Telecommunications & Electrical Association
- Dallas, TX, April 18—20: National Disaster Medical System
- San Antonio, TX, April 19—21: AFCEA Fiesta TechNet
- Denver, CO, April 24—29: DOD Emergency Preparedness Liaison Officer
- Charlotte, NC, April 25—27: American Water Works Association Security

- Indianapolis, IN, April 26—May 1: Fire Department Instructors Conference
- Washington, D.C., May 2—4: American Hospital Association
- Las Vegas, NV, May 5—7: National Academies of Emergency Dispatch
- Nashville, TN, May 16—19: United Telecom Council
- Las Vegas, NV, May 18—20: National Air Transportation Association
- Tampa, FL, May 24—28: Florida Hurricane
- Ocean City, MD, May 24—28: Maryland Emergency Management Association
- Warrenton, VA, May 24—28: TS/WPS Team Forum
- Hunt Valley, MD, June 3—6: International Association of Fire Chiefs HAZMAT
- Burlington, VT, June 13—17: Adjutant Generals Association of the United States
- Tampa, FL, June 13—17: National Emergency Number Association
- Chicago, IL, June 20—24: SUPERCOMM '04
- Las Vegas, NV, June 22—25: American Public Communications Council
- Philadelphia, PA, June 28—29: Information Sharing for Homeland Security
- Washington, D.C., July 27—29: Ready! Emergency Preparedness & Response
- New Orleans, LA, August 12—15: International Association of Fire Chiefs
- Nashville, TN, August 16—19: GSA/Federal Technology Service
- New York, NY, September 9—14: National Emergency Management Association
- Atlanta, GA, September 12—15: American Public Works Association
- New York, NY, September 14—15: U.S. Maritime Security
- Las Vegas, NV, September 14—16: National Guard Association of the United States
- Philadelphia, PA, September 16—21: American Association of State Highway and Transportation Officials
- San Diego, CA, September 19—27: Disaster Recovery Journal
- Long Beach, CA, September 22—October 1: American Association of Port Authorities
- Sacramento, CA, September 27—30: Californian Emergency Management Association

- St. Paul, MN, September 27—30: Association of State and Territorial Health Officials

Operational Analysis Branch

The OA Branch of the CIP Division serves as the focal point for developing analytical assessments to ensure the availability of NS/EP telecommunications services despite threats to or disruptions of the infrastructure. Analytical initiatives conducted during FY 2004 include:

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 conducted 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 allow the NCS to make recommendations for improving the ability of WPS to handle the needs of priority users.

Network Analysis Wizards
The OA Branch developed a requirement specification for the development of user-friendly, automated network analysis wizards to support the analysis and visualization of networks. The wizards will be designed to accommodate users with differing levels of technical skill and telecommunication knowledge. The network analysis wizards will support joint recoverability assessments between NCC telecommunications carriers and various sector stakeholders. In addition, the network analysis wizards will examine possible telecommunications network resiliency and diversity issues that could affect core sector processes. Through the use of the wizards, stakeholders will be able to visualize and evaluate potential mitigation strategies designed to reduce risks within their networks.

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 communication (such as cellular phones) had failed. The capabilities of these wireless messaging devices and their nationwide coverage make wireless messaging a potentially good medium for emergency communications. However, the wireless messaging networks supporting these devices have not been fully explored. The OA Branch conducted a study to examine the robustness of the wireless messaging network architecture, its dependence on the wireline network, and its potential vulnerabilities and mitigation options. Results from this study will allow the NCS to make recommendations for improving the ability of wireless messaging services for emergency communications.

Emergency 911 Assessment
Across the country, the 911 systems are in varying stages of compliance: From no 911 service, to basic 911 service, to fully enhanced 911 service. Given recent legislation, which has brought about a great deal of change to the emergency system (especially for the wireless network) the OA Branch completed an assessment of the 911

system to examine the various 911 architectures and system components for the wireline and wireless networks. Results of this assessment will allow a better understanding of the interactions betweenthe 911 service and NS/EP telecommunications services.

Submarine Cable Outage Impact Study
In October 2003, TAT-14, a major transatlantic cable was severed in two locations, resulting in the complete failure of the submarine cable. The OA Branch assisted its customers in investigating the nature and cause of the failure. Furthermore, based on concerns raised about the potential impact of a large-scale submarine cable outage, the OA Branch initiated a study to quantify the impacts from a range of submarine cable outage scenarios. The range of scenarios and the corresponding impact analysis results will provide information to help determine the scale at which submarine cable outages become a national security concern. Results from this study (expected to be completed in FY 2005) will also assist in defining recommendations for mitigating against such large-scale outages and protecting critical international communications.

Telecommunications Assets Prioritization Assessment
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies the need to take stock of key assets to reduce the vulnerability to physical attack on the national critical infrastructure. The OA Branch developed and implemented an iterative methodology to provide a prioritized list of telecommunications assets in the telecommunications infrastructure. The list of prioritized telecommunications assets will allow the OA Branch to effectively focus their analysis initiatives on the most critical assets in order to support the development and implementation of protective actions to mitigate against potential risks.

Streamlined Analysis Processes
In the past, the OA Branch repeatedly has been called upon to produce analysis results in short timeframes. To improve the response time for future analysis requests, the OA Branch streamlined and standardized its processes for producing its analysis products. This streamlining effort enhances the capability of the OA Branch to provide consistent and timely analysis results in as short as 30 minutes during crises, disasters, and other national security events.

Telecommunications Dependency Analysis
The increasingly interdependent nature of the nation's infrastructures has the potential to create new and hidden vulnerabilities, the exploitation of which could cause widespread damage to our nation's infrastructures, economy, and national security. To uncover, mitigate, or neutralize these vulnerabilities, the OA Branch has initiated a series of case studies to exercise an operational approach for analyzing and assessing the dependencies of the nation's critical infrastructures on telecommunications. This approach will enable the OA Branch to conduct dependency analyses at an operational level and produce actionable results in short timeframes when an actual outage occurs, or when a threat against a critical infrastructure is imminent.

Information Technology Support

In support of NCS users, the IT Branch collected requirements and is working with DHS preparing for an agency move to multiple facilities. As the

Defense Information Systems Agency (DISA) local area network (LAN) liaison, the IT Branch represented OMNCS interests in areas such as proposed DISA network enhancements, the migration of desktops to Win2000, which includes purchasing a major CPU upgrade. The branch assessed impacts to operations resulting from the implementation of new, or modification to, existing DHS, DOD, and DISA policy including the impact of shutting down ports and protocols to the network and the migration of equipment into a DMZ subnet.

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 DHS to DISA 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 according to DHS and DISA policies. During the past year, the Branch has assisted in the reaccreditations of the TSP system, the NCS homepage server, the Watch Daily Analysis, ACN/CWIN, GEWIS, & the N2 Laboratory. Additionally, the Branch ensured that NCS systems and practices are maintained within evolving security guidelines. The branch has also decommissioned the Emergency Response Link (ERLink) and Information Sharing and Analysis System (ISAS), and led the migration of the NCS homepage server from DOD to DHS network assets.

PLANS AND RESOURCES DIVISION

The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, manpower 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 DHS directorates on financial and acquisition matters; DHS Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The division 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 Year Homeland Security 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 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

National Communications System Committee of Principals/Council of Representatives

The NCS COP is a presidentially designated interagency committee that provides the President of the United States with advice and recommendations on NS/EP telecommunications issues. COP membership is comprised of members from 23 Federal departments or agencies that lease or own telecommunications facilities or services of significance to NS/EP communications. The DHS became the newest member of the group when the NCS transitioned to the DHS from the DOD on March 1, 2003. The COP serves as a forum where senior Federal Government officials meet to study emerging issues, exchange ideas, and form recommendations that go to the Manager of the NCS, the Secretary of Homeland Security, the Director of the Office of Science and Technology Policy (OSTP); the Director of the Office of Management and Budget (OMB), the Chair of the National Security Council; and the President. COP meetings afford the opportunity for members to report on, discuss, and debate plans and programs to meet NS/EP telecommunications objectives.

The Council of Representatives (COR), the working group of the COP, was established via the COP Bylaws as a mechanism to contribute to the focus and direction of the COP by addressing timely issues related to present needs and requirements in the NS/EP telecommunications arena.

In FY 2004, COP members provided comment and input on important NS/EP plans, such as the Baseline National Incident Management System (NIMS) and the HSPD-7 Telecommunications Sector Specific Plan.; reviewed and revised several NCS issuances in accordance with changes in National-level authority documents; and oversaw the activities of three working groups. They approved a motion to revise NCS Manual 1-2-1, COP Bylaws, to permit the ability to vote by e-mail and to update the COP membership. COP members also approved a motion to revise NCS Directive (NCSD) 1-1, National Communications System Issuance System, and NCSD 1-2, National Communications System Membership to bring the directives in line with the Homeland Security Act of 2002, and the amended Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions. Revised NCS Directives 1-1, 1-2, and the NCS Manual 1-2-1 were forwarded to the EOP for review and consideration.

Specific working group activities and the results of their analyses including recommendations are discussed below.

Critical Facilities Working Group

The Critical Facilities Working Group (CFWG) was established in October 2002 to address how Federal entities can ensure reliable NS/EP communications for their critical facilities. During the course of its work, the working group scrutinized diversity definitions, examined NRIC Best Practices, and coordinated its efforts with the NSTAC's Industry Executive Subcommittee (IES).

In its report, the CFWG outlined the following options to improve diversity within facilities: (1) purchase primary and diverse services from one supplier; (2) purchase from two or more suppliers; (3) purchase through a telecommunications aggregator; or (4) use alternative media for backup facilities. The report also delineates the positive attributes as well as the challenges that each option presents, in addition to recommendations that a Federal agency with NS/EP communications requirements should take into consideration to help ensure diverse services.

The CFWG Report made additional recommendations for the FCC, GSA, NCS, and Network Reliability and Interoperability Council (NRIC). These recommendations included tasking the FCC, in conjunction with the NCS, to conduct a proceeding to define facility diversity for NS/EP communications; tasking the FCC to examine tariff penalties and other incentives related to NS/EP functions; and tasking NRIC to develop best practices for telecommunications service providers that offer facility diversity communications for NS/EP organizations. The report further recommends that GSA consider adherence to NRIC best practices in requests for proposals. The CFWG's report was signed by DHS Secretary Ridge and is currently under review at the White House.

Continuity Communications Working Group

Previously named the Enduring Constitutional Government Working Group, the Continuity Communications Working Group (CCWG) was established in June 2004 to develop a Federal enterprise architecture (FEA) to support the performance of Federal Executive Branch (FEB) minimum essential functions under all circumstances, including crisis or emergency,

attack, recovery, and reconstitution. Since its creation, the group has begun drafting the Continuity Communications (CC) FEA Strategic Vision that will provide the overarching objectives, general operational concept, and key technical characteristics for the effort. The CCWG is committed to producing a requirements-based, service-oriented architecture that offers operational, rather than technical, solutions, and providing an interface control document that will allow FEB organizations to map to the CC FEA. The CCWG expects to deliver the CC FEA to the COP by August 31, 2005.

Priority Services Working Group
Established in February 2004, the Priority Services Working Group (PSWG) was tasked to: (1) conduct a review of existing priority telecommunications service programs including outreach strategies and issues of affordability; and (2) to recommend necessary changes to existing programs, including the need to implement new programs. To accomplish its mission, the PSWG received briefings from various telecommunications carriers, participated in tours of the Maryland and Pennsylvania Emergency Operations Centers, discussed service pricing, examined grant opportunities for the programs, and analyzed participation rates.

Based on its data collection activities, the PSWG conducted a comprehensive review of the rules and directives associated with the priority services programs and recommended a variety of changes to the documents to ensure conformity with current Executive Orders, Presidential Directives, and the Homeland Security Act of 2002. Specifically, the working group recommended changes to the following issuance: FCC TSP Rules, FCC WPS Rules, OSTP NS/EP Rules, OSTP Rules on NCS Organization, NCS TSP Procedures, and NCS SHARES Procedures. The working group outlined its findings in its Recommended Administrative Changes to Top-Level NCS Priority Services Guidance Report. The COR and the COP both approved the PSWG's findings.

National Security Telecommunications Advisory Committee

Established by Executive Order 12382 in September 1982, the NSTAC is a presidentially appointed advisory committee comprised of no more than 30 industry chief executives representing the major communications, network service provider, information technology, finance, and aerospace companies. The NSTAC provides industry-based advice and expertise to the President on issues related to NS/EP communications policy. Since its inception, the NSTAC has addressed a wide variety of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns. The Committee held its 27th meeting on May 19, 2004, at which time the Principals met with senior Administration officials to review the efforts of the past cycle and to identify several issues for consideration during the NSTAC XXVIII Cycle. Specific task force activities and the results of their analyses, including recommendations to the President of the United States, are discussed in the following sections.

Robert Liscouski (left), Department of Homeland Security Assistant Secretary for Infrastructure Protection and the Manager of the NCS, chats with BellSouth Chairman and Chief Executive Officer F. Duane Ackerman during a break from the Business Session portion of the President's NSTAC Meeting, held May 19, 2004, in Washington, DC. Mr. Ackerman later assumed duties as the NSTAC Chair, replacing Dr. Vance D. Coffman, Chairman and CEO of Lockheed Martin. (Photo by Donna Burton, Defense Information Systems Agency.)

Industry Executive Subcommittee

During FY 2004, and per requests from the NSTAC's Principals and Government stakeholders, the NSTAC's IES continued to identify communications issues critical to NS/EP activities for further consideration by the Committee's task forces. These key topics included the vulnerabilities resulting from the interdependencies between the telecommunications and financial services industries, vulnerabilities within the commercial satellite infrastructure, trusted access to key infrastructure facilities, provisioning of NS/EP services over NGN, research and development (R&D) important to the future of NS/EP services, communications related legislative and regulatory concerns, and NSTAC outreach to key stakeholders.

