Fiscal Year 2006 Report

National
Communications
System

NATIONAL COMMUNICATIONS SYSTEM

Ensuring Essential Communications for the Homeland

Prepared by the Office of the Manager,
National Communications System

FOREWORD

The most destructive natural disaster in United States history—Hurricane Katrina—marked its one-year anniversary on August 29, 2006. While challenges still remain in recovering from this tragedy, the Department of Homeland Security (DHS) has moved aggressively to address communications enhancements, including implementation of actionable solutions to address problems. Concurrently, the Department has continued its focus on also ensuring a robust national security communications capability. Accordingly, NCS worked diligently with its member agencies and industry partners to enhance national security and emergency preparedness (NS/EP) telecommunications response, recovery, and coordination procedures and capabilities.

Over the past year, NCS led numerous activities to better prepare for the 2006 hurricane season. As the primary agency supporting the National Response Plan's Emergency Support Function 2 (ESF-2)—Communications, many of NCS's efforts focused on improving its capabilities to better meet these responsibilities. These efforts included revising the ESF-2 Operations Plan; developing and implementing an ESF-2 Training and Response Improvement Program; and working with the ESF community to assess the Government's ability to ensure industry priority access to fuel, security, temporary housing, and temporary staging sites for emergency responders. Additionally, NCS is engaging in activities to improve its response capabilities and the emergency communications infrastructure. These activities consist of assuming the lead coordination role in the development of the interim *National Emergency Communications Strategy* as required by the White House's *The Federal Response to Hurricane Katrina: Lessons Learned* Report; developing the plans for deploying a reliable communications capability for emergency responders; inventorying the communications-related solutions available in the public and private sectors; and developing a Communications Asset Database to store this information so it may be promptly located and used when needed.

NCS also worked diligently with its Federal and industry partners to develop solutions to ensure the resiliency of the telecommunications infrastructure. On December 8, 2005, representatives from DHS and NCS met with members of the President's National Security Telecommunications Advisory Committee (NSTAC) to discuss Hurricane Katrina response challenges and to identify actions that industry could undertake to assist in meeting those challenges. Moreover, NCS is working closely in partnership with Federal, State, and local government entities as well as the private sector to develop an access standard operating procedure and ensure that private-sector critical infrastructure responders receive priority access to disaster areas.

Furthermore, NCS made impressive advances in its technological programs and services. While continuing to provide priority services to the NS/EP communications user base, NCS also aggressively pursued the migration of its existing priority services to next-generation networks. One such example involved the exploration of NS/EP priority services within the next-generation networks environment through participation in a Next Generation Priority Services Experimental Testbed Environment. Through an extensive outreach program, NCS promoted its existing priority services to potential new customers across Federal, State, and local governments. Additionally, the Wireless Priority Service (WPS) was expanded through the addition of new users and the continued deployment of WPS capabilities in Code Division Multiple Access. Supporting its strong modeling, analysis, and assessment capability, NCS designed an Abridged Route Diversity Methodology to enable agencies to provide critical infrastructure self-assessments. A Route Diversity Forum was held with communications officials from Federal departments and agencies to socialize route diversity methodologies and findings.

Additionally, the NCS Committee of Principals assumed a significant advisory role and provided interagency coordination in the establishment of a National Command and Coordinating Capability in support of continuity communications. During this time, NCS initiated efforts to analyze the ability of Federal departments and agencies to interoperate and effectively perform their primary mission-essential functions under all circumstances in support of continuity communications. The end result will be a continuity communications architecture (CCA) that will support the ability of the Executive Office of the President to respond deliberately and appropriately to any crisis. The CCA assures responsive, reliable, and survivable communications processes and systems to support command and coordination of operations among Federal, State, and local governments, as well as private organizations, foreign governments, and international entities, as needed.

NCS built upon its already extensive relationships with industry and government partners by serving as Executive Secretary for and participating in numerous meetings of the NSTAC, the NCS Committee of Principals and Council of Representatives, the National Coordinating Center (NCC), the Communications Information Sharing and Analysis Center, and the Network Security Information Exchanges. These relationships promote the sustained sharing of information between industry and Government, currently unparalleled across the public and private sectors.

NCS—as the designated Communications Sector Specific Agency (SSA)—worked with members of industry to support the establishment of the Communications Sector Coordinating Council (CSCC) while serving as the Chair for the Communications Government Coordinating Council (CGCC). As the SSA, NCS worked closely with the CSCC and CGCC to develop and complete the Communications Sector Specific Plan. Furthermore, NCS coordinated with NCC industry members to develop an emergency wireless protocol to support the termination of cellular network connections when emergency circumstances warrant and the restoration of services following the emergency.

These activities, over a very short period of time, have transformed NCS's response and recovery capabilities and represent a significant improvement in the Federal Government's preparedness. Through its many efforts, NCS remains dedicated to its mission to ensure essential telecommunications services in the face of both *national* and *homeland* security threats, and I would like to personally recognize the extraordinary efforts of the NCS staff members who have worked diligently to ensure that lessons learned are also lessons implemented.