Satellite Task Force

At the request of the National Security Space Architect, the NSTAC embarked on a study of infrastructure protection measures for commercial SATCOM systems during NSTAC XXVII. The NSTAC established the Satellite Task Force (STF) to examine how Federal departments and agencies use commercial satellite systems for NS/EP services; the vulnerabilities in the commercial satellite infrastructure and the standards for mitigating those vulnerabilities; and how Global Positioning System timing capabilities affect communications.

Based on its analysis of the commercial satellite communications infrastructure, the STF made several findings ranging from the nature of the procurement process to vulnerabilities of the systems themselves and concluded that the Government does not optimize or fully protect the satellite infrastructure despite its importance to NS/EP communications. In addition, the STF found that there is a shortage of "in-house" technical expertise to integrate satellite technology into agency network architecture, and the procurement process does not allow agencies to effectively compete for commercial SATCOM capacity.
From the vulnerability analysis, the STF determined that all components of commercial satellite systems are susceptible to intentional and unintentional threats and Federal agencies need to decide what additional mitigation techniques should be required to protect the integrity of their communications carried over satellite systems. Furthermore, the STF found that the Government does not have an adequate and proactive information assurance policy.

On the basis of the STF's analysis, the NSTAC made a variety of recommendations to the President, designed to ensure that current and future NS/EP needs are met by the crucial capabilities that commercial SATCOM systems provide within the overall NS/EP communications architecture: (1) Develop a national policy with respect to provisioning and management of commercial SATCOM

services integral to NS/EP communications; (2) implement a commercial SATCOM NS/EP improvement program within the NCS to procure and manage the non-DOD satellite facilities and services to increase the robustness of Government communications; and (3) appoint members from the commercial satellite industry to the NSTAC to increase satellite industry involvement in NS/EP communication issues.

To guide the implementation of these recommendations, the NSTAC provided an action plan framework for use by Federal departments and agencies. To improve NS/EP policy, the NSTAC suggested establishing a steering committee to examine how commercial SATCOM can be used to support the National Response Plan and NS/EP missions. To increase the robustness of Government communications, the NSTAC suggested that the Government:

- Maintain awareness of commercial SATCOM usage to allow for rapid prioritization to support NS/EP needs during emergencies
- Extend TSP to all fixed satellite service operators and extend WPS to all mobile satellite operators
- Develop a strong and proactive information assurance policy

Furthermore, to mitigate vulnerabilities in the SATCOM infrastructure, the NSTAC suggested that the Government:

- Conduct studies on physical vulnerabilities
- Identify a hierarchy of physical and cyber vulnerabilities
- Develop a plan and process to rapidly mitigate interference
- Develop security requirements commensurate with NS/EP communications needs

Financial Services Task Force

Upon the recommendation of Mr. Steve Malphrus, Federal Reserve Board (FRB), and Ms. Catherine Allen, BITS, who briefed the IES in November 2002, on the financial services sectors' concerns regarding network resiliency, redundancy, and diversity in support of critical financial services sector processes, the NSTAC established the Financial Services Task Force (FSTF). The FSTF was tasked to examine, from an NS/EP perspective, vulnerabilities related to infrastructure interdependencies between the telecommunications and financial services industries and to analyze issues regarding network redundancy and diversity that could impact the financial services sector and, consequently, the United States economy. The FSTF issued its final report in April 2004, and among its findings, the FSTF noted that recovery and redundancy together cannot provide a sufficient level of network resiliency if these measures can be disrupted by a single event; therefore, diversity is crucial. The FSTF stated that industry best practices for diversity include separation of multiple circuit paths, decentralization of office facility connections, and alternative transmission technologies. Moreover, the task force found that diversity solutions will continue to evolve if the telecommunications sector continues R&D efforts, and if the Federal Government and critical infrastructure customers continue to encourage and participate in those efforts.

As a result of the FSTF deliberations, the NSTAC made the following recommendations to the President:

- Support the Alliance for Telecommunications Industry Solutions' National Diversity Assurance Initiative and development of a process to examine diversity assurance capabilities, requirements, and best practices for critical NS/EP customers and, where needed, promote R&D to increase resiliency, circuit diversity, and alternative transport mechanisms

- Support financial services sector initiatives examining the development of a feasible "circuit by circuit" solution to ensure telecommunications services resiliency, and the benefits and complexities of aggregating sector-wide NS/EP telecommunications requirements into a common framework to protect national economic security

- Coordinate and support relevant cross-sector activities (e.g., standards development, R&D, pilot initiatives, and exercises) in accordance with guidance provided in Homeland Security Presidential Directive (HSPD)-7

- Provide statutory protection to remove liability and antitrust barriers to collaborative efforts in the interest of national security

- Continue to promote the TSP program as a component of the business resumption plans of financial services institutions

- Promote R&D efforts to increase the resiliency and the reliability of alternative transport technologies

- Examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions

Trusted Access Task Force

The NSTAC established the Trusted Access Task Force (TATF) following the NSTAC XXVI meeting to address the Administration's concerns that the telecommunications infrastructure may be vulnerable because trusted physical access to critical telecommunications facilities is routinely granted to individuals who require access to telecommunications assets to perform their jobs without ensuring that the individual will not pose a threat to the facility or the telecommunications infrastructure at large. Specifically, the TATF was charged to help mitigate potential threats to the telecommunications infrastructure by working with Government representatives, at the Federal, State, and local levels to develop guidance for the creation of national standards for national security personnel screenings and verification/credentialing procedures for key personnel. The TATF is nearing completion of its report, which offers recommendations in three key NS/EP telecommunications areas: screening processes, credentialing, and perimeter access control at national special security events (NSSE).

The TATF began its work by assessing the current state of background screenings within critical facilities by engaging both industry and Government organizations through a questionnaire and a series of interviews. Upon the completion of this research, the TATF concluded that the

telecommunications sector relies on varied and limited investigations and screenings by private contractor firms that do not have access to Government databases containing critical terrorist and criminal intelligence upon which access decisions should partially be based. Consequently, the telecommunications sector cannot fully protect the infrastructure against threats to national security. Furthermore, the task force identified the DHS Transportation Security Administration's (TSA) screening model as one which addresses several of the same challenges currently facing the telecommunications industry, including large numbers of facilities with varying degrees of security and access requirements in combination with a broad scope of employees, including contractors and vendors. Based on these similarities, the TATF has begun examining the benefits and challenges of leveraging the TSA program, or a program modeled after it, to screen private sector employees at critical facilities upon the request of private industry.

The task force also recognized that the presentation of a credentialing document to personnel is required to signify the successful completion by employees of a standard screening process and to designate the facilities to which personnel are allowed access. However, the task force noted that industry typically develops and issues such credentials as an individual company, and many times for each of their facilities separately. Thus, no highly secure, standard certificate-based picture identification card is employed industry-wide. Recognizing the importance of such a credential, the task force is in the process of finalizing recommendations aimed at developing a standard credential and has engaged the GSA Federal Identity Credentialing Committee to identify best practices in credentialing that should be applied to private sector critical telecommunications facilities.

During the May 2004 NSTAC XXVII Meeting, Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, DHS, emphasized the importance of the TATF's ongoing work, commenting that the Government needs to act quickly to ensure the security of numerous NSSEs over the coming months, including the Democratic and Republican National Conventions. He asked the NSTAC to provide DHS with actionable recommendations on short-term initiatives that could be undertaken to further increase security at these upcoming events.

To this end, the TATF, with the assistance of the NCC member companies, established a pilot program to pre-screen a small subset of industry employees who may have access to physical sites or critical information concerning NSSEs and associated critical facilities against Federal terrorist lists/Government databases. The purpose of the ongoing trial is to identify screening and credentialing obstacles specifically for industry support to NSSEs and to determine the requirements for and feasibility of initiating a centralized screening and credentialing process for the telecommunications industry over the long term. The insights raised by this program will also be incorporated into the recommendations for the future TATF report. The TATF expects to complete its report and issue final recommendations for review by the NSTAC Principals by December 2004.

Next Generation Networks Task Force

The convergence of wireless, wireline, and IP networks into the global NGN is causing a shift in the way that Governments and

critical infrastructures will meet their needs for NS/EP communications today and in the future. As a result, at the NSTAC XXVII Meeting, NSTAC Principals agreed that a task force should be created to engage subject matter experts (SMEs) in an examination of NS/EP requirements and emerging threats to the NGN.

Accordingly, the Next Generation Networks Task Force (NGNTF) was created to: (1) agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely; (2) identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and (3) examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements. The NGNTF was also tasked to explore international issues, both in terms of NS/EP functions that must be provisioned internationally and international threats to the NGN.

As an initial step, the NGNTF assembled a group of SMEs and Government stakeholders in August 2004 to discuss the NGN issues. As a result of the meeting, five fundamental issues were identified as essential to the work of the task force: (1) a description of the NGN; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. The task force established working groups to address each of these areas.

During the meeting, questions from Government stakeholders also arose regarding how NS/EP communications would be affected by the transition to the NGN, and efforts that could be taken immediately to preserve or enhance NS/EP communications for the future were of particular interest. Consequently, the NGNTF formed the Near Term Recommendations Working Group (NTRWG) to examine: (1) near-term opportunities for using existing technology to improve the security and availability of NS/EP communications on converging networks; and (2) areas where Government involvement was needed in the near term because of the immediacy of events such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs. The NGNTF expects to complete its NTRWG Report by October 2004, and to present the status of the efforts by its working groups to the NSTAC Principals at the NSTAC XXVIII Meeting in May 2005.

Research and Development Task Force

During FY 2004, the Research and Development Task Force (RDTF) focused its efforts on developing a proceedings document outlining the discussion from the 2003 Research and Development Exchange (RDX) Workshop held at the Georgia Institute of Technology in Atlanta, Georgia, and further addressing issues of concern also raised at the Workshop. In its proceedings document, the RDTF identified the following seven major findings regarding the trustworthiness of NS/EP telecommunications and information systems:

- A strong sense of frustration and urgency related to a lack of action and implementation of security

"remedies" identified at conferences and events

- A need to clarify the definition of NS/EP telecommunications in the post 9/11 world
- A need to address major challenges on driving technology innovation into NS/EP systems and functions
- A need to establish partnerships for R&D integration
- 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 direct response to these findings, the task force produced a white paper that outlined the various Presidential documents containing partial definitions of the terms national security and emergency preparedness. The white paper also noted the need for Government to more clearly define the term NS/EP in its entirety in a post-September 11, 2001, world characterized by a rapidly changing technology and threat environment. In addition, the task force began the development of a white paper stressing the importance of developing a pilot testbed for use by the NS/EP community upon which to test telecommunications related technologies. The task force plans to complete the white paper by May 2005.

Finally, the task force continued to prepare for the 6th RDX Workshop, titled "A Year Later: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness," which is scheduled to be held on October 28—29, 2004, in Monterey, California. Expected guest speakers for the event include Mr. F. Duane Ackerman, BellSouth and Chair of the NSTAC; Mr. Stratton Sclavos, chief executive officer of VeriSign and NSTAC Principal; and Dr. Charles E. McQueary, DHS Under Secretary for Science and Technology.

Legislative and Regulatory Task Force

At the request of the NSTAC Principals and Mr. Liscouski, the Legislative and Regulatory Task Force (LRTF) initiated an examination of the national and homeland security implications associated with the availability of open source critical infrastructure information on the Internet. The tasking arose in response to a discussion, led by an NSTAC Principal, on an industry sponsored analysis of open source infrastructure information. That discussion concluded that information regarding network architecture, local exchange routing guides, connectivity, and fiber-optic routing data was publicly available on the Web sites of numerous Government agencies, universities, telecommunications providers, and State and local Government regulatory agencies. In response, the Principals agreed that the NSTAC should review its Web publishing practices and policies and individual companies should be encouraged to conduct similar reviews. In addition, Mr. Liscouski encouraged a review of the available information on the Internet with an emphasis on noting data required to be posted to the Internet by Federal, State, and

local regulators. During the January 2004 IES Meeting, the IES tasked the LRTF with analyzing the availability of open source infrastructure information on the Internet.

The LRTF initiated its examination with a review of the Web publishing practices and policies of the Government, telecommunications carriers, and third-party Web sites. The examination included a review of the NCS practices and policies with regard to the NSTAC Web site. The task force also received briefings from Mr. Doug Langley, BellSouth, on an industry analysis of publicly available data; Mr. Jim Dailey, Office of Homeland Security, FCC, on the Commission's Web publishing policies; and Mr. Fred Herr, NSIE, on the NSIE's analysis of risks posed by publicly available information to the United States' telecommunications infrastructure.

In addition, the LRTF reviewed the National Institute of Standards and Technology's guidelines for posting Government information to the Internet and the NRIC best practices. The task force also reviewed Freedom of Information Act requirements and current Federal guidelines in the E-Government Act, the Office of Management and Budget's (OMB) Recommended Policies and Guidelines for Federal Public Websites, the "Federal Web Content Manager's Toolkit," and the DOD's Air Force Web publishing evaluation checklist. The LRTF plans to continue to examine national and homeland security concerns associated with open source infrastructure information on the Internet into FY 2005 and will develop a letter with recommendations to the President based on the results of it analyses.

At the same time, the LRTF also initiated an examination of the NS/EP concerns associated with implementation of the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act, receiving a briefing from the American Insurance Group regarding liability issues related to the Act. The LRTF will continue its examination of this topic into FY 2005, to determine if there are issues of concern relating specifically to telecommunications NS/EP services upon which recommendations to the President should be made.

NSTAC Outreach Task Force

The NSTAC Outreach Task Force (NOTF) operates to foster the exchange of information between key NSTAC stakeholders within both industry and Government. The NOTF is tasked to: (1) raise the awareness of the NSTAC across the Federal Government, industry, and academic and research communities; (2) solicit feedback and input on NSTAC products and outreach initiatives from these critical stakeholders; and (3) promote the adoption of NSTAC recommendations to the aforementioned key stakeholders.

The NOTF achieved these goals during FY 2004 by: providing briefings on NSTAC reports and recommendations to key stakeholders (including regular briefings to the NCS COP/COR, and meetings with several agencies in the EOP);

- creating the NSTAC video
- participating in the GSA/Federal Technology Service Conference
- participating in the Military Communication Conference

As a standing task force, the NOTF will continue to work with key stakeholders to

ensure broader awareness of the NSTAC's work within the national and homeland security communities.

Public Affairs Activities

The NCS continues receiving 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. The NCS coordinates all inquiries with the communications director for the DHS IAIP Directorate to ensure that the Department approves all requests for interviews and information about the NCS.

Inquiries continue to focus on the NCS role in the Department of Homeland Security and within the IAIP. Inquiries have also focused on the National Coordinating Center for Telecommunications and its Telecom ISAC, WPS program, the GETS, the TSP program and the NCS mission to work with industry in support of emergency communications.

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

Under DHS management directives, all press releases on the NCS and NSTAC are now coordinated through the DHS IAIP communications director and released by the Department.

The NCS published the NSTAC Reports for the NSTAC XXVII cycle in early May 2003. The NSTAC XXVII Issue Review is scheduled for publication in September. The NCS also produced a series of three-fold brochures outlining NCS operational programs such as the WPS, TSP, CWIN, and the ACN.

Outreach

The NCS Director 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 to do 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 the 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.

NCS Web Site

The NCS Web Site (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.

In February 2004, the NCS launched its new Web site, providing NS/EP telecommunications customers with easier navigation through the sites numerous sections. Of special significance is an expanded virtual library of published materials from both the NCS and NSTAC; a

better organized news archive, a section dedicated to frequently asked questions about the NCS, and direct access to program pages such as GETS, TSP and WPS.

The NCS continues to work with the DHS as the department upgrades its own site and incorporates the sites of its 22 Federal agency members into its revised site, as well as two DHS Intranet sites: DHS Interactive and DHSOnline. The NCS is responsible for coordinating input to the all DHS sites with the DHS IAIP communications director prior to submitting materials for posting on the DHS sites.


NATIONAL COMMUNICATIONS SYSTEM
NCS

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 United States (U.S.) foreign policy. This mission determines the Department's telecommunications support requirements. Essential DOS telecommunications functions include:

- 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 (IT) Facilities Consolidation

The Department continues to progress on consolidating and standardizing its enterprise server operations. This project was started in mid-Fiscal Year (FY) 2001 with the strategic goal of establishing a comprehensive "server farm" concept for consolidating IT facilities and processing resources, such as servers, databases and applications into centrally managed facilities and systems. The benefits include savings in manpower and facilities throughout the Department, improved security, data integrity, operational reliability, technical support and around-the-clock availability. As of 2004, the server farm infrastructure (also termed ESOC — Enterprise Server Operation Center) now consists of two main ESOCs, providing department-wide systems backup and recovery, and serving as a continuity of operations for the Department's financial service center in Charleston, South Carolina. Upwards of 1,000 servers are anticipated to be housed in the ESOCs.

Interagency Collaboration

The Department is committed to the enhancement of inter-agency communications and collaboration, particularly overseas. It is pursuing several complementary approaches toward that objective: acceleration of a modern messaging and archiving system – State Messaging and Archive Retrieval Toolset (SMART); expanded use of Open Source Information System (OSIS) and Secret Internet Protocol Router Network (SIPRNet); and, short-cut routing email connectivity between all embassy elements via a direct connection at post rather than through Washington Agencies' headquarters. Beginning with the new embassy in Baghdad, Iraq, the Department is also now requiring direct email connectivity among agencies represented at embassies, under Chief of Mission authority as expressed in Network Security Decision Directive 38. DOS is coordinating the effort through the Inter-Agency Collaboration Working Group chaired by Ambassador James H. Holmes, Deputy Chief Information Officer for Business, Planning and Customer Service.

The Department has greatly expanded the publication of classified reporting on SIPRNet; more than 100 embassies and bureaus maintain pages linked from its gateway site at http://www.state.sgov.gov. The Department is also moving ahead to improve communications and collaboration among agencies via the OSIS. OSIS is a virtual private network 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 and administrative data, 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 United Stated Agency for International Development (USAID), which recently joined OSIS.

The Department and USAID have established a Joint Management Council to build a common management foundation. As a result, the two agencies are working toward common use of networks, consolidation of technical and operational support, development of a joint Enterprise Architecture, and collaboration on Knowledge Management strategies. They are

DEPARTMENT OF STATE (DOS) *continued*

participating in each other's IT Capital Planning and Investment processes and developing joint Office of Management and Budget (OMB) Exhibit 300 submissions for major IT projects.

Messaging Systems
On April 4, 2002, the Under Secretary for Management approved a recommendation to accelerate the implementation of a SMART, 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 current processes for messaging including cables, memoranda and email, resulting in the preservation of the complete record of Foreign Affairs data information. The Inter-Agency Collaboration Working Group, serves as a sounding board for other agencies that may consider adopting the SMART Messaging System for part or all of their operations under OMB guidelines to promote shared technology development among Government agencies.

Classified Connectivity Program
The Classified Connectivity Program (CCP), started in 1999 to modernize the Department's classified infrastructure, providing authorized employees posted overseas with desktop access to classified email, telegram services, and SIPRNET, a Web-based tool that allows users access to certain Intelligence Community (IC) Web pages. This capability will facilitate closer collaboration among agencies working together to serve and protect the United States, 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 ended in September 2003, beating its scheduled end date by three months. At this time, 225 eligible overseas posts have a modernized classified infrastructure fully capable of supporting foreign affairs functions.

Secure Voice Program
The Department is nearing completion of the transition of its legacy secure voice system to the new National Secure Voice Standard, the Secure Terminal Equipment (STE) system. Currently over 4,200 units have been fielded worldwide with the remaining units to be deployed by December 2004. The STE have also been provided to support Embassy Baghdad and the Athens Olympic games. The replacement of the legacy secure voice system has also enhanced our interoperability with the Department's RED Switch. The STE enabled RED switch interface system enables higher quality voice service while maintaining backward compatibility with older secure voice systems used by our coalition partners.

Anti-Virus Program
The Department's Anti-Virus program has intercepted and destroyed over 7,000,000 virus attacks in the first half of calendar year 2004; compared to only 633,000 in all of 2003. This program has resulted in no major network outages during 2004 due to malicious code. A combination of robust network design, perimeter and desktop anti-virus tools has resulted in a very successful program. In an effort to educate users and to prevent unknowing introduction of malicious codes, nearly 20,000 anti-virus software CDs have been provided to Department employees for home use during the same period. This proactive measure controls virus incidents from emails or documents prepared by employees at home. The Anti-Virus program is now deploying new desktop software that will also scan for adware and spyware in addition to malicious codes thus further protecting the DOS IT infrastructure.

Communication Security Modernization
The Department is continuing its effort to modernize its national security level encryption systems, by using the National Security Agency's (NSA) Inline Network Encryption (INE) devices, (such as KG-235s, KG-75s, KG-175s). These new devices replace aging encryption systems and allow new higher-capacity robust network designs that leverage traditional Government-owned or leased circuits and Internet telecommunication services. In conjunction with the Department's SMART and Internet Virtual Private Network programs, INEs will allow state of the art real-time interagency secure communication of classified

DEPARTMENT OF STATE (DOS) *continued*

information. The INE devices have been provisioned to each diplomatic facility able to process classified information. Installation teams have been funded to complete the last 70 overseas Post activations. Additional KG-75 equipment is on order to further enhance the Department's domestic network and integrate it fully into the IC resources to ensure rapid reliable exchange of information.

The Department has installed and is implementing the NSA's Electronic Key Management System (EKMS). The migration over the next two years to full EKMS key distribution will allow the Department to quickly respond to emergencies as needed in almost real time. By using electronic distribution, key deliveries can be accomplished in minutes instead of days. The EKMS will eliminate the danger of intercepting the diplomatic courier in route with replacement key materials, thus reducing the vulnerability of the Nation.

Domestic Wireless Program
The Domestic Wireless Program provides ultra-high frequency (UHF) radio services to 24 Diplomatic Security (DS) Field Offices, Diplomatic Security protective details, and the buildings security force. Conversion to a new industry baseline/interoperability standard (APCO 25) allows equipment to meet new federal 12.5 kHz narrow-band standards and ensures interoperable capabilities among local, State and Federal public safety and law enforcement agencies. The replacement of analog by digital equipment significantly improves voice quality and voice communications security. Significant funds are dedicated annually for this program to support new security communications requirements, especially an expanding fleet of Diplomatic Security vehicles requiring mobile radio equipment and installations. Currently, 22 of 24 Diplomatic Security Field Office upgrades have been completed, with the final two ending by September 2004.

The Radio Programs Branch is also moving forward on a radio interoperability program, which directly supports the President's Quicksilver Initiative SAFECOM. SAFECOM is the umbrella program within the Federal Government to oversee all communication and interoperability initiatives and projects. Through SAFECOM, the Federal Government is addressing public safety communications issues in a more coordinated, comprehensive and, therefore, effective way. The Department of State's Radio Programs Branch initiated a radio interoperability program in FY2003 to meet this goal. LWS/RPB was accepted into the Department of Justice/Alexandria Police Department sponsored radio interoperability network located in the Greater Washington, D.C. area. The Advanced Generation of Interoperability for Law Enforcement utilizes JPS ACU 1000 interoperability units. The success of the JPS ACU-T equipment during LWS/RPB testing has led to the development of a new interoperability-training program within the Department and the planned sponsorship of a new interoperable network located in Portsmouth, NH (completion expected 12/2004). LWS/RPB is researching new venues for additional interoperability networks throughout the U.S. and overseas. Radio interoperability is an important tool used to coordinate interagency communications in support of homeland security efforts.

Washington Area Radio Network
Washington Area Radio Network (WARN) is currently a 15 year-old radio network. The upgrade program is introducing new SIMULCAST technology to greatly improving radio coverage. Conversion to a new industry baseline/interoperability standard (APCO 25) allows equipment to meet new Federal 12.5 kHz "narrow-band" standards and ensures interoperable capabilities among local, State and Federal public safety and law enforcement agencies. The replacement of analog by digital equipment will significantly improve voice quality and voice communications security by allowing for an improved version of the Digital Encryption Standard to be utilized. In the Greater Washington, D.C. area, WARN provides dedicated radio communication networks for all major DS divisions, most notably, Secretary of State's Protective Detail , Dignitary Protection , Domestic Facilities Protection and Washington Field Office. Upon completion of upgrade (expected completion March 2005), WARN will provide effective voice-radio communications in the Greater Washington, DC area to all subscribers.

High Frequency Radio Network
The High Frequency (HF) program utilizes 500-watt radios to provide long-range Emergency & Evacuation communications between embassies and consulates, DOD assets, other governments, NGO, and in some

DEPARTMENT OF STATE (DOS) *continued*

countries, U.S. citizens. The new HF equipment installed worldwide features automatic link establishment, which provides automatic frequency scanning technology, ensuring that radio communications are received regardless of the frequency channel selected. HF radio is independent of the host nation's local IT infrastructure, meaning that when phone lines or cellular phone systems are down, and other means of communications are not available, HF may provide a post its last possible means of communications when everything else has been destroyed or disabled. HF radio is used to communicate and coordinate evacuation of Foreign Service employees and their families, and other U.S. citizens. HF radio has been particularly successful in coordinating rescue and evacuation efforts in Africa for decades.

Communication Security (Public Key Infrastructure)
The Department is currently operating a Public Key Infrastructure (PKI) at the Federal PKI Policy Authority (FPKIPA) high-assurance level. In a team effort, the DS and Information Resource Management (IRM) Bureaus, have issued over 17,000 intelligent Smartcard Identifications that are being used for both physical access and logical PKI functions on the Department's unclassified Sensitive But Unclassified (SBU) systems. PKI hardware and software have been installed in over 15,000 domestic and overseas workstations with projected completion to occur in FY2006. The FPKIPA has cross-certified the Department's PKI systems and allowed it to connect to the Federal PKI interagency bridge. This gives the Department's current 17,000 (43,000 at full deployment) PKI users the ability to share SBU information rapidly in a secure manner, with eight Government agencies and the State of Illinois through the use of PKI digital certificates. Currently the Department's PKI program is providing the Smartcard based access control technology to the Department of Justice's Bureau of Citizenship and Immigration Services (BCIS), formally Immigration and Naturalization Service users at 88 locations around the country. BCIS estimates PKI services provided by the Department have saved taxpayers conservatively over $700,000 annually. The PKI program is also working with the Consular Affairs Bureau to integrate PKI into the Congressionally-mandated electronic intelligent passport also known as the Machine Readable Travel Document program. This system will digitally sign passport information using the Department's PKI to ensure the officially issued information can be verified and has not been altered in real time at the Nation's ports of entry. In the FY2006 timeframe, this system will support the production capacity of 7 to 10 million U.S. passports a year.