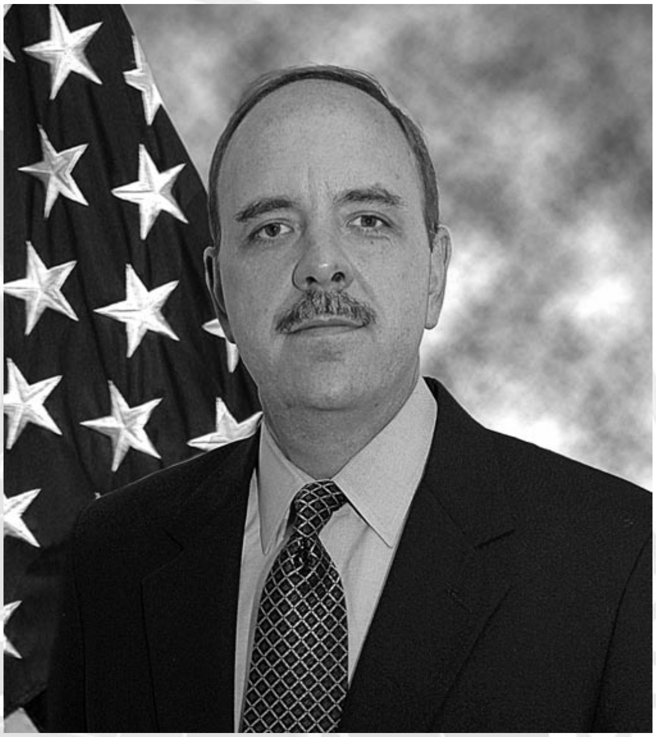
George W. Foresman

George W. Foresman
Manager, NCS

NCS Leadership

Mr. Robert S. Zitz
Principal Deputy Manager

Mr. Gregory T. Garcia
Deputy Manager

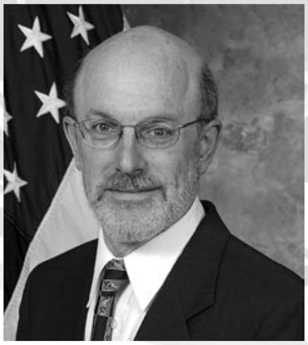


The Honorable George W. Foresman
Manager

Dr. Peter M. Fonash
Deputy Manager and Director

Col. Victoria A. Velez, USAF
Chief of Staff

Mr. Gary D. Amato
Chief
Technology and Programs Division



Mr. Jeffrey A. Glick
Chief
Critical Infrastructure Protection Division

Mr. James G. Bittner
Chief
Plans and Resources Division

Mr. Thomas J. Falvey
Chief
Customer Service Division

NCS Committee of Principals

Department of State (DOS)
Mr. James Van Derhoff

Department of the Treasury (TREAS)
Mr. Ken Ricinni

Department of Defense (DOD)
Dr. Linton Wells

Department of Justice (DOJ)
Mr. Kent Holgrewe

Department of the Interior (DOI)
Mr. Timothy Quinn

Department of Agriculture (USDA)
Ms. Janice Lilja

Department of Commerce (DOC)
Mr. William Lay

Department of Health and Human Services (HHS)
Mr. Gary Wall

Department of Transportation (DOT)
Mr. Robert Schmidt

Department of Energy (DOE)
Mr. Harry Hixon

Department of Veterans Affairs (VA)
Mr. David Cheplick

Department of Homeland Security (DHS)
Mr. Anthony Cira

Federal Emergency Management Agency (FEMA)
Mr. Rex Whitacre

The Joint Staff (JS)
VADM Nancy Brown, USN

General Services Administration (GSA)
Ms. Margaret Binns

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

Nuclear Regulatory Commission (NRC)
Mr. Melvyn Leach

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

National Security Agency (NSA)
Mr. Morris Hymes

United States Postal Service (USPS)
Mr. Harold Stark

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)
Ms. Vicki Waizenegger

Department of Defense (DOD)
Maj. Patrick Ryder, USAF

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. David Jarrell

Department of Health and Human Services (HHS)
Mr. Gary Wall

Department of Transportation (DOT)
Mr. Michael Dammeyer

Department of Energy (DOE)
Mr. David Biser

Department of Veterans Affairs (VA)
Mr. David Cheplick

Department of Homeland Security (DHS)
Mr. Julio Murphy

Federal Emergency Management Agency (FEMA)
Ms. Jeanne Etzel

The Joint Staff (JS)
Maj. Susan Caromoda, USA

General Services Administration (GSA)
Mr. Douglas Covert

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

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

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

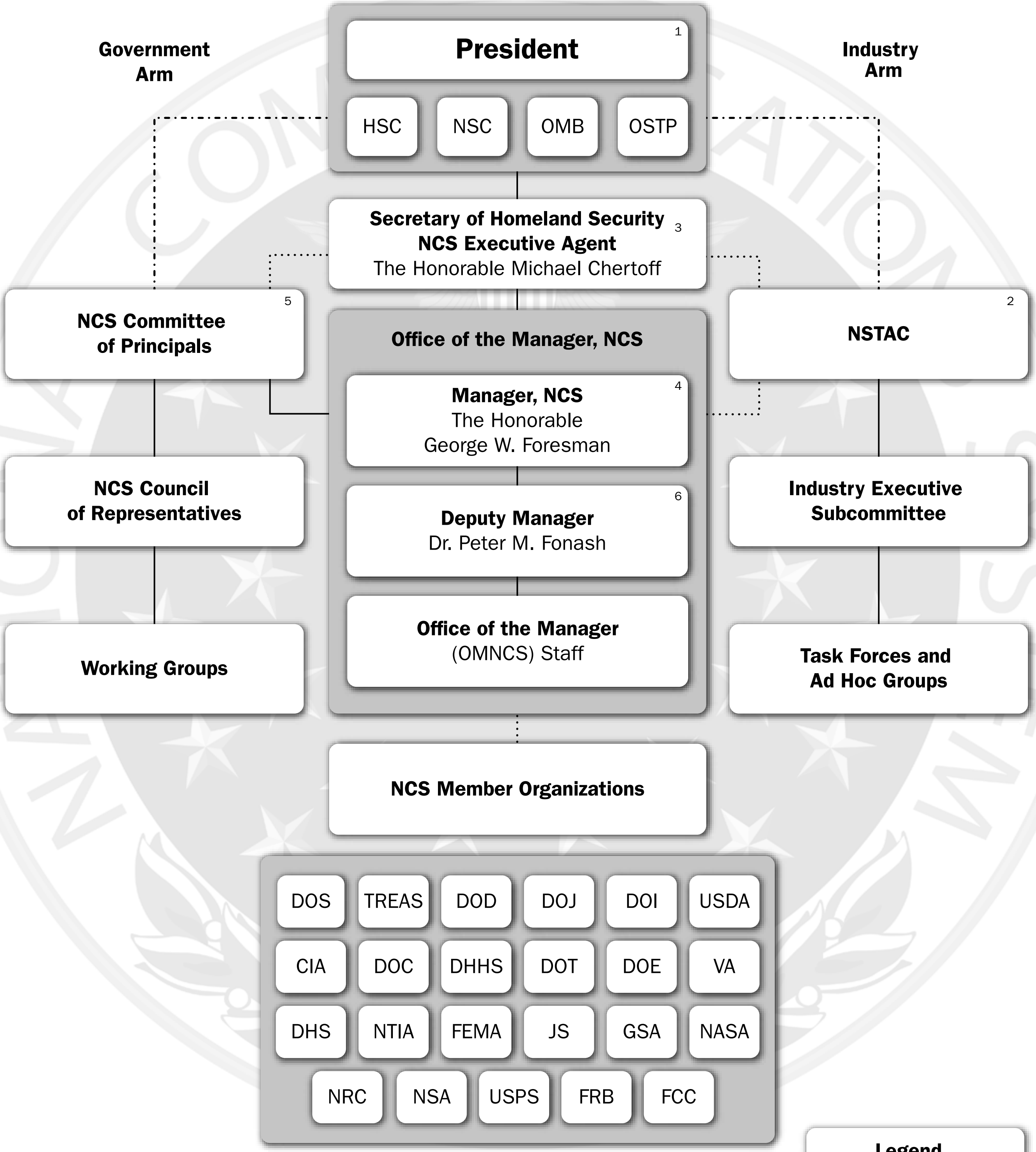
National Security Agency (NSA)
Mr. Anthony Cornish

United States Postal Service (USPS)
Mr. Warren Schwartz

Federal Reserve Board (FRB)
Mr. Wayne Pacine

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

THE NCS STRUCTURE



1. Policy Direction and Direct Execution of War Powers Function
2. The President's National Security Telecommunications Advisory Committee created by Executive Order 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

TABLE OF CONTENTS

Page Number

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, reports on national security and emergency preparedness (NS/EP) activities and telecommunications events, and highlights the agency's innovations, programs, and achievements during fiscal year (FY) 2006.

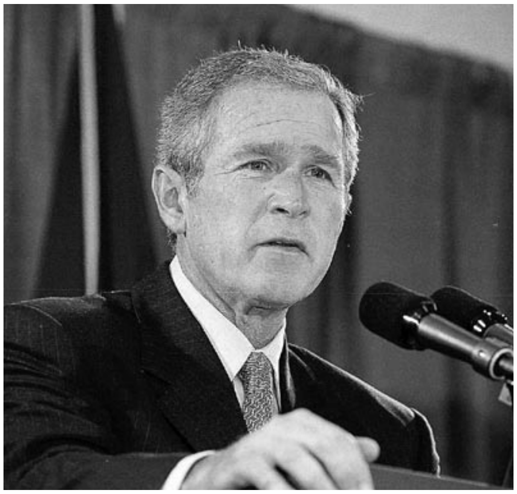
On July 11, 1963, President John F. Kennedy signed National Security Action Memorandum 252, *Establishment of the National Communications System*, ordering the formation of the National Communications System (NCS) in the wake of communications difficulties encountered during the Cuban Missile Crisis. A study conducted by the National Security Council (NSC) in the wake of the crisis determined that a consolidated system to support critical Government communications functions should be created. As directed by this memo, 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."

Over the past 43 years, the role of telecommunications in supporting the Nation's NS/EP functions, as well as the mission of the NCS has steadily grown. By the late 1970s, Government policy formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and recovery in the event of a nuclear attack. During the early 1980s, the impending divestiture of AT&T, the proliferation of service providers in the telecommunications industry, and the expansion of network capabilities complicated the means for satisfying NS/EP requirements. In response

New York, NY, September 27, 2001 – The remaining section of the World Trade Center is surrounded by a mountain of rubble following the September 11 terrorist attacks. *Photo by Bri Rodriguez/ FEMA News Photo*

to the new environment, President Ronald Reagan, signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions* on April 3, 1984. E.O. 12472 amended the NCS structure to include the Secretary of Defense as the Executive Agent; the Manager, NCS, and staff; and a Committee of Principals (COP), to represent the Federal member organizations with NS/EP responsibilities. E.O. 12472 also expanded the mission of the NCS, requiring it to assist the Executive Office of the President, including the NSC; the Office of Science and Technology Policy; and the Office of Management and Budget in the exercise of wartime and non-wartime emergency telecommunications responsibilities, and to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

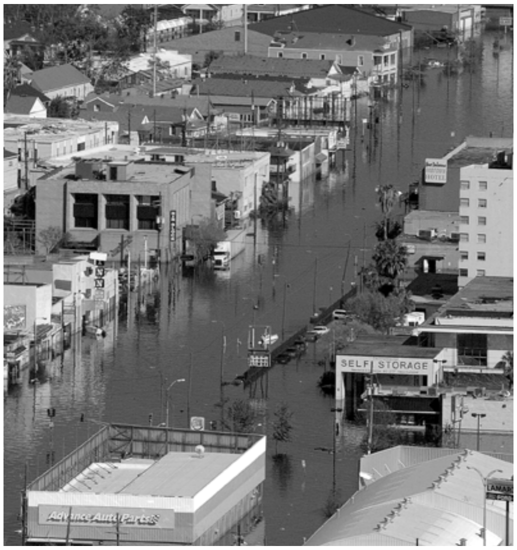
The NCS mission greatly expanded in both 1998 and 2001 to include a greater number of critical infrastructure protection (CIP) and homeland security-related responsibilities as a result of the publication of Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructure,* and the attacks of September 11, 2001, on the World Trade Center in New York City and the Pentagon in Washington, D.C. On October 8, 2001, in the wake of the terrorist attacks, President George W. Bush issued E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council,* which created the White House Office of Homeland Security (OHS), and tasked it to coordinate protection efforts for critical public and privately owned information systems within the United States. The E.O. also authorized the OHS to coordinate efforts to ensure the rapid restoration of telecommunications and critical information systems after disruption by a terrorist threat or attack. President Bush also issued E.O. 13231, *Critical Infrastructure Protection,* on October 16, 2001, which called for the formation of the President's CIP Board and re-established the NCS' COP as a permanent standing committee with additional reporting requirements to the new CIP Board, in addition to its firmly established reporting functions and responsibilities maintained under E.O. 12472.



On November 25, 2002, President Bush signed into law the *Homeland Security Act of 2002*, which established the Department of Homeland Security (DHS) and initiated a major reorganization of Government departments and agencies with homeland security missions. 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 Department of Defense to DHS. The NCS officially became a part of the DHS' Information Analysis and Infrastructure Protection Directorate on March 1, 2003. On November 15, 2005, the NCS was again realigned under the newly established Office of Cyber Security and Telecommunications within the Department's new Preparedness Directorate, which took place in response to Secretary Michael Chertoff's Second Stage Review.

NCS ENVIRONMENT— THE IMPLEMENTATION OF LESSONS LEARNED

On July 5, 2005, a series of coordinated bomb blasts struck London's public transportation system at the height of rush hour traffic. Within 50 seconds, three blasts significantly damaged a similar number of cars on the city's Underground trains while, almost an hour later, a fourth blast destroyed a bus in the highly traveled Tavistock Square. As a direct result of these bombings, United States authorities initiated the termination of cellular network services in the Lincoln, Holland, Queens, and Brooklyn Battery Tunnels on the suspicion that similar attacks might also be perpetrated in the tunnels leading to and from New York City.



New Orleans, LA, September 8, 2005 – FEMA's US&R teams in route by helicopter to conduct a search in St. Bernard Parish, view the flooding in New Orleans. *Photo: Michael Rieger/FEMA*

Just over a month later, on August 29, 2005, the Nation experienced its worst natural disaster, as Hurricane Katrina slammed ashore near New Orleans, Louisiana, causing massive infrastructure damage and flooding along the Gulf Coast region. These two unfortunate incidents reinforced within the NCS the need to maintain focus on an all hazards approach to NS/EP telecommunications. The NCS launched a series of activities within the organization which, over the course of FY 2006, would improve the agency's preparedness posture and operational ability to respond to such events in the future.

Though vital security concerns rooted the decision to terminate cellular networks following the London bombings, the resulting situation, undertaken without prior notice to wireless carriers or the public, created disorder for both Government and the private sector at a time when use of the communications infrastructure was most needed. Consequently, in the months that followed, the NCS worked in partnership with the National Coordinating Center and private industry to develop a procedure for cellular service disruption. The protocol, which DHS approved in March 2006, codifies a shutdown and restoration process for use by commercial and private wireless network providers during national crises both within a localized area, such as a tunnel or bridge, and within an entire metropolitan area.

In a speech to the American public from New Orleans on September 15, 2005, President Bush challenged the Federal Government to review its response to and learn the lessons of Hurricane Katrina so that the Nation will be better prepared for any natural or man-made disaster in the future.

In response to this request, Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, presented the President in February 2006, with the *Federal Response to Hurricane Katrina: Lessons Learned*. The document outlined numerous lessons learned and identified 17 challenges facing the Federal Government, including communications and critical infrastructure protection. Specifically, the document charged the Executive Office of the President (EOP) with organizing an interagency group to begin development of a national emergency communications strategy to be completed by May 31, 2006, which would provide guidance and direction to address the deficiencies identified in the Hurricane Katrina response. In turn, the EOP tasked the NCS to undertake this mission.

Over the course of two months, the NCS worked in partnership with a Federal interagency working group to develop a strategy that would encompass a full range of hazards, provide a framework for future U.S. Government planning efforts, and inform revisions to key policy documents governing emergency communications support. On May 17, 2006, the NCS submitted the interagency interim *National Emergency Communications Strategy,* to the EOP for further review and consideration.

In addition to the development of the strategy, the NCS engaged in numerous other activities designed to improve its response and recovery capabilities based on lessons learned from Hurricane Katrina. As the primary agency supporting the Emergency Support Function 2—Communications (ESF-2) Annex to the National Response Plan, the NCS conducted an after action session to collect detailed lessons learned from those who responded at the local level and then revised the ESF-2 Operations Plan. The NCS developed and implemented an ESF-2 Training and Response Improvement Program and worked with the ESF community to assess the Government's ability to ensure industry priority access to fuel, security, temporary housing, and temporary staging sites for emergency responders.

Furthermore, the NCS developed plans for deploying a reliable communications capability for emergency responders, inventoried the communications-related solutions available in the public and private sectors, and is developing a communications asset database to store this information so it may be promptly located and utilized when needed. Additionally, the NCS has made improvements to several tools to improve situational awareness around asset location, network impact, and communications coverage. Finally, representatives from DHS and the NCS met with industry partners from the President's National Security Telecommunications Advisory Committee to identify actions industry could undertake to assist in meeting the challenges stemming from the hurricane and to develop an access Standard Operating Procedure to ensure that private critical infrastructure responders receive priority access to disaster areas.

Baton Rouge, LA, June 13, 2006 – Federal, state and local emergency support function leaders gather for a week long exercise in Baton Rouge to test the standard operating procedures and new structures relevant to emergency management's response throughout hurricane season. *Robert Kaufmann/FEMA*

The NCS' activities during FY 2006 were also heavily influenced by several other factors including the implementation of new policy tools, the development of telecommunications-related risk management methodologies and techniques, and organizational change.

In June 2006, the DHS published the National Infrastructure Protection Plan (NIPP) to meet the requirements outlined in Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*. The NIPP framework, which enables the prioritization of protection initiatives and investments across sectors to mitigate against risk, also requires the sector specific agencies (SSA) to develop sector specific plans (SSP). As the SSA for telecommunications, the NCS has worked through the Government Coordinating Council with the Communications Sector Coordinating Council to jointly finalize and implement the SSP. The NCS anticipates the completion of the SSP by the end of 2006.

Furthermore, in its May 2006 *National Strategy for Pandemic Influenza Implementation Plan,* the Homeland Security Council identified telecommuting as a key component of the national response to a pandemic influenza and questioned whether the telecommunications infrastructures and enterprise networks are prepared to handle the anticipated change in communications traffic in response to a pandemic influenza. To address the issue, the NCS agreed to undertake a study titled *Pandemic Influenza Impact on Communications Networks.* The study focuses on the technical feasibility of national policy and business continuity planning related to telecommuting in response to the pandemic influenza threat. It builds upon work the NCS conducted in an initial assessment of the potential impacts of a pandemic influenza on the communication networks in November and December of 2005. This earlier study identified potential congestion points for various types of telecommunication access and enterprise networks.

To mitigate against risk to the telecommunications network posed by both natural and man-made disasters, the NCS designed an abridged route diversity methodology to enable agency self-assessment and held a route diversity forum with communications officials from Federal departments and agencies to socialize its route diversity methodologies and findings. Additionally, the NCS has actively participated in the development of a national command and coordination capability to further support continuity communications while its Continuity Communications Architecture program office initiated efforts to analyze the ability of Federal departments and agencies to perform their primary mission essential functions also in support of continuity communications.

With each new challenge, the NCS continues to evolve its existing partnerships, programs, and risk management approaches to meet the changing policy, technology, and threat environments. The NCS remains committed to fulfilling its mission and providing its stakeholders with proactive solutions to meet current and future homeland and national security communications requirements in an all hazards environment.

II

Emergency Response Activities

SECTION II
EMERGENCY RESPONSE ACTIVITIES

HURRICANE SEASON 2005

During the 2005 Hurricane Season a series of powerful tropical storms and hurricanes struck the Southeastern United States and the Gulf Coast. Two storms—Hurricanes Katrina and Rita—resulted in unprecedented damage to the communications infrastructure and significant problems for communications service providers. Through a detailed evaluation of these events, during 2006, the National Communications System (NCS) modified policy, procedure and organizational structure to more effectively address future catastrophic events. These modifications are outlined in detail in the "National Security and Emergency Preparedness (NS/EP) Telecommunications Support, Activities and Programs" section of this report. The final significant storm of the 2005 season, Hurricane Wilma, occurred in fiscal year (FY) 2006.

Hurricane Wilma

Hurricane Wilma first made landfall as a Category 2 hurricane on October 23, 2005, in Southwest Florida. Telecommunications carriers' initial assessments reported generally stable communications conditions with most of the outages occurring in Broward, Miami-Dade, Monroe, and Palm Beach counties due to the loss of power. Emergency Support Function-2, Communications (ESF-2) was activated and conducted daily conference calls with industry and Government representatives to facilitate information sharing and coordinate response actions. These conference calls helped to identify communications assets for potential deployment and track industry efforts to stage generators, ice, food, fuel, water, and personnel for quick response. After impact, ESF-2:

- Identified requirements and provided communications support to the response efforts;
- Coordinated with State officials from Florida to issue an access letter permitting telecommunications teams to work after curfew; and
- Worked to resolve fuel access issues for restoration workers.

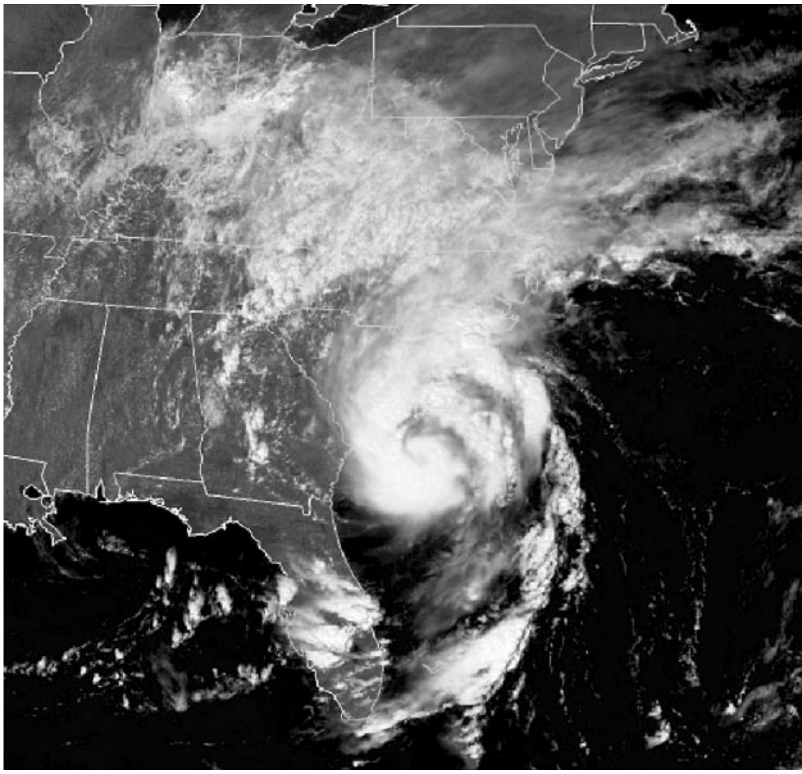
The NCS National Coordinating Center (NCC) actively tracked and communicated pre- and post-landfall response activities in coordination with ESF-2 partners, field office components, and telecommunications industry partners. Specifically, the NCC:

- Established information sharing channels with communications service providers, mitigated potential facility damage, and helped to reduce anticipated recovery times;
- Developed a detailed impact analysis of the wireline/wireless telecommunications assets and facilities within the path of Wilma and distributed it to ESF-2 partners at Headquarters and in the field;
- Ensured the communications needs of 9-1-1/Public Safety Answering Points were being met; and
- Activated the Shared Resources (SHARES) High Frequency Radio Program.

HURRICANE SEASON 2006

The 2006 Hurricane Season was remarkably calm compared to the 2005 season, with only two tropical storms, Chris and Ernesto, requiring the activation of ESF-2. Although ESF-2 was activated at the National Response Coordination Center (NRCC) for Tropical Storm Chris, no communications assets were significantly impacted. Tropical Storm Ernesto had a somewhat greater impact and required ESF-2 activation on both the regional and Federal level. Despite the low level of activity, the NCC maintained a high alert posture throughout the hurricane season and monitored, analyzed, and assessed all approaching storms.

Tropical Storm Ernesto



Tropical Storm Ernesto makes landfall on North Carolina coast

Ernesto made landfall as a tropical storm on August 31, 2006, near Long Beach, North Carolina. Federal Emergency Management Agency (FEMA) Region IV stood up a Joint Field Office and an Emergency Response Team-Advance deployed to the region with an ESF-2 representative. The NCS also provided three ESF-2 representatives to the National Response Coordination Center and elevated the SHARES operational status to Level-2 (indicating that a potential emergency exists and operators should verify equipment and personnel readiness). The NCS stood ready to supplement the NCC and stand up an Analysis Response Team, which provides impact analysis of the telecommunications infrastructure. However, these measures did not need to be implemented for this event. The ESF-2 team at the NRCC held conference calls with industry and

Government representatives to facilitate information sharing and coordinate response actions. They also:

- Implemented new procedures to post situation reports on the Homeland Security Information Network;
- Developed a relationship with FEMA Mobile Emergency Response Support detachments to maintain visibility of communications assets being deployed to the region, increasing situational awareness; and
- Coordinated with the Department of Defense (DOD) logistical planners assigned to the NRCC to integrate their capabilities into response actions.