Global Information Technology Modernization Program
The Global IT Modernization (GITM) program, which was initiated on October 1, 2003, enables the Department to implement a disciplined approach to consolidate all modernization efforts for classified and unclassified local area networks (LAN) worldwide (overseas and domestic) under a centralized program for execution. This program protects the Department's substantial investment in IT infrastructure by modernizing the LAN segment of the Department's networks on a four-year life cycle. GITM modernizes existing LANs using emerging technologies, which are suited to meet new business requirements, vice the replacement of equipment. In this way, equipment obsolescence is eliminated and the latest lines of business-driven requirements can be met. By providing reliable, secure, robust and scaleable LAN infrastructures, foreign affairs workers will have the necessary tools to enable communications, collaboration, knowledge management, and the sharing of data and information in both classified and unclassified environments.

Public Diplomacy Net-OpenNet Plus Integration Completed
The Department completed the Public Diplomacy (PD) Net-OpenNet Plus Integration Project. The PDNet-OpenNet Plus Integration Project successfully integrates all PDNet users, from 32 domestic offices and 219 overseas locations, to the OpenNet Plus network. This was truly a team effort, with unprecedented cooperation between the Bureaus of Information Resource Management and International Information Programs—Educational and Cultural Affairs.

Department Networks Duplication Action Team
In response to a request by the Under Secretary for Management, IRM is supporting the E-Gov Program Board's Duplication Action Team initiative. Bureau action teams have been identified to review specific projects and systems within DOS.

DEPARTMENT OF STATE (DOS) *continued*

The Department Networks Duplication Action Team is analyzing and validating the business requirements of existing DOS networks and determining the feasibility and schedule by which non-corporate networks should be consolidated into existing enterprise-wide network services that meet its business requirements.

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 Virtual Private Network (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 227 alternate routes using this technology, with plans to implement at all posts by FY 2005. Current average VPN network availability is above 99%, with a goal of 99.7% in FY2007.

Certification and Accreditation Efforts
In December 2002, the Department had no formal authorization process and, indeed, had only authorized one system. Accordingly, OMB mandated that the Department authorize its existing operational systems before the end of FY 2004 or face redirection of its IT funding. Systems authorization—a risk management process—is imperative in today's world of complex networking, electronic information exchange and the inevitability of cyber terror events. It allows the Department to identify and reduce risk, balancing security requirements with operational necessity and mission accomplishment. Over the past fifteen months the Department has developed and implemented a robust process for Systems Authorization (also called Certification and Accreditation) as required since 1987 by OMB Circular A-130. Today, the Department has authorized over 90% (161) of its systems and is the first major Federal agency to do so.

DEPARTMENT OF THE TREASURY (TREAS)

NS/EP Telecommunications Mission

The United States (U.S.) Department of the Treasury 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 National Security/Emergency Preparedness (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 U.S. economic and financial management institutions, 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

The Department of the Treasury manages its telecommunications services through the Office of Chief Information Officer (CIO). The CIO provides oversight and management of NS/EP support activities and 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 information technology (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.

Ongoing NS/EP Telecommunications Activities

Treasury Communications System
The Treasury Communications System (TCS), the Treasury Department's nationwide 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.

During fiscal year (FY) 2004, cyber security was improved through a two avenues. FY 2004 saw the implementation of a layered approach to IDS management. Intrusion Detection SYstem (IDS) instances were deployed at various bureaus and departmental agencies allowing each organization to monitor and respond to their own internal alerts. Additionally, data is being sent to the central TCS Security Operations Center allowing for a larger consolidated view of activity across the Treasury network. This additional capability brings the total sensor count to 26 deployed across the Treasury network. The Bureaus fielding IDS instances include the Office of the Controller of the Currency and the Bureau of Public Debt. Additional agencies include the Departmental Offices (DO), Community Development Financial Institution , and HRConnect. The second avenue involves the ability to provide host-based intrusion detection systems (HIDS) allowing for individual system monitoring. To date, 18 HIDS have been deployed to various TCS and bureau assets. These additional capabilities extend the breadth of our cyber security monitoring and allow for quicker response times to major incidents.

DEPARTMENT OF THE TREASURY (TREAS) *continued*

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 was tested at the Treasury Alternate Operating Facility (AOF). The TCS Distributed Architecture Disaster Recovery facility backup center was completed in June 2004 and currently supports all Treasury bureaus alternate operating facilities and servers as the Disaster Recovery backup for the primary TCS facility.

In addition, the Treasury Headquarters' DO's 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 the Treasury AOF facility.

Additionally, Treasury Headquarters and associated Bureaus have designated which circuits and locations are to be supported through the National Communications System (NCS) TSP Program. TSP 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, before any non-TSP circuits, in case of a national emergency or disaster. This capability was utilized this year to restore several sites in the Southern U.S. that suffered damage during the Hurricanes this year. The Department of the Treasury currently maintains 746 TSP level 1 & 2 circuits.

Treasury Emergency Management Center Capability

As part of Treasury's COOP, 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 the Treasury Department in a crisis or emergency. Currently, these centers are being improved and modernized around changes in the Treasury Department's operating principles and practices and the associated IT systems for enhancing their business management information systems.

Certification and Accreditation

The TCS Security Assurance Program continues to make 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 2004, the TCS Security Assurance Program maintained its own accredited environment by ensuring that new services or changes added to the General Support System or Major Applications go through the complete C&A process as the original systems. In addition, the TCS Security Assurance Program has also performed C&A packages for other bureaus and agencies including: the Treasury external access network known as the Secure Extranet Gateway; HR Connect-Detroit Computing Center; and ProSight Portfolios used to support Treasury-wide capital planning and investment control (CPIC). The TCS Network itself also underwent the process of re-certifying and accrediting the entire TCS as part of the proscribed three year re-certification process and practice.

Currently, the TCS Security Assurance Program is in the process of certifying and accrediting the newly created Command Caller, Data Store, Neoteris. There is also a three year re-certification in progress on the Foreign Credit Reporting System.

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 CPIC 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 Public Key Infrastructure Development

The Treasury Department continues to provide technical, operational, and leadership support in the development and use of an interoperable Government-wide Public Key Infrastructure (PKI) to permit electronic transactions over the Internet in a trusted environment.

DEPARTMENT OF THE TREASURY (TREAS) *continued*

Treasury's enterprise PKI 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 National Aeronautics and Space Administration (NASA)) that have been cross-certified with the Federal PKI Bridge. This effort has allowed Treasury to strengthen its secure communications processes in conjunction and alignment with its development of a common infrastructure landscape. Treasury also has been working very closely with the General Services Administration's E-Authentication Initiative in helping define the Federal E-Authentication Technical Architecture and in leveraging Treasury's investment in PKI technology and relationships with the Financial Community. To date, all but one Treasury Bureau has implemented a PKI solution, with the remaining Bureaus planning implementation within the next year.

Public Safety/Law Enforcement Wireless Activities

The Treasury Wireless Programs Office was transferred to the Department of Homeland Security (DHS) in March 2003. During 2004, and in light of the organization's transfer to the Homeland Security Department, Treasury continues to partner with the Department of Justice, 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 the Treasury Department, 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 the Department of Justice and DHS in a joint radio system venture for the future.

Summary

The COOP requirements for the Treasury Communications System has been fully coordinated and synchronized with the plans and programs operating under the Treasury Department's Office of Emergency Preparedness. Notwithstanding the devolution of the Treasury law enforcement organizations to DHS, the issuance of Government Emergency Telecommunications Services cards continued to increase in FY 2004. Also during 2004, Treasury expanded the Treasury Emergency Management/Operations Center within the greater Washington D.C., metropolitan area to further strengthen Treasury's emergency preparedness posture. Key operational functions and capabilities expanded in FY 2004 are: Additional Department of Treasury Emergency Management Centers 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; and Local Treasury Headquarters connectivity to Treasury enterprise services, such as e-mail, business applications, and other information services.

Once completed, these enhancements and modernization initiatives in FY 2004 will allow Treasury to respond, operate and function in a crisis, emergency, or national disaster.

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 National Security and Emergency Preparedness (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

DD 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 specific 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 (ASD) for Networks and Information Integration (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 ASD (HD) for NII. C3 requirements are the concern of the Joint Staff J6.

Current /Ongoing NS/EP Telecommunications Activities

The Deputy Secretary of Defense signed a Memorandum September 8, 2003, realigning Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense. 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, the Department of Homeland Security (DHS), other Executive Departments and Federal Agencies, and State and local entities.

In 2004, ASD NII established the Global Information Grid (GIG) End-to-End Systems Engineering Activity. The focus of the activity is to deliver needed GIG-related products in time to support the execution of multiple programs. The objective is to synchronize programs, acquisitions, standards, architectures, and funding to ensure DOD has quality of service, network management, and information assurance within the GIG from an end-to-end standpoint in order to achieve net-centric operations.

The five major NII investment areas are:

- The Bandwidth Expansion program, or GIG BE, which provides a secure, robust, optical IP terrestrial network
- Joint Tactical Radio System (JTRS), 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 SATCOM, which provides ubiquitous communications with optical quality bandwidth
- Net-Centric Enterprise Services, which supplies infrastructure and services to support the broad range of applications and data used in a net-centric enterprise
- Information Assurance, which is vital to support all efforts to ensure that the Internet is robust, reliable, and trusted

Additionally, in August 2004, the ASD(NII) announced the successful completion of the Quantum Leap II Demonstration in support of the Horizontal Fusion initiative. The demonstration's focus was on software application interoperability at the data link layer to facilitate transferring, receiving, and retrieving data using a services oriented architecture over DODs SIPRNET. When successfully

DEPARTMENT OF DEFENSE (DOD) *continued*

implemented, this architecture will allow interoperability between different software applications with minimal impact to the user. The intent of the Horizontal Fusion Portfolio Initiative is to integrate and optimize technology and operations to facilitate net-centric operations.

DOD continues its partnership with DHS on the SAFECOM program. DHS is the lead Federal Agency charged with assisting State and local Governments address barriers to interoperability. They do this through requirements, definitions, development of interoperable communications standards and guidelines. DHS' Office for Domestic Preparedness, has responsibility for the actual implementation of interoperability programs, such as grants for equipment, training, and technical assistance.

In direct support of the NS/EP community of interest, the Continuity Communications Working Group (CCWG) was established in 2004 as an interagency body reporting to the National Communications System Committee of Principals. The purpose of the CCWG is to develop a Continuity Communications (CC) Federal Enterprise Architecture Framework (FEAF) and oversee the development of a Continuity Communications Federal Enterprise Architecture (CC FEA) to support the performance of Federal Executive Branch (FEB) minimum essential functions under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The mission of the CCWG is to define a CC FEA strategic vision, document continuity communications requirements and translate them into actionable performance criteria, develop a CC FEAF, document and normalize the existing FEB CC enterprise architectures, determine where requirements shortfalls exist and planned capabilities overlap, and make recommendations on a FEA to best meet FEB continuity communications requirements. The working group will leverage the existing Office of Management and Budget FEA and related architectural frameworks to accelerate the establishment of an integrated, secure, standards-based, survivable, scalable, reliable, and converged CC FEA supporting the FEB minimum essential functions under all hazards, to include natural disasters, manmade incidents, terrorism, and war.

DEPARTMENT OF JUSTICE (DOJ)

NS/EP Telecommunications Mission

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

Telecommunications Staff Organization

The Deputy Chief Information Officer, Operations Services Staff (OSS) operates and manages DOJ's consolidated data transport network, law enforcement message processing systems and Telecommunications Services Center. OSS also provides networking and technical assistance to DOJ's offices, boards, divisions and bureaus. Secure interagency message transmission is offered through separate facilities (Defense Message System, and Justice Automated Message System). The Drug Enforcement Administration (DEA), FBI, and United States Marshals Service (USMS) continue to administer their own communications security programs. The Immigration and Naturalization Service has moved to the Department of Homeland Security and the Bureau of Alcohol, Tobacco, Firearms, and Explosives has moved to the Department of Justice.

Current/Ongoing NS/EP Telecommunications Activities

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

- OSS provides representation for DOJ on the NCS Committee of Principals (COP)
- OSS provides representation for DOJ on the Council of Representatives (COR)
- A OSS representative serves on the Telecommunications Service Priority (TSP) Oversight Committee
- DOJ continues its active participation in the NCS activities of the Committee of Principals (NCS)/COP, and participates 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 a number of commercial companies which are either departmental component contractors or engaged in national security and emergency preparedness support in their normal duties (e.g. 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, the department is an active participant in the Government Emergency Telecommunications Service Program, the Wireless Priority Service, the Telecommunications Service Priority Program, and the Shared Resources High Frequency Radio Program.

DEPARTMENT OF THE INTERIOR (DOI)

NS/EP Telecommunications Mission

The Department's mission is to efficiently manage the Nation's natural resources. DOI and the United States (U.S.) Department of Agriculture co-manage the National Interagency Fire Center in Boise, Idaho. It is the Nation's primary emergency support facility for forest fire suppression. It provides 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 are primarily provided by MCI via the General Services Administration FTS2001 contract. DOI is in the process of consolidating its bureau backbone data communications networks to a single Department-wide Multi Protocol Label Switched based architecture with enhanced network security functionality. We are 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 U.S. Department of Agriculture, Justice, Homeland Security, Treasury and others 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 participate in the e-Gov SAFECOM program which will improve interoperability of public safety radio systems.

Key officials, emergency coordinators, and telecommunications managers throughout the Department have Government Emergency Telecommunications Service Cards for long distance emergency telephone communications and Wireless Priority Service. Cellular phones have been provided to key officials in Washington, D.C. Secure Telephone Units, Third Generation, and Secure Terminal Equipment secure telephones are used to support DOI national security programs and high-fidelity backup radio links are used to augment DOI emergency relocation site communications.