OTHER EVENTS

Despite a relatively slow hurricane season, the NCS did support response efforts for a number of minor events. Specifically, the NCC Watch performed infrastructure analyses to determine the impact to telecommunications assets for the following events:

- Northern California floods, Sacramento – San Joaquin Delta Region, January 1-6;
- Texas/Oklahoma wildfires, Callisburg, Cross Plains, TX; Mustang, Guthrie, Oklahoma City, OK, January 1-6;
- Two major communications outages in the Western U.S. due to a California mudslide and an accidental fiber cut in Arizona, January 9;
- San Francisco subway fire, March 9;
- Texas wildfires, Texas Panhandle Region, March 14;
- California levee breach, California Central Valley Region, April 4-12;
- Northeastern U.S. flooding, MA, NH, Southern ME, May 15-17;
- East Coast flooding, VA, PA, MD, DE, DC, NC, June 28; and
- Tropical Storm Chris, August 2-4.

The NCC Watch notified and distributed relevant situation reports to the appropriate Communications Information Sharing and Analysis Center (ISAC) members during these events. In addition to these minor emergency response events, the NCC Watch participated in a number of cyber events during FY 2006. The role of the NCC Watch was to distribute information advisories to Communications ISAC members and provide coordination and situational awareness to appropriate organizations, such as the DOD's Joint Task Force for Global Network Operations and the U.S. Computer Emergency Readiness Team.

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) 2006.

National Communications System Organization and Leadership Changes

Just prior to the end of FY 2006, the President announced that George W. Foresman, the Department of Homeland Security's (DHS) Under Secretary for Preparedness would become the Manager of the National Communications System (NCS), retroactive to August 16, 2006. Mr. Foresman replaced Robert B. Stephan, who managed the NCS for 16 months. Mr. Stephan remains with DHS and continues his duties as the DHS Assistant Secretary for Infrastructure Protection. Mr. Robert Zitz, Mr. Foresman's Deputy Under Secretary for Preparedness, serves as the NCS Principal Deputy Manager and assumed supervisory duties over both the NCS and the National Cyber Security Division (NCSD), formally transferring both entities from DHS Infrastructure Protection.

As part of the DHS's Second Stage Review (2SR) completed in August 2005, the department reassigned the NCS and NCSD to the DHS Preparedness Directorate's Cyber Security and Telecommunications Branch. During most of the year, the NCS and NCSD remained administratively under the Office of Assistant Secretary for Infrastructure Protection while awaiting the appointment of an assistant secretary. That wait ended in late September when the President appointed Gregory Garcia—formerly the Vice President of Information Security Programs and Policy with the Information Technology Association of America—as Assistant Secretary for Cyber Security and Telecommunications.

Two other changes occurred within the NCS staff. Air Force Colonel Victoria A. Velez replaced Air Force Colonel Sheron Bellizan as the NCS Chief of Staff, and Brian Carney returned to the NCS in April 2006 to serve as Manager of the National Coordinating Center (NCC). Mr. Carney replaced Donald Smith, who transferred to the DHS's Infrastructure Protection Branch.

NCS INTERNATIONAL

Background

The NCS addresses the international component of its NS/EP goals through engagement with close allies and other countries, as well as international organizations. Working within an interdepartmental and interagency process in close consultation with industry, the NCS seeks to engage nations in a concrete, mutually beneficial manner to achieve NS/EP goals, including Critical Infrastructure Protection (CIP) and Civil Emergency Planning (CEP). The International Affairs Advisor, a Department of State (DOS) detailee, coordinates the NCS International program.

Summary

Over the course of the year, the NCS maintained its robust relationships with Canada and the United Kingdom, meeting frequently throughout the year in a variety of fora to discuss areas of mutual concern and seek solutions to issues that impact each nation. The Security and Prosperity Partnership (SPP), with Canada and Mexico, completed its first year with the NCS taking the lead on four initiatives, completing several of the sub-tasks with others on target. The North Atlantic Treaty Organization (NATO) also remained a key focus, with the United States providing substantial contribution to the work of the Civil Communications Planning Committee (CCPC) and NATO CEP.

Representation of the United States at the United Nations' International Telecommunications Union (ITU) was significant with increasing focus on Next Generation Networks (NGN) and its implications for U.S. NS/EP communications. With the official release of the National Infrastructure Protection Plan (NIPP), the NCS verified that its International Strategy was aligned with the goals and partners identified in the international annex of the NIPP. Additionally, the NCS provided information and coordination for the Secretary's office on Homeland Security Telephone Links. Finally, the NCS continued its role as a reviewing organization to the Committee on Foreign Investment in the United States.

These core capabilities are highlighted in the bilateral and multilateral engagements of the NCS, key details of which are provided below.

Multilateral Engagements

The Security and Prosperity Partnership

The leaders of the United States, Canada and Mexico celebrated the one-year anniversary of the SPP in July 2006. The NCS worked with its United States, Canadian, and Mexican counterparts on several initiatives of the security pillar's Goal 9, which addresses protection, prevention and response. The NCS work with Canada resulted in completion of all three of the initiatives targeted at the six-month mark. Progress with Mexico moved at a slower pace, with all three of the initiatives at the six-month mark delayed as the Government of Mexico transitioned to new leadership.

The North Atlantic Treaty Organization's Civil Communications Planning Committee

The NCS International Affairs Advisor heads the United States delegation to the Civil Communications Planning

Committee CCPC) with a U.S. telecommunications industry representative as well as representatives of the U.S. Postal Service. During FY 2006, the CCPC met twice in plenary session, as well as four times in working group format to work on tasks from the 2005/2006 CCPC Work Program (WP). Major FY 2006 activities and accomplishments included:

- The United States led Task 2.1 of the 2005/2006 CCPC WP, which analyzed the relevance of NATO's policy on censorship with regard to NATO and national responses to terrorism. The resulting finding determined the 1963 policy as impractical and outdated, recommending its deletion with no subsequent replacement.

- Members of the U.S. CCPC and NATO Joint Medical Committee delegations met with Canadian counterparts to discuss potential effects of Pandemic and Avian flu on NATO CEP.

- The United States participated in the joint CCPC and Civil Protection Committee seminar in Tallinn, Estonia to explore crisis communications requirements (both the message and the means) to respond, recover and mitigate disasters.

- Among many other contributions to the CCPC, the United States participated in efforts to update the CCPC Compendium, as well as contributed to CCPC working papers analyzing the Local Loop, Telecommunications Interconnections, and International Telecommunications Organizations. The United States also provided feedback on the NATO Civil Rapid Reaction Team Handbook.

Bilateral Engagements

Canada—The NCS maintained its very strong working relationship with Canada throughout FY 2006, embodied primarily in the United States/Canada Civil Emergency Planning Telecommunications Advisory Group (CEPTAG). Most notable this year was Canadian support to the United States following the devastation of the Gulf Coast hurricanes. Working in close cooperation with the NCS and its industry partners, Canadian government and industry played a key role in the response and recovery efforts. In addition to virtually continuous informal correspondence with Canadian colleagues, engagement included the following activities during FY 2006:

- Information sharing between the NCS Network Security Information Exchanges (NSIE) and Canada's NSIE continued, with Industry Canada (IC)—a Canadian Government agency—participation and a joint NSIE meeting in Canada.

- At the invitation of the NCS, a senior representative of IC attended the President's National Security Telecommunications Advisory Committee (NSTAC) annual meeting.

- As prescribed in bilateral agreements, CEPTAG held two official meetings, with agendas including such topics as: the SPP, the effects of Avian Flu, the NCS Government Emergency Telecommunications Service/Wireless Priority Service (GETS and WPS), Internet Impact Study and Route

Diversity Methodology, Hurricane Katrina Lessons Learned, Can Alert and U.S. National Alerting System, and NATO.

- To promote watch and warning coordination, IC detailed two officials for a month to the NCS NCC and the NCS continued to conduct weekly video teleconferences with IC.

- Officials from IC attended the NCS GETS/WPS Forum in Richmond, Virginia, in May 2006.

- Officials from the NCS attended the Canada Telecommunications Emergency Preparedness Association meeting in Canada in May 2006.

- Canada hosted in September 2006, the first international NSTAC Research and Development Exchange, which included representatives from the United States, Canada and the United Kingdom.

United Kingdom—This critical relationship also continued to flourish in FY 2006. Meetings and discussions were pursued under the auspices of the Joint Contact Group (JCG) and NATO. The NCS works with the organizations of United Kingdom's Cabinet Office—primarily the Central Sponsor for Information Assurance (CSIA). As with Canada, the NCS enjoys a substantial relationship with its United Kingdom counterparts. The notable activities for FY 2006 included:

- Following the London bombings in July 2005, officials from the NCS and CSIA met on several occasions to develop an initiative for resilient communications between the two governments during a crisis.

- The NCS conducted discussions with United Kingdom representatives about ongoing NATO CCPC developments, as well as their inclusion in the ongoing dialogue between the United States and Canada on international CIP issues.

- United Kingdom representatives attended the NCS GETS/WPS Team Forum, participating in a discussion of current and future architectures for priority services, particularly in Europe.

- The NSTAC invited the United Kingdom representatives to participate in the first-ever international Research and Development Exchange held in Ottawa, Ontario, Canada.

Mexico—The NCS began to engage Mexican telecommunications officials in October 2001, as a product of the work plan of the Border Partnership Accord. Monthly teleconferences conducted under the auspices of the accord continued until early in the 2005 calendar year when Mexican cabinet level reassignments resulted in a break of communication. Despite slow progress with Mexico during FY 2006, the NCS remained engaged in conjunction with parallel efforts of DOS. The NCS expects to move forward on several initiatives following the inauguration of Mexico's newly elected President.

Other Bilateral Engagements and International Activity

The NCS continued to work closely with DOS's Bureau of Political-Military Affairs, the Bureau of Economic and Business Affairs and other DOS bureaus, as well as with other agencies and offices within DHS and the U.S. Government to ensure continued appreciation of the overall strategic picture for U.S. international policies. The NCS also maintained representation at interagency working groups such as the U.S. Government's International CIP Working Group and Interagency Working Group on NGN. Additionally, the NCS either hosted or provided representation at bilateral meetings that included the following nations:

- **Italy**—The NCS hosted the Director General of the High Institute for Communications and Technology of Italy in February of 2006.