DOI SIGNIFICANT ACCOMPLISHMENTS

- Additional DOI Digital Narrowband Contracts were awarded. The National Park Service, Park Police, digital narrowband VHF trunked radio system for the National Capital region design has been completed and submitted to NTIA for approval. A draft MOU with Justice, Treasury and Homeland Security for interoperability with the Integrated Wireless Network is under review.
- Bureau implementations of Microsoft Active Directory are in progress.
- Partial deployment of the Department-wide root directory is completed.
- The Department's consolidated Enterprise Services Network design is completed. Consolidate Internet access points of presence are currently being installed.

U. S. DEPARTMENT OF AGRICULTURE (USDA)

NS/EP Telecommunications Mission

The United States Department of Agriculture (USDA) engages in a number of national security and emergency preparedness (NS/EP) telecommunications activities. These activities support USDA missions to: provide for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment; inspect livestock, poultry, and other products to ensure the safety and wholesomeness of food; and, manage the protection and use of national forests, 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

In 2004 USDA has began coordinating its efforts with the Department of Homeland Security (DHS) to ensure that the Department has access to National Security Administration (NSA) compliant infrastructure for the transmission of secure data communications.

Fiscal Year (FY) 2005 planned activities include: planning for the integration of network infrastructure to support secure data exchange; the development of Departmental guidance for operating and managing NSA-certified equipment and infrastructure; the establishment of equipment and infrastructure standards for secure data transmission; and the incorporation of a secure component into the USDA Enterprise Architecture.

Activities planned for FY2006 will include infrastructure installation between key NS/EP designated sites; the development and implementation of a training program for network administrators, users, and non-cleared personnel; and, the implementation of a pilot.

USDA has replaced over 85% of the original Secure Telephone Units, Third Generation with the Secure Terminal Equipment, and has installed and/or ordered additional units to meet the growing requirements of DHS, Continuity of Operations (COOP) relocation sites, and mission areas. In addition USDA participates in the Cellular Priority Access Service, and is in the process of installing a secure video conferencing system to support Homeland Security requirements. USDA also supports the Government Emergency Telecommunications (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.

The USDA Office of the Chief Information Officer's Telecommunications Services and Operations (TSO) continues to work closely with the COOP Planning Staff to meet Departmental information technology requirements related to COOP activities. During FY 2004, the TSO upgraded COOP related voice systems, enhanced remote connectivity, and installed additional telecommunication infrastructure. For the remainder of FY04, the TSO will enhance the local area network to include Virtual local area network capabilities to better meet COOP exercise requirements. The TSO is investigating alternative voice services such as Voice over Internet Protocol and Internet telephone services as well as enhancing the file, print, and mail services.

NS/EP Partnership Activities

The USDA Forest Service participates in the National Response Plan. The number of emergency and major disaster responses has increased in recent years and the Forest Service expects their level of involvement to remain high. The Forest Service maintains a large cache of radios in the National Interagency Fire Center located in Boise, Idaho. Last year, the Forest Service contributed portable radios to assist in the recovery of the Space Shuttle Columbia representing the 2nd largest use of portable radios from the cache in its history. In 2004 the Fire Radio cache will supply radios for the protection of delegates at the 2004 Democratic Convention.

USDA continues to support SAFECOM, one of the President's top three Electronic Government initiatives focused on interoperable public safety radio communications. In addition to financial contributions, the Department actively participates in SAFECOM's

U. S. DEPARTMENT OF AGRICULTURE (USDA) *continued*

Federal Interagency Coordination Council, the Federal Partnership for Interoperable Communications and the Resources and Federal Funding Coordination Subgroup. The USDA Forest Service has representatives participating in the Standards, Testing and Evaluation of Emerging Technologies, and Training and Technical Assistance Subcommittees.

This year USDA has established a Department-wide Public Safety Land Mobile Radio program called the Agriculture Public Safety Radio System (AgPRS) to: provide better coordination among all intra and inter departmental radio projects; achieve economy of scale in procurement management; achieve cost savings in infrastructure and assets sharing; and provide interoperability capabilities to communicate with other federal, state and local public safety agencies. AgPRS has developed a business case to migrate the Department to next generation radio technologies over the course of the next ten years.

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 America 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. It makes possible the weather reports heard every morning. It facilitates technology that Americans use in the workplace and home every day. It supports the development, gathering and transmitting of information essential to competitive business. It makes possible the diversity of companies and goods found in America's (and the world's) marketplaces. It 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 at the events on 9/11 and the aftermath of that event in support of Homeland Security.

Telecommunications Staff Organization

The DOC manages its telecommunications through the Office of the Chief Information Officer.

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 9/11 environment with the necessary information technology equipment, software and hardware upgrades. Its headquarters in Washington, D.C. has recently implemented a new Emergency Broadcast System (EBS) that can send pre-recorded or ad hoc messages to every Voice Over Internet Protocol telephone in the Herbert C. Hoover Building (HCHB). The EBS alerts users at their desks by turning on lights on the phones and playing audio messages through the phones' speakers and handset. A text message, identical to the audio message, simultaneously appears on the LCD screens of the phones to notify hearing-impaired occupants of the HCHB. This system integrates with the Public Address System, to alert users in common areas of the building such as hallways, bathrooms, and the White House Visitors' Center.

To enhance our Continuity of Operations Planning, the Office of Human Resources Management is currently implementing a new state-of-the-art employee alert, notification, and accountability system titled *The Communicator!* This system automates the current manual notification procedures, through all available communications media. Notification call-outs are activated remotely by phone or directly from the desktop, initiating hundreds, or even thousands of notifications within minutes. The system allows for incoming/outgoing calls in tandem, on-the-fly message recording, a built-in bulletin board feature for inbound status updates, message receipt confirmation, and 24/7 readiness for any notification need. The system also automates employee accountability via the ability to ask qualifying questions during notification call-outs, and record and report on the responses.

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 its use of National Communications System services and programs, especially in light of the tragic 9/11 events and post-9/11 security programs.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

NS/EP Telecommunications Mission

To provide the necessary technical and support capabilities for preparation, mitigation, response, and recovery the U. S. Department of Health and Human Services (HHS) has continued a strong commitment to designing and implementing sound technology that meets the diversity necessary for National Security and Emergency Preparedness telecommunications systems. Each core operating division of HHS has focused on developing and implementing the necessary strategies to provide voice and data systems for:

- Communication on Public Health issues within the Federal Government
- Communication on Public Health issues with State and local cooperators
- Communications on Public Health issues with Non-Governmental Organizations

Providing a mechanism to exchange critical information by voice, video, and data is essential to the Department's mission to manage public health. Future HHS projects will strengthen the Department's efforts with all Governmental and non-Governmental partners in creating an integrated public health architecture that continues to stimulate the sharing of critical data during national and international emergencies. This integration of systems utilizes a strategy that ensures backwards compatibility to other cooperator's legacy systems that may not necessarily utilize the most current standards. These systems support the mitigation and response efforts to natural disasters, and man-made events that require intervention by the Department and the United States Government.

In an effort to increase the ability for global surveillance of public health issues DHHS has collaboratively begun a process to extend communications technologies to the World Health Organization (Geneva), Health Canada, and the Mexican Ministry of Health. These extensions of the Department's capabilities have created a more vigilant environment to discover and analyze emerging public health threats such as Severe Acute Respiratory Syndrome and Avian Influenza.

DEPARTMENT OF TRANSPORTATION (DOT)

NS/EP Telecommunications Mission

Unprecedented transportation challenges in recent years require strong leadership, effective management, and total commitment to the highest standards of public service from the Department of Transportation (DOT). As DOT plans for transportation's future, we acknowledge that the extraordinary events of the past two years have made DOT a more innovative, more agile and more mature organization.

Today, DOT is the architect of the future and is redefining its core mission in light of future challenges to transportation. DOT's core mission emphasizes the national interest in safe and efficient transportation under all circumstances including during times of national security and emergency preparedness incidents. *The Department of Transportation Act of 1966* calls for "…the development of transportation policies and programs that contribute to providing fast, safe, efficient, and convenient transportation at the lowest cost…."

This core mission is valid today and will be valid well into the future even with a global economy where anything can be made anywhere and sold everywhere else around the world. Today, multinational manufacturers source inputs from international suppliers, bring these inputs to production facilities, assemble them and ship them to customers around the globe. Competitive international trade depends on transportation. Disruption of the transportation systems jeopardizes the public safety and disrupts American economic well being.

Transportation is an integrated network consisting of publicly and privately-owned and operated equipment, infrastructure and logistics systems. Increasingly, the equipment—cars, trucks, buses, trains, ships, airplanes, launch vehicles, and pipelines—uses information technology to ensure that the person or good being moved arrives at the right place at the right time. Similarly, the infrastructure—highways, port facilities, airports, space launch and reentry sites, railway and transit stations—is connected by communication and information networks. Improvements in logistics systems sparked by information technology—such as navigation equipment, air traffic control systems, and tracking systems—increase not only the efficiency but also the safety of transportation. The Nation's economic growth and prosperity are dependent upon the synergies of our transportation and information networks.

Developing a strategy for protection of our integrated transportation systems is essential in light of the challenges inherent in a global economy. Americans will require even safer and more efficient domestic and international transportation to support their daily lives, to underpin the economy and to connect the United States to the rest of the world. DOT is committed to a safer, simpler and smarter transportation system for the benefit of all Americans—Safer because we will place greater emphasis on saving lives and reducing accidents than ever before; Simpler because we will improve the management of our resources by consolidating and streamlining programs; and smarter because we will focus on improving efficiency, achieving results and increasing accountability.

Current/Ongoing NS/EP Telecommunications Activities

The Department participates in several ongoing NS/EP telecommunications activities to include: Active participation on the NCS Committee of Principals/Council of Representatives, the President's National Security Telecommunications Advisory Committee, and actively supports NCS NS/EP activities and programs. The Department of Transportation, Office of Chief Information Officer has a resident member on-site at NCS headquarters to serve on the Telecommunications Priority Services Working Group, the Continuity of Communications Working Group, Telecommunications Services Priority Oversight Board and to perform joint outreach activities with NCS in the transportation sector. DOT is working to ensure that it is taking maximum advantage of the various NS/EP programs and services offered by the NCS.

Government Emergency Telecommunications Service (GETS)
The Department has been involved with the NCS GETS program since its inception. GETS cards have been

DEPARTMENT OF TRANSPORTATION (DOT) *continued*

assigned to Regional Emergency Transportation Coordinators and Representatives across the United States and overseas for use during natural disasters and other emergency situations and exercises. The Department has also provided GETS usage sponsorship for State and local Government transportation system officials, as well as key private sector transportation officials. This year the GETS program has been offered to transportation sector industries who are partners with the Federal, State, and local Governments responding to National Security and Emergency Preparedness events.

The Department is also participating in the Wireless Priority Service program to further enhance its emergency communications capabilities. Both T-Mobile cellular and Globalstar satellite handsets have been 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.

Other NS/EP Programs

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

DOT SIGNIFICANT ACCOMPLISHMENTS

- All Operating Administration of DOT participated in the Forward Challenge exercise sponsored by the Departments of Homeland Defense, Federal Emergency Management Agency. DOT developed some specific scenarios of its own that were enacted during the course of the Federal event. The feedback from the participating DOT players was invaluable towards better preparing the Department to respond during emergency situations, continuity of operations, and continuity of government.

DEPARTMENT OF ENERGY (DOE)

Metropolitan Area Network Upgrade

During Fiscal Year (FY) 2004, Headquarters has completed the process of upgrading the DOE Washington, D.C., Metropolitan Area Network, between the Germantown and Forrestal facilities. Past connections on OC-3 and DS-3 asynchronous transfer mode (ATM) circuits using Cisco 8540 ATM switches were upgraded to dual Gigabit Ethernet connections running on an OC-12 SONET ring using Cisco 6513 and ONS optical switches. This upgrade provides increased network performance and availability at reduced cost.

Headquarters has completed its Voice-over-IP (VoIP) pilot using solutions from both Cisco and Nortel, where each system was tested and proven to successfully interoperate with the existing legacy analog phone switch, directly connect out to the public switched telephone network, deploy native Internet protocol telephones across the network, and provide voicemail service accessible from anywhere for end-users. In addition, the pilot confirmed that a single cable plant, with one network connection per user, can provide both voice and data services where user desktop computers are daisy-chained through the VoIP telephone, separating voice and data traffic through the use of 802.1q VLAN tags. Finally, video over IP testing was also performed concurrently with the VoIP pilot to exercise a fully converged network environment simultaneously carrying voice, video, and data traffic.

The switched voice network call completion capability for the Forrestal and Germantown Headquarters buildings has been diversified by splitting the Department's dedicated FTS2001 network access between MCI and AT&T. This arrangement provides physical access infrastructure diversity as well as network switch and network backbone diversity that significantly improves the survivability of Headquarters call completion capability. Headquarters survival call completion capability has also been augmented by the distribution of 404 Government Emergency Telephone System (GETS) calling cards, 24 Satellite Telephone units and Wireless Priority Service for mobile telephones for key personnel.

Bonneville Power Administration

Bonneville Power Administration (BPA) has corrected deficiencies in backup emergency generator power feeds for critical telecommunications equipment at BPA's headquarters building. (This was accomplished during the last building power outage).

The Bonneville Power Administration is currently developing new continuity of operations plans and refining existing plans for the entire agency. Part of this work is identifying telecommunication needs including cell phones, satellite phones, and GETS cards to individuals identified as being key to the operations and restoration of critical systems and any other telecommunications devices.

BPA also began major core network switch replacement project to enhance reliability of agency Local and Wide Area Network. Project estimated completion date: Core switches completed 8/28/2004, outlying access switches 12/30/2004.