- **Afghanistan**—The NCS hosted a delegation from Afghanistan's Ministry of Communications in August of 2006.

- **Japan**—The NCS participated in a State Department-hosted U.S. Government bilateral meeting on CIP with government and industry representatives.

- **Israel**—The NCS attended DHS Office of Intelligence and Analysis-sponsored coordination and preparatory meetings on bilateral issues with Israel.

- **Australia**—The NCS participated in State Department-hosted U.S. Government bilateral. Presented on and extended offer to explore implementation of a hotline between the Secretary of Homeland Security and his Australian counterpart.

Plans for FY 2007 and Beyond

The NCS will continue to review and update its international strategy with key DHS and other agency stakeholders. The NCS staff will place particular emphasis on ensuring the goals outlined in the NIPP and address coordination with the NCSD on international priorities. Specific areas of focus will be as follows:

Security and Prosperity Partnership

The NCS will continue to work with its counterparts in the United States, Canada, and Mexico to achieve the goals established in the SPP. Several of the U.S.-Canadian initiatives led by the NCS have deadlines in early FY 2007. The NCS also hopes to renew its partnership with Mexico and to make progress on the goals defined in the SPP.

North Atlantic Treaty Organization's Civil Communications Planning Committee

The United States will maintain representation in the CCPC to ensure that the NATO body addresses the Nation's interests and goals. The CCPC will finalize its 2007-2008 work plan in early FY 2007, and the United States is working with partner nations to ensure the committee's goals are relevant, achievable, and promote U.S. interests.

Bilateral Relationship with Canada

The United States expects to continue its strong working relationship with Canada in FY 2007. The NCS expects to attend several face-to-face meetings with Canadian colleagues, as well as maintain regular communications with working-level officials.

Bilateral Relationship with the United Kingdom

The NCS will continue to work closely with the United Kingdom on international CIP issues and the resilient communications initiative through the JCG. It also hopes to further engage the United Kingdom through the inclusion of its representatives in CEPTAG, NSTAC, and NSIE events.

Bilateral Relationship with Mexico

With the inauguration of a new president in Mexico in late-2006, the NCS anticipates improved opportunities to engage with the Mexican Government on telecommunications issues. The NCS hopes to finalize key U.S./Mexican documents and establish sound working-level relationships with appropriate officials.

TECHNOLOGY AND PROGRAMS DIVISION

The Technology and Programs Division develops programs, technical studies, modeling capabilities/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. The NCS brings this information to industry and international standards organization meetings to ensure organizations incorporate NS/EP requirements into any recommendations.

The following pages highlight the major projects undertaken by the Technology and Programs Division during FY 2006.

Emergency Communications Services

Government Emergency Telecommunications Service

Background

The NCS 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. Reaching full operational capability (FOC) on September 30, 2001, the GETS program continues to ensure that NS/EP users receive a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters.

From the beginning, GETS planners focused on the public switched telephone network (PSTN) as the most efficient, reliable, and robust technology for supporting a service that would meet NS/EP mission requirements.

GETS leverages the PSTN's vast resources—a $400 billion infrastructure with more than 178 million access lines[1] and approximately 29,000 switches.[2] The ubiquitous, robust, and flexible PSTN supports more than 90 percent of the Government's telecommunications needs. Despite its enormous size and complexity, the telecommunications industry designed the PSTN to provide 99.999 percent availability.[3]

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 PSTN assets enabled early implementation and provided technical currency by leveraging continual improvements made by the industry. Embedding GETS primarily within the software resources of the PSTN 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 (now Verizon Business), and Sprint (now Sprint Nextel), the three largest IXCs and the only IXCs that can authenticate and process GETS calls. As such, access to these carriers must be available at all public switched network (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. The NCS competitively awarded the integration contract for the 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, 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. GETS features are being deployed on additional switches as they are upgraded to required software releases or as additional LECs are brought under contract. In addition, as industry upgrades networks, the GETS program continues to deploy enhancements that will help GETS calls terminate from the PSTN to customer premises and to simplify carrier provisioning of GETS features. As the PSTN evolves, the NCS 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 the NGN and development of requirements related to next generation call processing in acquisition packages for the IC and IXC follow-on contracts.

Operations and Features

Accessing GETS is quick and simple: Users dial the universal access number (710-NCS-GETS) using common telephone equipment, such as a standard desk set, payphone, secure telephone (for example, Secure Telephone Unit-Third Generation, cellular phone, facsimile, or modem. Telephones on the Federal Technology Service (FTS), the Diplomatic Telecommunications Service, and the Defense Switched Network also provide access to GETS.

When a user dials the GETS universal access number, a tone prompts for a personal identification number. Next, 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 has been demonstrated many times, most notably during the September 11, 2001, attacks on America and again during the hurricane seasons of 2004 and 2005.

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the NCS works 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 Standard ANSI T1.631-1993, which provides a class mark for NS/EP-related signaling messages. ANSI reaffirmed this standard in December 1999 and revised it in 2005 based on NCS input. The class mark allows NS/EP calls to be recognized in any U.S. network, facilitating the application of available GETS features.

In 1996, the 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 Program Management Office 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, the NIIF accepted Issue No. 0095, Implementing POTS IAM Priority Level 0. 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 between networks and service providers. The NCS works 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 PSTN for off-net GETS calls.

Like other services, GETS must adapt to the new services-rich, but highly competitive, telecommunications environment resulting from 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 Private Branch Exchanges (PBX). Previous testing showed 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 NCS 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 9-1-1 emergency and toll-free calls.

Successes

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

In the hurricane seasons of 2004 and 2005, GETS assisted NS/EP emergency response and recovery communications along the Gulf Coast region. During the three major hurricanes of 2005, Katrina, Rita and Wilma, 40,768 GETS calls originated or terminated in the affected areas. The NCS issued over 2000 new GETS cards to support NS/EP activities.

The GETS program continues to make significant progress in its outreach efforts to all levels of government (Federal, State, and local) and other qualified NS/EP industry and non-profit organizations. As of September 30, 2006, there were 140,743 active GETS cards– an increase of 30,283 cards since September 2005.

Table 1. GETS User Breakdown

GETS NS/EP Category	GETS NS/EP Users
Federal	80,871
State	13,464
Local	22,214
Industry	22,501
Other NS/EP organizations	1,693

Wireless Priority Service

Background

Like GETS, WPS supports NS/EP emergency response and 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.

In the past 10 years, the number of mobile wireless telephone subscribers in the United States increased from 33.8 million to over 200 million, served by over 5,000 mobile switching centers.[4] Globally, wireless subscriptions exceeded two billion at 2005 year's end.[5] Early in 1995, the NCS recognized that the significant annual increases of wireless telephony subscribers indicated a need for priority communications over the wireless networks and initiated efforts to develop and implement a nationwide cellular priority access capability in support of NS/EP telecommunications. Since then, the NCS pursued a number of activities to improve wireless call completion during times of network congestion. In 1998 and 1999, the NCS worked with an industry switch vendor and successfully demonstrated end-to-end wireless priority features.

In response to an October 1995 petition from the NCS, the Federal Communications Commission (FCC) released a Second Report and Order (R and O) [FCC-00-242, July 13, 2000] on wireless Priority Access Service (PAS). The R and O offers Federal liability relief to wireless carriers if the carriers implement the service in accordance with uniform operating procedures. The FCC made PAS voluntary for the wireless service providers, found it to be in the public interest, and defined five priority levels for NS/EP calls.

The days following the September 11, 2001, attacks saw widespread wireless network congestion, with wireless traffic demand estimated at up to 10 times the norm 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 guidance to the NCS regarding the development and implementation of WPS.[6] Responding to this guidance, the NCS provided an off-the-shelf immediate WPS (I-WPS) solution, with limited capabilities, by the February 2002 Winter Olympics in Salt Lake City. The I-WPS was operational by May 2002 in the District of Columbia and New York City. The NCS achieved nationwide WPS in December 2002.

Operations and Features

Due to the requirement for nationwide WPS coverage, enlisting multiple carriers and multiple access technologies was necessary. WPS is available in both of the access technologies most widely available in the United States: Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). GSM carriers T-Mobile, Cingular Wireless, and Sprint Nextel provide WPS with T-Mobile deploying WPS full operating capability in December 2003. Cingular Wireless followed in July 2004. The Sprint Nextel (iDEN) completed its full operating capability deployment in late 2005, thus completing the WPS rollout in GSM. As a result, user subscriptions for WPS have nearly tripled in the past year.

The provision of WPS capabilities in CDMA is well underway with the major CDMA carriers, Verizon Wireless and Sprint Nextel. Verizon Wireless is in the process of deploying WPS FOC Phase 1, which provides priority access to local radio channels when originating a WPS call; FOC Phase 2 deployment is planned for 2008. Sprint Nextel plans nationwide single-phased FOC implementation for 2007. A reduction in available funding, however, will affect WPS availability in approximately 20 percent of the CDMA carrier markets.[7]

In June 2006, the NCS tested QUALCOMM QSec-2700 CDMA-based secure phone interoperability with the General Dynamics GSM-based Sectera secure phone. The WPS-enabled QSec-2700 Release 3 software will be available within the 2006 calendar year pending National Security Agency certification.

Many of the significant challenges facing WPS stem from technology upgrades, requiring the NCS to assure continued availability of WPS capabilities as wireless carriers move to third generation (3G) wireless technologies.

Industry Requirements

WPS is based on wireless standards and industry requirements (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. The NCS completed initial requirements in February 2002, only four months after the NCS received direction from the NSC. The FOC requirements for both GSM and CDMA are complete. In addition to establishing engineering requirements, the NCS uses these documents as a basis to issue requests for proposals for the WPS.

The IRs provide a method for use of the Nation's cellular telecommunication networks by NS/EP personnel that will not hinder public use during emergency events by defining a standards-based priority queuing capability. As a result, the IR documents stipulate that a reasonable amount of capacity is always available for public use.

Successes

During the 2004 and 2005 hurricane seasons, WPS assisted NS/EP emergency response and recovery communications along the Gulf Coast region. Following Hurricane Katrina in August 2005, the NCS approved 2,500 new WPS users. Subscribers placed thousands of WPS calls into and out of the affected regions.

In the past year, the WPS program 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 non-profit organizations. As of September 30, 2006, there were 38,668 authorized WPS users—a 51 percent increase since September of 2005.

Table 2. WPS User Breakdown

WPS NS/EP Category	WPS NS/EP Users
Federal	29,830
State	1,049
Local	3,151
Industry	4,633
Other NS/EP organizations	5

For NS/EP users, WPS and GETS are significant emergency communications assets and they have proven to be effective during natural and man-made disasters.

NS/EP Priority Services in Next Generation Networks

Telecommunications engineers specified, engineered and implemented historical NS/EP priority services, such as GETS and WPS when the PSTN was based exclusively on circuit-switched technology. Today's PSTN is incorporating, and eventually replacing, circuit-switched equipment with the packet-based technologies supporting Internet Protocol (IP) data networks for some time. This convergence into a packet-based technology dictates the evolution of GETS and WPS into the NGN. Using packet technology, NS/EP NGN will provide priority NS/EP communications not only for voice, but also for broadband applications, such as video and data.

The NCS assessed emerging IP technologies and found that there was no overall priority or end-to-end quality of service architecture in place today. Service providers are deploying quality of service and priority techniques only within their managed IP networks and only for limited applications and users. The NCS developed an NS/EP NGN reference architecture and continues to work with service providers and vendors to assure they consider NS/EP requirements as they develop their individual architectures.

Working with industry and the international standards bodies, the NCS participates in the development of a standard for the Session Initiation Protocol (SIP) to mark and communicate priority attributes. The Internet Engineering Task Force (IETF) identifies this "resource priority" header (RPH) as identified in IETF Request for Comment

4412, dated February 2006. The NCS is participating in a MultiService Forum (MSF) global interoperability event demonstrating priority voice calling and priority video conferencing using RPH in the NGN.

During this past year, the NCS surveyed emerging Voice over Internet Protocol (VoIP) service providers and determined that many were not routing 710 GETS calls properly. To correct this problem, the NCS worked with Telcordia Technologies to update the Telcordia Local Exchange Routing Guide (LERG); ongoing testing confirms that the majority of VoIP service providers are now routing 710 properly. The LERG serves as a database of voice switching assets that facilitate the routing of interLATA telephone calls throughout the PSTN.

The NCS will continue to coordinate with industry partners to jointly develop NS/EP solutions—a highly successful approach proven during the development of the GETS and WPS programs. This ensures that users will continue to be provided with the priority services they need to meet their NS/EP mission requirements.

NS/EP Standards Development

Presidential Executive Order (E.O.) 12472 *Assignment of National Security and Emergency Preparedness Telecommunications Functions* directs NCS consideration of evolving national and international standards with respect to NS/EP telecommunications, and Office of Management and Budget (OMB) Circular A-119 calls for Government to adapt the products of commercial/industry standards committees—and to participate in their development. The NS/EP Standards Branch personnel work with a number of national and international telecommunications industry standards organizations to ensure that evolving commercial standards address the technical requirements of NS/EP telecommunications.

Ongoing standards development initiatives encompass prime functionalities of: signaling, access, management, transport, interoperability, mobility, and their associated architectures. Standards work in support of NS/EP communications is being done under the term Emergency Telecommunications Services (ETS).

Engineers designed traditional NS/EP telecommunications services around the circuit-switched infrastructure of the PSTN. However, public networks are now merging with packet-switched infrastructures and evolving into converged NGN. As this evolution continues to mature, priority telecommunications services will be guided by commercial standards stemming from technologies based on packet-switching, such as IP based networks. Recognizing that IP and 3G and beyond wireless public networks have become increasingly vital during NS/EP events, the NS/EP Standards Branch primarily focuses on these two telecommunications media by working proactively with industry in standards development organizations.

The NS/EP Standards Branch provides direct support to the U.S. DOS 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. In addition, branch members actively participate in the work of various commercial/ industry standards development organizations including:

- Alliance for Telecommunication Industry Solutions (ATIS);
- Telecommunications Industry Association;
- International Telecommunication Union, Telecommunication Sector (ITU-T);
- Internet Engineering Task Force (IETF);
- TeleManagement Forum;
- Third Generation Partnership Project; and
- Third Generation Partnership Project 2.

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 (such as 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, and tunneling, mobility);
- Performing and promoting independent testing and implementations of proposed technical solutions; and
- 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 telecommunication services.

During FY 2006, the NCS played a role in the following ETS accomplishments:

- ATIS-PP-1000010.2006: Standard for Support of ETS in IP Networks; and
- ATIS-0100006: Service Restoration Priority Levels for IP Networks.

Approval of Amendments to ITU-T Recommendations:

- Q.761: Signaling System No. 7—ISDN User Part Functional Description;
- Q.762: Signaling System No. 7—ISDN User Part General Functions of Messages and Signals;
- Q.763: Signaling System No. 7—ISDN User Part Formats and Codes;
- Q.1902.1: Bearer Independent Call Control protocol (Capability Set 2)—Functional Description;
- Q.1902.2: Bearer Independent Call Control protocol (Capability Set 2) and Signaling System No. 7 ISDN User Part—General Functions of Messages and Parameters;
- Q.1902.3: Bearer Independent Call Control protocol (Capability Set 2) and Signaling System No. 7 ISDN User Part—Formats and Codes;
- Q.1902.4: Bearer Independent Call Control protocol (Capability Set 2) and Signaling System No. 7 ISDN User Part—Basic Call Procedures;
- Q.2630.3: AAL Type 2 Signaling Protocol—Capability Set 3; and
- Q.1950 (12/02): Bearer Independent Call Control Protocol.

Internet Engineering Task Force approved the following RFC:

- RFC 4190: Framework for Supporting ETS in IP Telephony;
- RFC 4375: ETS Requirements for a Single Administrative Domain; and
- RFC 4412: Communications Resource Priority for the SIP.

Modeling, Analysis and Technology Assessment

As directed by E.O. 12472, the NCS uses modeling and analysis techniques and applications to "conduct technical studies or analyses … for the purpose of identifying … improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives."

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 invested many years establishing strong working relationships with commercial carriers and Government departments and agencies, and in developing PSN modeling methodologies, tool sets, and unique databases that include proprietary data from the major carriers. The NCS uses the NDAC to conduct studies that cover multiple communications areas such as wireline, wireless and the Internet.

Route Diversity Project

The Route Diversity Project 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. Concurrently in Phases III, IV, and V, the NCS is assessing various wireless technologies to determine their potential to enhance communications resiliency (Phase III). Phase IV included the development of a route diversity methodology to enable Federal agencies in the Washington, D.C., area to assess their current level of diverse communications connectivity into the public networks. As directed by the White House, the NCS will continue to assist Federal agencies to analyze their communications and, when required, determine the optimum technical solution to increase resiliency.

Next Generation Networks Modeling

The convergence of the PSN circuit-switched architecture with the packet-switched technologies of the Internet is changing the communication infrastructure upon which NCS bases programs and analyses. As the infrastructure changes, NDAC tools and methodologies must evolve to support the analysis of these NGNs. The NDAC is currently analyzing the effects of routing convergence and network configuration on present and future priority treatment services. Because the technologies, architectures, and protocols used by service providers are in flux, the NCS is modeling multiple NGN architectures and analyzing their performance under various damage and congestion scenarios. The NCS will use the results of this effort to quantify the effectiveness of proposed priority service mechanisms and feed policy and budgetary decisions related to NCS programs such as GETS and WPS.

Internet Analyses

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 NCS must model logical and physical infrastructures of the Internet to support NS/EP analyses. With the on-going NDAC expansion to include packet-switched networks, the NCS developed an Internet modeling capability that captures physical and logical interdependencies between Internet Service Providers from both architectural and traffic perspectives. The NCS uses this capability to determine the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure, and provide situational awareness information in support of the NRP's Emergency Support Function 2 (ESF-2).

Traffic Analysis of Critical Federal Telecommunications Infrastructures

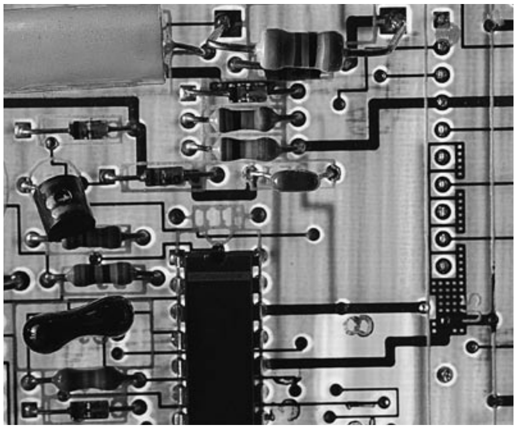
The NCS developed an analysis capability to identify the most critical Government and telecommunications provider locations necessary to ensure Government connectivity during crises. NCS coordinated with the GSA to obtain FTS2001 traffic data, and used this data to conduct critical infrastructure analyses for 12 NCS member agencies, including GSA, the National Aeronautics and Space Administration, the Department of Transportation, the National Telecommunications and Information Administration (NTIA), the Department of Agriculture, the Department of Health and Human Services, the Nuclear Regulatory Commission, the DOS, the Department of Defense (DOD), and DHS.

DHS OneNet Integration Support

When 22 agencies were brought together to create DHS, a hodgepodge of IT systems resulted. The DHS chief information officer's (CIO) challenge is to integrate these systems into DHS OneNet under GSA's new Networx contract. The DHS CIO opted to use the NCS demonstrated network modeling proficiency, tools, and data to support this effort.

Supervisory Control and Data Acquisition Modeling

To determine the applicability of implementing priority service mechanisms for electric grid applications, the NCS is developing Supervisory Control and Data Acquisition (SCADA) system models and the capability to model and test interactions between SCADA communication protocols and the telecommunications infrastructure. Through collaboration with Idaho National Labs, the NCS is using the National SCADA testbed to calibrate NDAC-developed SCADA communications dependency and vulnerability models. The NCS will use these models to analyze the performance of critical SCADA time-sensitive applications and to identify communications threats and vulnerabilities of the SCADA control system. The result of these analyses will provide recommendations and best practices to utility industries.