DEPARTMENT OF VETERANS AFFAIRS (VA)

Current/Ongoing NS/EP Telecommunications Activities

Wide Area Networking
The Department of Veterans Affairs (VA) is optimizing its corporate wide area network (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. Currently, TMP is extending the enterprise architecture design to each VA facility or campus that has been designated access nodes. The overall TMP implementation is scheduled to be completed by July, 2005.

VA Nationwide Teleconferencing System
The VA Nationwide Teleconferencing System (VANTS) provides full-time 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 the Department of Defense. 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 National Telecommunications and Information Administration in pioneering a Government-wide, classified data exchange beta test that will make the Government Master File 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 high frequency radio system is under engineering review for conversion from the existing analog, shared frequency radio system to the wide-area, digital trunking system provided service to a widely expanded area with a vastly increased capacity for voice, secure voice, and data communications. This VA Trunking System will be integrated into 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 (IG) Network
The VA Radio Frequency Management Office, working with the IG, has completed implementation of a nationwide, narrowband fixed/mobile radio network. The very high frequency 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.

DEPARTMENT OF HOMELAND SECURITY (DHS)

NS/EP Telecommunications Mission

One of the top priorities of DHS is effectively communicating and sharing equipment, in preparation for, or during times of crisis. Since its inception in 2003, the Department has made significant progress in focusing and integrating vast national networks, organizations, and institutions involved in preparing for potential disasters and securing the nation against terrorist threats. In performing this vital role, the Department has the lead responsibility for many of the U.S. Government's most important national communications functions while creating new programs to meet emerging communications needs and requirements at all levels of government.

The Department provides a wide array of communications services to stakeholders across all levels of government, including National leaders, cabinet officials, and Federal agencies with homeland and national security missions. The Department's efforts reach State, local, tribal communities, and public and private sector entities that own and operate critical infrastructure and key resources.

To most effectively carry out the Department's mission and serve these customers, the Department established and maintains several programs to oversee the complex issues involved in improving communications capabilities. Included in this effort is the development of critical infrastructure, communications security, communications equipment, and training.

Current/Ongoing NS/EP Telecommunications Activities

The Department is involved in the following NS/EP-related telecommunications activities:

DHS Wireless Management Office (WMO)
In FY04, the DHS WMO was established to lead a unified effort to move toward an integrated wireless enterprise across the Department. Central to this mission is direct support to the NS/EP communications capabilities of DHS Components, and state and local entities. In FY04, the DHS WMO was involved in the following NS/EP-related activities:

- Supported the Integrated Wireless Network (IWN), a joint initiative between DHS, Department of Justice (DOJ), and Department of the Treasury to provide nationwide interoperability and tactical communications for Federal wireless users
- Partnered in the DOJ 25 Cities Interoperability Project to improve wireless interoperability capabilities in high-threat metropolitan areas
- Initiated the development of operational plans, processes, and procedures for coordinating and managing DHS wireless resources to ensure continuity of operations during crisis situations
- Initiated the coordination of deployable communications assets to improve emergency response across the Department in the event of a national emergency
- Advanced the use of emerging wireless technologies across DHS by incorporating new technologies to assist the investigative and emergency response missions of DHS Components

SAFECOM
SAFECOM, a program within DHS' Science and Technology (S&T) Directorate's Office for Interoperability and Compatibility (OIC), serves as the umbrella program within the Federal Government to help local, tribal, State, and Federal public safety agencies improve emergency response through more effective and efficient interoperable wireless communications. SAFECOM was developed by public safety agencies for public safety agencies and has involved law enforcement, fire, and EMS officials, including the broader public safety community.

SAFECOM's accomplishments include:

- Released version 1.0 of the first Public Safety Statement of Requirements (SoR) for Communications and Interoperability
- Coordinated spectrum policy through participation in the White House Spectrum Policy Task Force

DEPARTMENT OF HOMELAND SECURITY (DHS) *continued*

- Coordinated grant guidance that was subsequently incorporated into the FY04 Community Oriented Policing Services (COPS) awards and FY04 Office for Domestic Preparedness (ODP) awards

- Partnered with the State of Virginia to develop the Statewide Communications Interoperability Planning (SCIP) Methodology, which details phases for developing a statewide interoperability plan

- Worked with industry to learn about new technologies to improve interoperability

National Response Plan
DHS served as the lead agency in the development of the National Response Plan. The National Response Plan establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the Federal Government coordinates with State, local, and tribal Governments and the private sector during incidents.

High Speed Operational Connectivity Program (Hi-SOC)
The Hi-SOC Program provides the underlying network infrastructure to support the Transportation Security Administration's (TSA) mission objectives. The program includes establishing Local Area Network (LAN) connections within an airport and Wide Area Network (WAN) connections between the airport and the TSA Hosting Center, along with intelligent phones and standardized desktop/laptop computer configurations.

The ability to transfer data quickly and securely is paramount to threat mitigation. Several high impact software systems are available, or being developed, that require high speed connectivity to realize their value propositions. These threat mitigation applications include Threat Image Projection System (TIPS), Electronic Surveillance System (ESS), Performance and Results Information System (PARIS), and US VISIT among many others.

National Incident Response Unit/Technical Maintenance Facility (NIRU/TMF)
NIRU/TMF provides rapid deployment support of radio equipment and personnel for emergency response and large event activities (such as the G-8 Summit). This support includes two-way radio support for Immigration and Customs Enforcement (ICE) offices nationwide including distribution, programming, and repair and maintenance of subscriber (handheld and vehicle) and infrastructure radio equipment.

NIRU/TMF support ensures reliable interoffice and inter-agency communications for agents and officers enabling more efficient completion of daily law enforcement duties and enhanced officer safety.

NIRU/TMF provided the following NS/EP support during FY04:

- Distributed over 1400 radio assets and associated equipment to ICE offices totaling over seven million dollars

- Participated in the Unified Tactical Communication Transition Team (UTCTT) and Integrated Project Teams (IPT)

- Provided radio equipment and programming support for the following events:
  - G-8 Summit
  - Republican and Democratic National Conventions
  - Presidential Inauguration

DEPARTMENT OF HOMELAND SECURITY (DHS) *continued*

- Provided radio equipment, programming, and training support for the following:
  - U.S. Secret Service DHS secretary security detail
  - DHS private travel security detail
  - DOJ Office of the Inspector General

Customs and Border Protection (CBP), Tactical Communications Organization (TCO)
CBP TCO operates very high frequency (VHF) and high frequency (HF) radio networks, CBP communications centers, CBP dispatch centers, and a variety of border security systems, such as seismic sensors and remote video cameras. CBP TCO does not have a statutory responsibility for ensuring national communications during crises. However, the assets maintained by CBP TCO can be employed during crises to ensure reliable, secure communications among federal users. Additionally, CBP's HF network is an active participant in the NCS Shared Resources (SHARES) HF radio program.

During FY04, CBP/TCO completed nationwide programming of common radio channels to ensure interoperability among CBP users and in certain locales, between CBP and ICE users.

DHS One Network (One Net)
DHS One Net is a general support system, providing wide-area communications for the service-wide DHS sensitive, but unclassified, environment. One Net will provide continuous monitoring of network activity to detect, analyze, report, contain, and remediate all potential adverse network events and security incidents. One Net is a dual-homed, fully redundant communications vehicle, capable of facilitating network transport from any DHS organization or first responder partner to all DHS constituents in a near real-time and secure manner.

DHS One Net was established in FY05. The Infrastructure Transformation Program/CIOC is now planning for complete transformation of the Day One Network or Data Communication Network to the next generation One Net.

Homeland Security Operations Center (HSOC)
The HSOC collects and disseminates threat information to appropriate intelligence and law enforcement agencies, manages incidents, and maintains domestic situational awareness by communicating information from the state and local level that may have an impact on the national level. The goal of the HSOC is to create a real-time snapshot of the nation's threat environment at any moment to help deter, detect, and prevent terrorist acts. The HSOC utilizes a number of communications technologies to communicate and share NS/EP and threat information. These methods include:

- Homeland Security Information Network (HSIN): An internet-based counterterrorism communications tool, supplying threat information to all 50 states, Washington, D.C., and more than 50 major urban areas

- HSOC staff can apply imagery capability by cross-referencing informational data against geospatial data that can then pinpoint an image down to an exact location using satellite technology

Homeland Security Data Network (HSDN)
In FY04, DHS initiated the development of the HSDN to support the secure transmission of classified information, which is often used to effectively coordinate NS/EP-related events. The HSDN will significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the Department's dependence on networks external to DHS. Looking to the future, the HSDN will be designed to be scalable in order to respond to increasing demands for the secure transmission of classified information among government, industry, and academia crucial to defending America from terrorist attacks.

A Possible Framework for Integrating Crisis-Related Communications Functions and Customers
DHS began a Department-wide initiative using Project Matrix, an IAIP Homeland Security Presidential

DEPARTMENT OF HOMELAND SECURITY (DHS) *continued*

Directive (HSPD)-7 methodology, to identify DHS Component National and mission critical functions/services and the requisite voice, video, and data communications assets required to ensure continuity of operations.

Project Matrix has been aligned with the White House National Essential Function Concept and supports the identification of functions/services and assets at the priority mission essential functions (PMEF) and secondary mission essential functions (SMEF) levels. Project Matrix Step 1 is a criticality assessment, which is a continuity planning practice. Business Impact Analysis is also used to further refine business resumption requirements and identifies recoverable supporting functions/services which Project Matrix Step 1 does not. NS/EP communications must be identified for national (PMEF), mission (SMEF), and support services that require recovery during an emergency.

CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP Telecommunications Mission

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

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

Telecommunications Staff Organization

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

The agency also provides telecommunications support to other United States 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 National Communications System activities of the Committee of Principals/Council of Representatives

Continued support of the Government Emergency Telecommunication Services, the Federal Telecommunications Standards Committee, the Telecommunications Service Priority System, and the Shared Resources High Frequency Radio Program.

CIA SIGNIFICANT ACCOMPLISHMENTS

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

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP Telecommunications Mission

As a major component of the Department of Homeland Security (DHS), FEMA's 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 helps communities to face the threat of terrorism, and the National Preparedness Division ensures that the Nation's first responders are trained and equipped to respond to all types of hazards, including weapons of mass destruction. To benefit from their experience, and to help first responders to be better prepared, EP&R establishes working relationships with State and local first responder and public safety communications associations. EP&R is seeking to improve the response time to Presidentially-declared disasters. The current standard is to set up a disaster field office within 72 hours after the Presidential disaster declaration. The goal is to ultimately reduce the response time to 12 hours.

EP&R currently sponsors ongoing efforts to enhance communications for emergency responders. The full implementation of these efforts is contingent on EP&R's receiving funding. One initiative invloves pilot programs for national warning systems. EP&R is in the process of initiating several pilot programs, including use of the Association for Public Television's bandwidth for reaching the public to disseminate warnings, the upgrade of some stations in the existing Emergency Alerting System to include satellite capability, and the pilot of a reverse 911 system in selected locations. EP&R is also working to establish dedicated channels of communications between Federal Continuity of Operations sites, and to upgrade the central control station for the FEMA National Radio System.

FEMA SIGNIFICANT ACCOMPLISHMENTS

As of August 2004, EP&R has provided telecommunications support for 41 Presidentially declared major disasters and 7 Presidentially declared emergencies. This includes telecommunications support for the ongoing response to Tropical Storm Bonnie and Hurricane Charley in Florida. EP&R has processed 156 Telecommunications Service Priority requests for provisioning circuits during Fiscal Year 2004. EP&R participates in the Government Emergency Telephone System and the Wireless Priority System. In Fiscal Year 2004, EP&R moved the National Disaster Medical System (NDMS) staff into FEMA facilities and accepted responsibility for all NDMS telecommunications. EP&R provided telecommunications support for other components of DHS, including the DHS Office of the Chief Information Officer, Customs, and the Transportation Security Administration.

THE JOINT STAFF (JS)

NS/EP Telecommunications Mission

The Command, Control, Communications and Computer (C4) Systems Directorate (J6) provides advice and recommendations on C4 matters to the Chairman of the Joint Chiefs of Staff and to the Joint Chiefs of Staff. J6 develops policy and plans, monitors programs of joint C4 systems, and ensures adequate C4 support to the National Communications System, Combatant 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.

Telecommunications Staff Organization

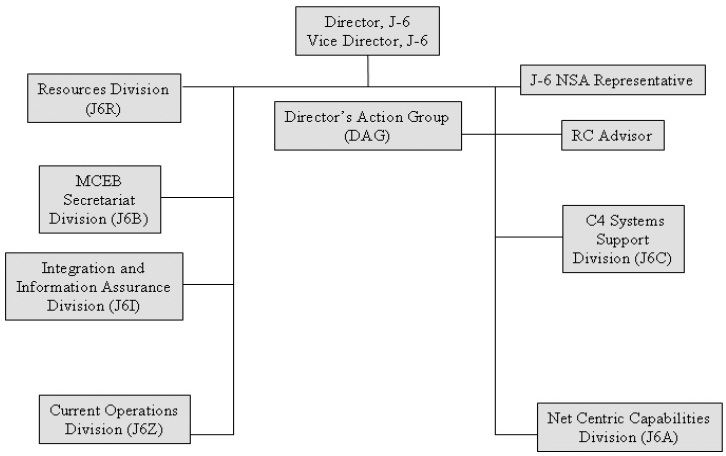
The J6 Directorate is led by the Director and Vice Director. The Director chairs the Military Communications-Electronics Board for the Secretary of Defense. The Director and Vice Director are general/flag officers from the Military Departments. The J6 Directorate includes six functionally aligned divisions,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

Significant Accomplishments
(Refer to Department of Defense (DOD) Section)

Current/Ongoing NS/EP Activities
(Refer to DOD Section)

Pending Issues
(Refer to DOD Section)

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE



JS SIGNIFICANT ACCOMPLISHMENTS

(Refer to DOD Section)

GENERAL SERVICES ADMINISTRATION (GSA)

NS/EP Telecommunications Mission

The General Services Administration (GSA) mission is to help Federal agencies better serve the public by offering, at best value, superior workplaces, expert solutions, acquisition services and management policies.