Technology Assessment and Data Analysis Cell

The NCS is developing a fully accredited facility to provide the capability to:

- Evaluate Contract Deliverables: Some contracts have software and/or hardware deliverables; the Technology Assessment and Data Analysis Cell (TADAC) can evaluate these deliverables for acceptance purposes.

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

- Host Applications and Databases: The TADAC 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 the NDAC—a set of tools, data sets, and methodologies that enable modeling and analysis of the PSN.

- 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 TADAC provides for this type of simulation.

- Participate in Community Research Projects: The TADAC enables the NCS to move beyond its role as a patron or sponsor of research, to become an actual participant. Besides enhancing our engineers' and computer scientists' expertise in critical areas, Internet community projects—such as The Honeynet Project[8]—provide an excellent opportunity to increase the respect and recognition of the NCS within research and development circles.

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

When fully developed, the TADAC will contain three networks with separate and distinct security accreditation boundaries. These networks include the Next Generation Priority Services eXperimental Testbed Environment (NGPS XTE), the Technology Assessment Network (TAN), and the classified Data Analysis Network (DAN).

Next Generation Priority Services eXperimental Testbed Environment

The NGPS XTE provides the ability to emulate a scaled-down version of the Internet and an Internet Service Provider's network, provide the capability to inject severe congestion both on the network and NGN end systems, and test and validate that emergency telecommunications services work properly from end-to-end. This is accomplished using call load generators and traffic generators coupled with a strong modeling and analysis capability. The NGPS XTE consists of:

- Network devices (routers and switches) simulating an ISP's backbone/core and access network

- Security devices (firewalls, session border controllers, and intrusion detection capabilities) to protect the network assets by detecting and responding to simulated threats

- Hosts and servers providing the invocation and termination of NGN services and priority services

- Test and analysis equipment to generate voice and data traffic and to gather results of the effects of congestion on NGN services

- VoIP telephones and systems to represent a VoIP service provider's service infrastructure

- High speed connection to the Defense Engineering Research Network (DREN)

Technology Assessment Network

TAN consists of a suite of equipment enabling the evaluation of cutting edge technology without jeopardizing existing development or production systems. This includes COTS/GOTS application evaluation and testing with respect to compatibility and interoperability, load stress, security features, and vulnerability identification. The TAN also hosts applications, databases and web-based tools; provides component-level network simulation; enables participation in community research projects; and provides a highly advanced training platform.

Data Analysis Network

DAN is a closed, classified network—meaning it has no external connections outside of the TADAC—that hosts the modeling applications and databases of the NDAC. It consists of a multi-vendor suite of tools and datasets enabling computer-based analyses of the PSN, including IP, Internet Telephony, and next generation packet-switched IP networks, under various conditions.

Advanced Technology Group

The NCS Advanced Technology Group (ATG) investigates new and emerging technologies with the objective of making them available to Government during national emergencies or crises. Over the past year, the ATG worked on a range of NS/EP communications topics such as ongoing Telecommunications Electromagnetic Disruptive Effects (TEDE) tests on next generation components, vulnerabilities to telecommunications service provider's operation support systems, vulnerabilities to synchronization support systems in telecommunications, vulnerabilities of SCADA, and satellite communications. The following paragraphs address these topics in detail.

Telecommunication Electromagnetic Disruptive Effects

Title 5 of the Code of Federal Regulations, Part 215, assigns the Executive Agent of the NCS as the Federal Government's focal point for electromagnetic pulse (EMP) technical data and studies concerning telecommunications. The NCS—specifically the ATG—coordinates and approves these tests and studies, and keeps the White House National Security Advisor informed of them. Moreover, the ATG looks at TEDE due to EMP, Magneto Hydro Dynamics (MHD), High Power Microwave (HPM), Directed Energy Systems, High Radiation Environments, solar flares, and the effects of lightning.

The ATG has coordinated and conducted numerous studies in the following topical areas:

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

The ATG conducted TEDE susceptibility tests of the telecommunications infrastructure to include:

- PSTN switching systems and infrastructure;
- Terrestrial/satellite transmission and power systems;
- Equipment level tests and network level modeling;
- Protection for new technologies and systems; and
- Partnered with congressional "Live Fire" high power microwave vulnerability tests of SCADA systems, PSTN switching systems, local area networks and computer systems.

Participating in the work of the Congressional EMP Commission, the ATG made legacy TEDE studies available and provided a briefing of current efforts, focusing on vulnerabilities to the telecommunications infrastructure. The ATG has also published documents delineating the vulnerabilities of telecommunication systems to EMP, MHD effects, HPM, Directed Energy Systems, High Radiation Environments, solar flares and lightning, and is continuing to lead the effort in identifying the vulnerabilities of IP-based systems to TEDE.

The ATG examined the risk of TEDE from High Power Electromagnetic generators to the wireline, wireless, and ground-based assets of satellite telecommunication infrastructure. The analysis also determined equipment vulnerability to upset and damage through preliminary testing of telecommunications and satellite equipment, developed a preliminary model on the effects of HPM threats on telecommunication infrastructure, and performed a preliminary risk evaluation by determining the minimum combination of threat parameters needed to exceed equipment vulnerability thresholds.

Vulnerability Issues

The ATG is publishing a number of technical reports concerning vulnerability issues associated with the telecommunications infrastructure. The following lists vulnerability studies conducted in FY 2006:

Configuration and analyses of commercial telecommunications equipment used by the Federal Aviation Administration (FAA) flight service centers, a medium-sized router, and a Voice over Internet Protocol (VoIP) telecommunications system to identify vulnerabilities as a result of HPM.

The objective of this analysis is to determine vulnerabilities of these telecommunications equipment to upset and damage. A preliminary model on the effects of HPM threats on the telecommunications infrastructure was developed and a preliminary risk evaluation was performed that determined the minimum combination of threat parameters needed to exceed the router's vulnerability thresholds. The ATG will provide recommendations on how to lessen telecommunications equipment susceptibility to electromagnetic disturbances.

Identify the vulnerabilities of fiber-optic telecommunication links due to secondary effects associated with X-ray illumination.

The objective of this analysis is to assess the maturity and availability of compact accelerator technologies suitable for conducting secretive attacks against the fiber infrastructure. The ATG will specify, acquire, assemble, and characterize a representative single-mode optical data link to serve as a target for the experiment and will:

- Identify and secure access to a laboratory-scale accelerator to conduct a series of controlled illumination experiments;
- Prepare a test matrix that identifies the parameters critical to the production of the desired secondary effect;
- Execute the proof-of-principle demonstration matrix; and
- Document the test results.

Evolving Technologies Studies

The ATG also analyzes emerging wireless and wire-line communications technologies and their impact on NS/EP telecommunications services. The following studies in evolving technologies were conducted in the past year:

Satellite Communications Program

The purpose of the Satellite Communications (SATCOM) Program is to examine the baseline capabilities of existing commercial SATCOM infrastructures, identify and make an initial assessment of key SATCOM vulnerabilities, analyze Federal agencies' SATCOM use via NS/EP functional requirements, and postulate candidate commercial NS/EP SATCOM programs.

Alerting and Coordination Network

The ATG is providing technical support to evaluate satellite technology as a backup to the Alerting and Coordination Network (ACN).

Global Positioning System Studies

As part of a coordinated interagency effort, the ATG provided an analysis of how loss of Global Positioning System timing services could affect key CIP sectors: Banking and Finance, Emergency Services, Energy, Telecommunications, Transportation, and Water.

Red Cell Emergency Alert Studies

The ATG is conducting research, analysis, and program planning for the integration of chemical, biological, radiological, nuclear and explosive sensor networks and emergency notification communications technologies. This effort will provide program management support through the development of the Red Cell communications concepts and the coordination of experiments and test scenarios with the NCS and DHS organizations as required. Products developed under this task are technical evaluation reports, test concepts, and documentation of results from prototypes, test runs, and experiments.

LOOKING AHEAD

The ATG is introducing concepts to solve credentialing (expedited disaster area access for restoration workers) using satellite technologies, in addition to investigating priority satellite communications for NS/EP.

One key approach the ATG is tracking is the satellite industry's development and implementation of the Ancillary Terrestrial Component, which is essentially a terrestrial repeater that amplifies and rebroadcasts weakened satellite signals. Within the past two years, the FCC has granted some Mobile Satellite System operators licenses to reuse their assigned frequencies to provide this hybrid satellite/terrestrial cellular service. The impact on NS/EP users will be substantial—indoor environments and dense urban areas will no longer impede a satellite telephone subscriber's ability to communicate during emergencies.

Continuity Communications Working Group

Background

The need for a Continuity Communications Architecture (CCA) was identified by the Enduring Constitutional Government Coordinating Council in 2004. The NCS was tasked with its development via the Office of Science and Technology Policy (OSTP), based on assigned responsibilities under E.O. 12472. Constituted under the NCS Committee of Principals (COP), the Continuity Communications Working Group (CCWG) addresses stove-piped systems and the lack of interoperability between Federal Executive Branch (FEB) departments and agencies in their continuity communications infrastructure.[9] In the case of the CCA, communications is defined in the broadest sense; that is, the information exchanged by departments and agencies as well as the telecommunications and computing mechanisms that support FEB continuity functions.

A critical part of the CCA is defining essential functions that departments and agencies must perform under the full range of NS/EP scenarios. In January 2005, the Assistant to the President for Homeland Security issued a memorandum to the FEB departments and agencies defining eight national essential functions (NEFs) that "… are necessary to lead and sustain the country."[10] departments and agencies were requested to define and submit their priority mission essential functions (PMEFs) in support of the NEFs before, during, and immediately following a national emergency.

The goals of the CCA program are:

- To develop prescriptive relationships between PMEFs, information flows, and mechanisms (such as communications infrastructure) by leveraging the Federal Enterprise Architecture (FEA) reference models;

- To collect and analyze the existing or 'As-Is', architecture; and

- To investigate existing and emerging communications capabilities to establish a set of future minimum communications requirements ('To-Be' architecture).