The GSA Federal Technology Service (FTS) mission is to provide information technology solutions, professional services, and network services that deliver the best value and innovations to support our customers' missions worldwide. The GSA NS/EP missions are specified as provided in following orders and plans:

- Executive Order (E.O) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*
- E.0. 12656, *Assignment of Emergency Preparedness Responsibilities*
- Office of Science and Technology Policy's (OSTP), *National Plan for Telecommunications Support in Non-Wartime Emergencies*
- *National Response Plan*

Current/Ongoing NS/EP Telecommunications Activities

GSA/FTS provides a variety of network services, information technology, and professional services that support federal agencies. These services include local and long-distance voice, data and video telecommunications, building and campus telecommunications infrastructure support, information technology solutions, and professional services.

FTS helps client agencies develop solutions for customers using a variety of contracts. FTS can assist with defining requirements, reviewing alternatives, developing performance based statements of objectives, awarding tasks, project management, and managing project funds.

GSA continues to support the National Communications System and Executive Office of the President, OSTP, and their emergency management programs.

GSA also provides Regional Emergency Communications Planners to provide expert telecommunications advice and services to the NCS, as NCS Regional Managers, and provides support to the Federal Emergency Management Agency (FEMA) during national security emergencies and/or Presidentially-declared disasters.

Other services offered by GSA/FTS included:

- Multi-Tiered Security Profiles, designed to provide enhanced Network Service offerings by integrating various security layers into the current portfolio of contracts
- Access Certificate for E-Services program provides digital certificates and managed PKI services to assist Federal agencies in meeting the requirements of the Government Paperwork Elimination Act

GSA/FTS Significant Accomplishments

- Provided support on continuity of operations (COOP) and NS/EP exercises throughout the country and provided telecommunications support to FEMA in response to several hurricanes
- Supported activities of the Committee on National Security Systems
- Procured Crisis Management Software and tailored this web-based applications program for FTS COOP and NS/EP response personnel during times of crisis for local or national security emergencies. It is an analytical tool featuring exhaustive maps, data sources, educational materials and near-real-time event data
- Supported the Federal Bureau of Investigations Communications Assistance for Law Enforcement Act Group at Chantilly, Virginia with the installation of a nationwide Digital Collection System Network consisting of approximately 61 Private Internet protocol Frame Relay sites
- Supported the Judiciary's Administrative Office (AO) of the U.S. Courts' COOP requirements for the Court

GENERAL SERVICES ADMINISTRATION (GSA) *continued*

Operations Support Center facility. It will house all the AO's critical data communications systems and staff, designed to secure their computer systems and maintain data integrity in case of an emergency or national disaster

- Provided the telecommunications support for the Department of Justice Immigration and Naturalization Service and the Department of Homeland Security backbone network, as well as the U.S. Customs Services' Managed Router Network, which ties into the DHS classified network

- Implemented the Department of the Interior (DOI) TrustNet, a new secure information technology infrastructure for Indian trust data. DOI utilized FTS2001 Managed Network Services to provide a total solution, and Multi-Tier Security Profiles to fulfill security and meet NS/EP requirements

GSA/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 Executive Order 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 Operations has programmatic responsibility for representing the organization, on behalf of the Administrator, in the National Communications System (NCS) process. The Associate Administrator for Space Operations assigned the Assistant Associate Administrator for Space Communications as NASA's Committee of Principals 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:

- Telecommunications Service Priority, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, and the National Telecommunications Management Structure

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

NASA NS/EP Telecommunications Assets

NASA NISN supports both space flight 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 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

- Transitioned NASA's wide-area network circuit and service contracts to General Service Administration contract vehicles.
- Initiated planning to replace both the mission and non-mission wide area network infrastructures and NASA's mission voice switches.
- Deployed resources to assist in the recovery and investigation of the Columbia shuttle disaster and provided services to support the Shuttle's return to flight.

NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP Telecommunications Mission

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

The Commission's NS/EP telecommunications provide for highly reliable connectivity between the NRC Operations Center, operating nuclear power plant control rooms, emergency operations facilities, and regional incident response centers. This connectivity ensures immediate notification to the NRC Operations Center of unusual occurrences and provides relevant information during accidents/events at NRC licensed facilities.

Current/Ongoing NS/EP Telecommunications Activities

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 throughout the country. Every location that supports ETS using FTS 2001 has Telecommunications Service Priority (TSP) coverage assigned to at least one circuit. There are 23 locations that do not support ETS through FTS 2001. Instead, they use their own corporate communication systems to meet the requirement.

The Government Emergency Telecommunications Service (GETS) continues to be highly recommended by NRC as a means of enhancing access to long distance service. NRC's participation in the program continues to increase. NRC and NCS are currently working together to optimize existing communications between NRC and nuclear plant licensees. A secure communications capability is established at NRC and nuclear plants. In the future, however, NRC would like to add a secure teleconferencing capability.

NRC SIGNIFICANT ACCOMPLISHMENTS

Secure Video Teleconferencing (SVTC) System

- NRC has successfully established a SVTC system in the Headquarters Emergency Operations Center and is working toward expanding that capability to all of the NRC regional incident response centers

Critical Warning Infrastructure Network (CWIN)

- NCS is currently in the midst of installing a new CWIN terminal at NRC's HQ Emergency Operations Center. The CWIN terminal is expected to be ready for use in October 2004

GETS

- 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 407 to 470 during this reporting period

TSP

- 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 Executive Orders 12046, 12472, and 12656 includes serving as the Executive Branch telecommunications policy adviser to the President, serving as the manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board. Thus, among other things, NTIA advises and assists the President in 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 its efforts to develop a United States (US) spectrum policy for the 21st century in response to the President's Spectrum Policy Initiative of May 2003. OSM developed a spectrum policy reform initiative workplan to guide its efforts in this regard. OSM's vision is to use information technology to automate the spectrum management business processes and minimize human intervention for routine actions. Specific examples of activities in support of the foregoing include the following:

- Updated and implemented various planned outcomes and improvement goals in the NTIA Federal Spectrum Management System/Information Technology Improvements Plan
- Established an OSM Enterprise Architecture Council to develop requirements and an implementation plan to satisfy the IT requirements of the Federal spectrum management community
- Initiated a memorandum of agreement with the Federal Communications Commission and the Department of Defense's (DOD) Joint Spectrum Center to leverage resources available to develop common spectrum management systems and approaches as appropriate
- Continued to partner with DOD Joint Spectrum Center to develop and field improvements to the SPECTRUM XXI Version 4.0 and other automated capabilities for use by all Federal spectrum managers
- Continued 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
- Continued to develop, field, and maintain several spectrum management automation tools for use by Federal spectrum managers to more effectively manage use of the radio frequency electromagnetic spectrum during NS/EP and normal conditions

In addition, NTIA:

- Provided a Co-Chair of the Government Emergency Telecommunications Service (GETS)/Wireless Priority Service 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 continuity of operations
- Participated in various activities and endeavors of the President's National Security Telecommunications Advisory Committee
- Participated in National Communications System (NCS) Committee of Principals (COP) and Council of Representatives activities and endeavors to include the NCS COP Priority Services Working Group and Continuity Communications Working Group
- Participated in NCS Shared Resources High Frequency Coordination Network Interoperability Working Group activities and endeavors

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) *continued*

NTIA SIGNIFICANT ACCOMPLISHMENTS

- Conducted over 200 meetings of the Interdepartment Radio Advisory Committee 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 US Government on many spectrum policy matters at various meetings of International Telecommunication Union working groups, study groups, and more.

NATIONAL SECURITY AGENCY (NSA)

NS/EP Telecommunications Mission

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

Information Technology (IT) And Information Assurance (IA) Organizations

Within NSA, two organizations share responsibility in supporting NS/EP related activities. The IT Infrastructure Services group is responsible for planning and operating the telecommunications systems and networks linking Agency elements worldwide, and for providing Agency connectivity to other Government services.

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

Current/Ongoing NS/EP Telecommunications Activities

National Security Incident Response Center

The National Security Incident Response Center (NSIRC) provides expert assistance to the national security community regarding computer network defense. This was accomplished through 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 to provide all-source threat reporting on Signals Intelligence threats to operations, exercises, information systems and force protection.

Global Information Grid

The Office of the Assistant Secretary of Defense Networks and Information Integration tasked NSA with developing an end-to-end IA perspective for the Global Information Grid (GIG). NSA Delivered version 1.0 of the end-to-end IA Component of the GIG Integrated Architecture.

Crypto-Modernization Initiative

The Crypto-Modernization Initiative is a Department of Defense-directed/NSA -led effort to transform and modernize IA capabilities for the 21st century. The Initiative continues toward the modernization of the DOD's IA capabilities to replace an aging cryptographic product inventory, meet increased interoperability requirements, keep pace with information technology evolution and achieve the vision of Defense in Depth.

Electronic Key Management System

Phase 4 of the electronic key management system (EKMS)—the multi-tiered, distributed key management system designed to generate and distribute electronic key and automate the management of physical key and cryptographic equipment—has achieved an initial operational capability.
Establishment of Phase 4 operations at the Central Facility was a major milestone in the overall EKMS effort to deploy thousands of EKMS workstations and consolidate the control of Service cryptographic key and equipment at the Tier 1 nodes.

Information Assurance Technology Development and Rollout

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

High Assurance Internet Protocol Encryption

Working towards securing the high-speed transport pipe with 100 Mbps High Assurance Internet HAIPE Inline Network Encryptors with migration to 1Gbps and 10 Gbps encryptors.

Security Assessments

NSA continues to perform security assessments to evaluate the security of both information systems and operations. Security assessments can include IA assessments, network technology analysis, technical security evaluations, Technical Security Countermeasures Operations and TEMPEST accreditation service.

U.S. POSTAL SERVICE (USPS)

NS/EP Telecommunications Mission

The Postal Service delivers more than 200 billion pieces of mail a year to over 141 million homes, business and post office boxes. In support of that effort, the USPS maintains one of the largest computing infrastructures in the world.

Every day the Information Technology (IT) organization gets the job done—securely, efficiently, and economically.

The U.S. Postal Service 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.

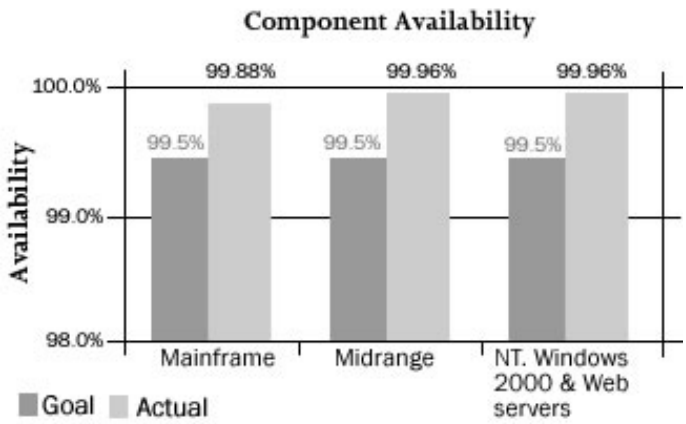
FY 2004 Infrastructure Components	Quantity
Desktops and Notebooks	128,225
Integrated Retail Terminals	17,880
Point Of Service Workstations	42,996
Handheld Scanners	331,231
Remote Dial-up Accounts	20,000
Virtual Private Network Connections (Cable/Broadband)	8,000
Satellite Connections	11,975
Routers	14,480
Internal E-Mail Users	163,000
Internal Emails Annually	1,508,000,00
National Applications	650
Visits to usps.com	256,200,00

USPS SIGNIFICANT ACCOMPLISHMENTS

Upgrading The Infrastructure

IT has established a modernized Postal Service distributed computing infrastructure. The Advanced Computing Environment (ACE) initiative was completed in 2004, ahead of schedule and under budget. The ACE model supports the following features:

- a standard suite of software products for all users
- efficient and responsive remote help desk support
- rapid deployment of software enhancements, including security protections against virus intrusions and network disruptions
- rapid delivery of new products and services
- reduced development, maintenance, and support costs



The new ACE model provides IT managers more efficient operational oversight through central hosting of applications. Standardizing these applications allows the organization to streamline application management procedures and future system integrations. In establishing the new model, IT converted 147 national applications to ACE and retired or converted 574 local applications. IT migrated over 130,000 employee workstations to ACE and removed over 12,000 servers from field sites.

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

USPS SIGNIFICANT ACCOMPLISHMENTS

IT also identified over 2,000 unregistered web sites, Commercial off-the-Shelf (COTS) products, and non-ACE related items in use in the Postal Service system. IT then either consolidated or eliminated them from its system. This initiative will be ongoing as will be the cost savings it is expected to generate.

Universal Computing Connectivity
The Universal Computing Connectivity initiative will provide always available connectivity to the Postal Service computing environment to those Postal Service managers and employees whose jobs require such access. The program involves the development of a system-wide network that combines voice, data, and video in a single design.

The Postal Service recognizes that as the organization and general commerce evolve, new advanced information services will be necessary to meet new or changed requirements, to improve performance and reliability, and to reduce operating expenses. To ensure that the Postal Service will continue to employ current telecommunication services, IT has issued a solicitation known as the Universal Computing Connectivity contract. Under the contract, all telecommunication services and features that will be available to the Postal Service shall evolve and be increased, enhanced, and upgraded as changes take place in the telecommunications industry. IT anticipates awarding this new contract and finalizing planning for its use by October, 2004.

In 2004, IT enhanced and expanded the infrastructure of its BlackBerry system. This wireless communications system provides remote communications capability to more than 4,000 Postal Service managers and Continuity of Operations team members, even when Postal Service facilities are without power or shut down. The BlackBerry system now includes additional functionality and twice the coverage area. By early 2005, the system will have an end-to-end remote administration capability.

In 2004, IT upgraded the bandwidth at more than 6,000 locations to improve system performance when employees are connected to the network. IT has also upgraded 2,700 local area networks throughout the infrastructure for improved performance.

Enterpise Data Warehouse
The Enterprise Data Warehouse (EDW) is a major information asset of the Postal Service. Initiated as a repository for key retail information and transactions, EDW is now the central source of information on retail, financial and operational performance.

Over the past year, use of EDW has grown from a few hundred individual users who generated approximately 600 reports per week to over 3,000 users creating more than 40,000 reports per week. To manage this growing data environment and to assure the business value of EDW initiatives and the consistency and quality of its data, IT created an EDW governance infrastructure in 2004. Recent improvements in the efficiency of frequently executed reports, as well as a planned upgrade to the EDW infrastructure, will enable IT to meet the challenge of EDW's rapid growth and institutionalization.

IT continues to add new data sources to EDW, focusing particularly on those systems that manage the movement of mail. In 2004, IT added Delivery Confirmation data, and plans are underway to add other sources, such as International Mail.

Enhancing Security
During Fiscal Year (FY) 2004, the USPS Information Technology Corporate Information Security Office (CISO) made significant progress in creating a climate where employees, customers, and partners understand that security brings real business value to our products and services. The Postal Service had no significant breaches or viruses that could have prevented us from serving our customers or conducting our day-to-day business functions.

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

USPS SIGNIFICANT ACCOMPLISHMENTS

Also during FY 2004, the Postal Service designed and put into operation 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; and
- Robust patch management oversight to ensure operating system and application fixes are applied in a timely manner to prevent exploitation of commonly known vulnerabilities.

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

The need to preserve the privacy and security of information that customers and others provide and the Postal Service uses in the course of its operations have resulted in a variety of security initiatives that include:

- The increased use of employee identification numbers in Postal Service applications and forms to reduce the reliance on Social Security Numbers and thus protect the privacy of employees' personal information.
- The implementation of a wireless infrastructure that controls the number and type of wireless access points and ensures that users and devices are authenticated and authorized before accessing the system, and that appropriate levels of encryption are employed to protect sensitive data.

Protecting Postal Service information resources from threats and ensuring the integrity of Postal Service applications and technologies. Such measures cover a lot of territory:

- Over 13 million Internet email messages scanned monthly for viruses.
- Over 55 billion network data packets scanned monthly for evidence of intrusion.
- Over 52,000 employees 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 the Department of Defense 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 over 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.
- The Postal Service has also worked closely with DOD to ensure that mail destined to our troops Iraq and Afghanistan keeps flowing from home.

FEDERAL RESERVE BOARD (FRB)

NS/EP Telecommunications Mission

The FRB's national security and emergency preparedness (NS/EP) responsibilities relate to the maintenance of the national 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 considers essential services and systems related to the national economic posture to include: critical funds transfer systems (wholesale/large-value payment systems); securities and derivatives clearing and settlement systems; supporting communications systems and service providers; and key financial market trading systems and exchanges.

Telecommunications Staff Organization

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

Current/Ongoing NS/EP Telecommunications Activities

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial telecommunications infrastructure and payment systems. The FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential telecommunications services supporting large-value payment systems, large-value clearing and settlement systems, major financial services exchanges and utilities, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. In addition, the FRB administers the TSP program for financial service organizations sponsored by the Securities and Exchange Commission (SEC), Office of the Comptroller of the Currency (OCC), Commodities and Futures Trading Commission (CFTC), National Credit Union Administration (NCUA) and the Office of Thrift Supervision (OTS).

The FRB sponsors the Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) for Federal Reserve Banks, depository institutions, key participants in the Nation's payment systems, and those foreign central banks that are critical to the maintenance of the Nation's economic posture.

The FRB continues to provide outreach to those financial institutions that support NS/EP functions and actively participates in NCS initiatives to enhance the resiliency of the Nation's financial telecommunications infrastructure.

By the end of Fiscal Year (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, 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 RESERVE BOARD (FRB) *continued*

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;

- The automated auction processing system for Treasury securities, and critical central bank functions circuits used by other payment systems (for example, the Society for Worldwide Interbank Financial Telecommunications and the Clearing House Interbank Payments System) that meet the FRB's eligibility criteria 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;

- Other qualifying financial service utilities circuits used by ACH operators and the CLS bank that meet the FRB's eligibility criteria circuits connecting customers of sponsored payment system, foreign exchange, and clearing and settlement utilities that meet the FRB's eligibility criteria circuits used by capital and futures exchange utilities; and

- Key participants that meet the SEC and CFTC eligibility criteria circuits used by market data providers that supply critical information needed by financial institutions circuits used by the World Bank to ensure continuity of operations.

By the end of FY 2004, there will be approximately 3,500 active TSP assignments including circuits directly sponsored by the FRB as well as those circuits administered for the SEC, OCC, CFTC, NCUA and OTS. 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 this fiscal year, the FRB will have sponsored approximately 48 institutions. During the last fiscal year, the FRB continued to participate in the evolution of the Wireless Priority Service (WPS) program. The FRB has sponsored 10 institutions for WPS with approximately 85 users currently enrolled in the service. There are approximately 60 pre-orders being held for WPS service that will be activated when WPS is expanded to additional cellular carriers.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

NS/EP Telecommunications Mission

The FCC national security and emergency preparedness (NS/EP) responsibilities include:

- Evaluating and strengthening measures for protecting U.S. telecommunications, broadcast and other communications infrastructure and facilities
- Ensuring rapid restoration of U.S. telecommunications, broadcast, and other communications infrastructure and facilities after disruption by a terrorist attack or natural disaster
- Ensuring 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, 2001 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 National Communications System (NCS) to develop an outreach program designed to ensure that the nation's 911 centers (Public Safety Answering Points) are registered in the Telecommunications Service Priority (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 required 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 E-911
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

A

AAA	Authentication, Authorization, and Accounting
ACE	Advanced Computing Environment
ACH	Automated Clearing House
ACN	Alerting and Coordination Network
ACR	Alternate Carrier Routing
AGCS	AG Communications Systems
AgPRS	Agriculture Public Safety Radio System
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
AO	Administrative Office
AOF	Alternate Operating Facility
ASD (HD)	Assistant Secretary of Defense for Homeland Defense
AT	Advanced Technology
ATM	Asynchronous Transfer Mode

B

BCIS	Bureau of Citizenship and Immigration Services
BDT	Backup Dial Tone
BGP	Border Gateway Protocol
BPA	Bonneville Power Administration

C

C4	Command, Control, Communications and Computer Systems
C&A	Certification and Accreditation
CAC	Connection Admission Control
CC	Continuity Communications
CC EA	Continuity Communications Enterprise Architecture
CCP	Classified Connectivity Program
CCPC	Civil Communications Planning Committee
CCWG	Continuity Communications Working Group

CDMA	Code Division Multiple Access
CFTC	Commodity Futures Trading Commission
CFWG	Critical Facilities Working Group
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CI/KR	Critical Infrastructure/Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISEN	Centro de Inteligencia y Seguridad Nacional
CISO	Corporate Information Security Office
CLEC	Competitive Local Exchange Carriers
CLS	Continuous Linked Settlement
CNSS	Committee for National Security Systems
COG	Continuity of Government
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CSC	Computer Sciences Corporation
CWIN	Critical Infrastructure Warning Information Network

D

DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DO	Departmental Offices
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DS	Diplomatic Security
DTS	Diplomatic Telecommunications Service

E

EA	Enterprise Architecture
EBS	Emergency Broadcasting System
EDW	Enterprise Data Warehouse
EKMS	Electronic Key Management System
eMLPP	enhanced Multi-Level Precedence and Preemption
EMP	Electromagnetic Pulse
ENM	Enterprise Network Management

E.O.	Executive Order
EOC	Emergency Operations Center
EOP	Executive Office of the President
EP&R	Emergency Preparedness and Response Directorate
ERLink	Emergency Response Link
ERT	Emergency Response Training
ESF	Emergency Support Function
ESOC	Enterprise Server Operation Center
ETS	Emergency Telecommunications System

F

FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FEB	Federal Executive Branch
FEMA	Federal Emergency Management Agency
FOC	Full Operational Capability
FRB	Federal Reserve Board
FSO	Free Space Optics
FSTF	Financial Services Task Force
FTP	Federal Technology Program
FTS	Federal Technology Service
FTS2001	Federal Technology Service 2001
FWUF	Federal Wireless Users' Forum
FY	Fiscal Year

G

GETS	Government Emergency Telecommunications Service
GEWIS	Global Early Warning Information System
GIG	Global Information Grid
GITM	Global IT Modernization
GN	Ground Network
GNSOC	General 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

HCHB	Herbert C. Hoover Building
HF	High Frequency
HHS	Department of Health and Human Services
HIDS	Host-Based Intrusion Detection Systems
HLR	Home Location Register
HPC	High Probability of Completion

HSPC	Homeland Security Policy Council
HSPD-7	Homeland Security Presidential Directive 7
HSTL	Homeland Security Telephone Link

I

IA	Information Assurance
IAIP	Information Analysis and Infrastructure Protection
IAM	Initial Address Message
IC	Integration Contractor (Section III)
IC	Intelligence Community (Section IV)
ICD	Infrastructure Coordination Division
IDS	Intrusion Detection System
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMA	Individual Mobilization Augmentee
IMF	Internet Modeling Framework
INE	Inline Network Encryption
INEEL	Idaho National Environmental and Engineering Lab
INFOSEC	Information Security
IOC	Initial Operating Capability
IP	Internet Protocol
IR	Industry Requirements
IRM	Bureau of Information Resource Management
ISAC	Information Sharing and Analysis Center
ISAS	Information Sharing and Analysis System
ISP	Internet Service Provider
IT	Information Technology
ITU-T	International Telecommunication Union, Telecommunications Sector
IWG	Interoperability Working Group
I-WPS	Immediate Wireless Priority Service
IXC	Interexchange Carrier

J

J6	Command, Control, Communications, and Computer Systems Directorate
JCS	Joint Chiefs of Staff
JTRS	Joint Tactical Radio System

L

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

M

MSC	Mobile Switching Center

N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCR	National Capital Region
NCS	National Communications System
NCSD	NCS Directive (Section III-37)
NCSD	National Cyber Security Division (Section III-19)
NCUA	National Credit Union Administration
NDAC	Network Design and Analysis Capability
NDMS	National Disaster Medical System
NGN	Next Generation Networks
NGNTF	Next Generation Networks Task Force
NGO	Non-Governmental Organizations
NICC	National Infrastructure Coordination Center
NIIF	Network Interconnection Interoperability Forum
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NOTF	NSTAC Outreach Task Force
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
NSSE	National Special Security Event
NSTAC	President's National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
NTRWG	Near Term Recommendations Working Group

O

OA	Operational Analysis
OC	Oversight Committee
OCC	Office of Comptroller of Currency
OCIO	Office of the Chief Information Officer
ODP	Office of Domestic Preparedness
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPT	Office of Priority Telecommunications
OSD	Office of the Secretary of Defense
OSI	Open System Interconnection
OSIS	Open Source Information System
OSM	Office of Spectrum Management
OSSS	One-Stop Shop Service
OSS	Operations Services Staff
OSTP	Office of Science and Technology Policy
OTS	Office of Thrift Supervision

P

PAS	Priority Access Service
PBX	Private Branch Exchange
PD	Public Diplomacy
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
PN	Public Network
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PSWG	Priority Services Working Group
PT&E	Planning, Training, and Exercise Branch
PTS	Priority Telecommunications Services

Q

QoS	Quality of Service

R

R&D	Research and Development
R&O	Report and Order
RDTF	Research and Development Task Force
RDX	Research and Development Exchange

RFI	Request for Information

S

SAFECOM	Wireless Public Safety Interoperable Communications Program
SAFETY Act	Support Anti-Terrorism by Fostering Effective Technologies Act
SARS	Severe Acute Respiratory Syndrome
SATCOM	Satellite Communications
S-BGP	Secure Border Gateway Protocol
SBU	Sensitive But Unclassified
SCADA	Supervisory Control and Data Acquisition
SEC	Security and Exchange Commission
SHARES	Shared Resources
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SMART	State Messaging and Archive Retrieval Toolset
SME	Subject Matter Expert
SMS	Short Messaging Service
SOC	Security Operations Center
SS7	Signaling System 7
SSU	Standing Subcommittee on Upgrades
STE	Secure Terminal Equipment System
STF	Satellite Task Force
STU III	Secure Telephone Units, Third Generation
SVTC	Secure Video Teleconferencing

T

TAL	Technology Assessment Laboratory
TATF	Trusted Access Task Force
TCS	Treasury Communications System
TEDE	Telecommunications Electromagnetic Disruptive Effects
TIA	Telecommunications Industry Association
TREAS	Department of Treasury
TSA	Transportation Security Administration
TSO	Telecommunications Services and Operations
TSP	Telecommunications Service Priority

U

USAID	United States Agency for International Development
USDA	U.S. Department of Agriculture
USPS	U.S. Postal Service

V

VA	Department of Veterans Affairs
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

W

WAO	Watch Analysis Office
WARN	Washington Area Radio Network
WPS	Wireless Priority Service


NATIONAL COMMUNICATIONS SYSTEM
NCS