Accomplishments

In FY 2006, the CCWG was reconstituted under the NCS COP with representatives from the FCC and the Federal Emergency Management Agency (FEMA) serving as co-chairs. The OMNCS established a funded CCA Program Office (PO) that includes support provided by staff from two federally funded research and development centers as well as four commercial contractors. The Program Office FY 2006 accomplishments are:

- CCA Program Management Plan approved April 2006;

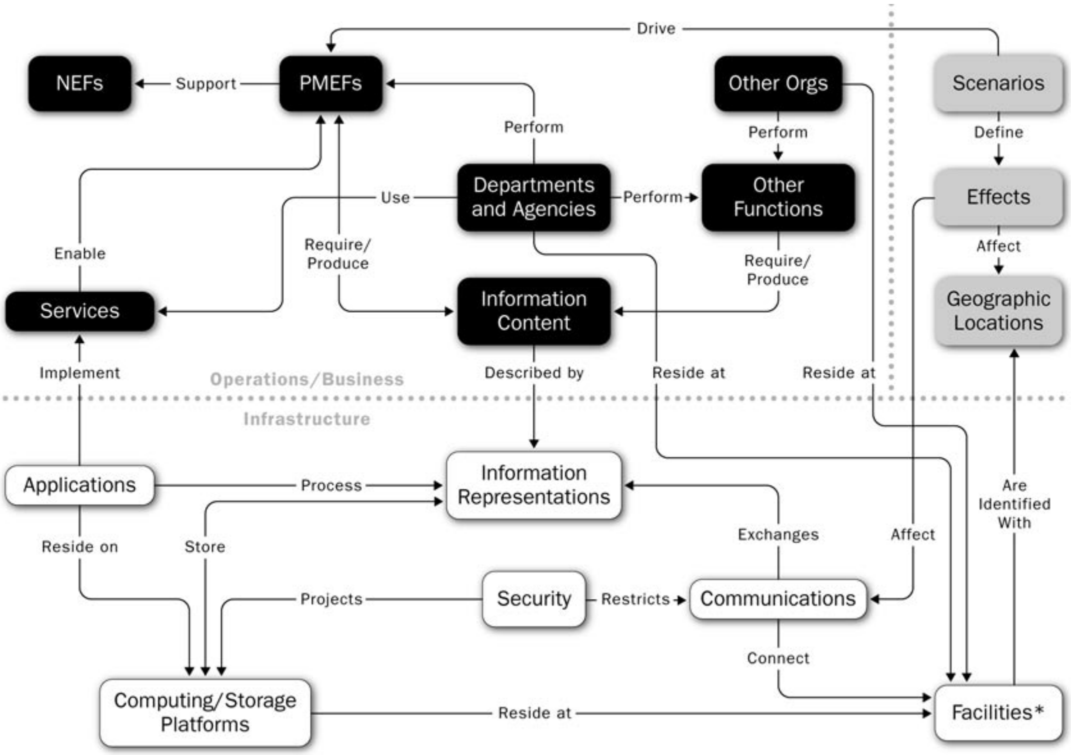
- CCA metamodel designed;

- CCA toolset developed; and

- Data collection with major departments and agencies, including the DOS and DHS, initiated.

A CCA metamodel (Figure 1) was developed to describe the relationships between functions (PMEFs supporting NEFs), environment, and infrastructure.

Figure 1. Continuity Communications Architecture Metamodel



* Fixed and/or mobile

Information flows describe the information content that is produced and required by the departments and agencies in order to perform their PMEFs. The environment covers the full spectrum of NS/EP scenarios and their related effects. The infrastructure consists of the facilities, communications systems, computing platforms, applications, and security devices that provide the means by which the departments and agencies exchange information. The PMEFs are mapped to the supporting infrastructure through the operational services implemented by specific applications that are used by the departments and agencies. The infrastructure that provides the mechanism for exchanging information in also tied to the PMEFs through the related information content. This metamodel will be used in the analysis of interdependencies between the departments and agencies in order to determine gaps in the communications infrastructure as well as the development of the 'To-Be' architecture.

In developing the CCA metamodel, the Program Office used the five FEA reference models as defined by the Office of Management and Budget.[11] The performance reference model can be tied to the PMEFs and NEFs to identify required performance measures enabling continuity. The business reference model relates to the departments and agencies and their PMEFs by tying the PMEFs to lines of business to ensure coverage of FEB responsibilities. The data reference model is used to map the departments and agencies' information requirements with specific formats. The service component and technical reference models provide examples of operational services, applications, information representations, and communications capabilities that departments and agencies use in performing their PMEFs.

Another accomplishment of the Program Office was the development of the CCA toolset. The toolset is a user interface and relational database based on the metamodel that is used for data collection and entry as well as a repository for the 'As-Is' architecture. The toolset includes pick lists of standard terminology embedded in a user interface to facilitate and normalize data collection and entry. The repository will include querying and reporting functions as well as specific data views that will be used in the analysis of the 'As-Is' architecture. The toolset was used to initiate the data collection effort with the CCWG members. A further use of the toolset is to develop and model the 'To-Be' architecture through scenario-based assessments of existing capabilities as well as emerging technologies.

In late FY 2006, the NCS also assumed a significant advisory and interagency coordination role for the National Command and Coordination Capability (NCCC). The NCCC, as defined by the NSC and Homeland Security Council (HSC) Deputies' Committee on August 31, 2006, serves as a means to provide the President with the ability to respond deliberately and appropriately to any crisis. It includes responsive, reliable, survivable, and robust processes and systems to command, control, and coordinate operations among Federal, State, Tribal, Insular, and local governments, as well as private organizations, foreign governments, and international entities, as required. The NCCC effort is relatively new and still evolving as a concept, with DHS serving as the Executive Agent for the program.

CRITICAL INFRASTRUCTURE PROTECTION (CIP) DIVISION

The CIP Division, through its unique industry-Government partnerships, ensures the availability of critical NS/EP communications services across the full spectrum of emergencies. Emergencies include, but are not limited to, conventional and terrorist attacks against the United States, natural and man-made disasters and other crises.

Organizational Structure

In response to lessons learned from the 2005 Hurricane Season, the CIP Division Chief organized a series of task forces to examine the division's preparation for and response to Incidents of National Significance. The following response related issues were examined:

- Preparedness and Planning;
- Operational Analysis;
- Staffing, Training and Exercise;
- Operations;
- Frequency Management;
- Contracting/Finance;
- Military Coordination;
- Security;
- Legal Authorities and Policies; and
- International Issues.

As a result of these discussions, the CIP Division modified its organizational structure to include the establishment of the Contingency Planning (CP) Branch which will focus its efforts on developing and implementing emergency response doctrines and operational plans. In addition to the new CP Branch, the Division includes: the Operations Branch—responsible for coordinating and managing emergency response, operations and information sharing activities among the communications industry, Government and International partners; the Operational Analysis (OA) Branch—responsible for providing near real-time analytical assessments of the communications infrastructure; and the Training and Exercise (TE) Branch—responsible for ensuring a cadre of fully knowledgeable and skilled emergency response personnel.

New Initiatives

These task forces revealed the necessity for a forward-deployed, permanent, regional presence for the NCS. Current NCS planning calls for the establishment of two permanent positions at each Federal region to assist in communications coordination. These positions, Regional Communications Coordinator (RCC) and Deputy Regional Communications Coordinator, will report to the CP Branch Chief but reside at the FEMA Regional Office.

Additionally, the NCS recognized the need to establish permanent Emergency Communications Teams (ECT) with well established and exercised functional duties and responsibilities. These teams are composed of personnel with the skills and knowledge required to meet the functional objectives of each position. Team members will train in the positions they will perform during an emergency such that all team members are familiar with one another and are proficient in their roles.

The task force discussions also revealed the need for a CIP tool to improve NCS' situational awareness of communications assets available to support disaster response. A prototype Communications Asset Database (CAD) has been developed to address this need. CAD will provide the capability to identify assets based on technology, technical description, location, quantity and status. Additionally CAD will allow operators to track the location and status of communications assets supporting disaster response.

Operations Branch

The Operations Branch is responsible for emergency response, operations and information sharing activities with industry, Government and international partners. The branch manages day to day operations of the NCC, the Communications Information Sharing and Analysis Center (ISAC) and several operational programs.

National Coordinating Center for Telecommunications

The NCC, an industry-Government collaborative body, is the primary mechanism within the NCS for fulfilling the emergency response role. 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 close relationship, between over 40 industry participants and 23 Federal Government agencies represented at the NCC, is the mechanism that ensures the success of this mission.

The operational arm of the NCC is its continuous watch and analysis operation, the NCC Watch. Senior level information assurance analysts located on site in the NCC Operations Center staff the NCC Watch as the focal point for all NCS emergency response operations. During response operations, the watch is the venue through which Government personnel communicate NS/EP requirement priorities to industry; and industry representatives provide the Government situational awareness of communications status in the disaster area.

Major NCC Activities in FY 2006:

- Maintained high-alert posture and monitored, analyzed, and assessed issues potentially impacting the communications infrastructure as a result of Hurricane Wilma. Actively tracked and communicated pre- and post-landfall response activities in coordination with ESF-2 partners, field components, and telecommunications industry membership;

- Conducted regular conference calls with NCC Industry and Government members to identify assets and communication conditions for area(s) impacted by Hurricane Wilma;

- Assisted telecommunications industry partners with access and fuel issues related to restoring communications in area impacted by Hurricane Wilma;

- Designed, developed, and implemented automated tools supporting ESF-2 activation and coordination [including ESF-2 Local Area Network (LAN), CAD, Master Station Log (MSL)];

- Supported the use of NCS priority telecommunications programs to assist in restoration of communications. GETS, Telecommunications Service Priority (TSP), and WPS programs were placed on alert and postured for assisting with priority communications needs;

- Established communications sector liaisons within the Homeland Infrastructure Threat and Risk Analysis Center to facilitate evaluation and monitoring of threats to the U.S. communications infrastructure;

- Developed the Emergency Wireless Protocol (EWP) to facilitate coordination with the cellular service providers requests for cellular service suppression in defined area(s). Began outreach endeavors with State and local emergency officials to increase awareness of EWP;

- Obtained accreditation certification of the MSL, which captures all watch activities, and NCC LAN infrastructure. Both systems are critical to the watch operational ability. Documentation was aligned to meet the DHS accreditation guidelines and helped DHS improve their Federal Information Security Management Act rating; and

- Expanded the NCC Industry membership to include new players, technologies, and sectors offering communications including satellite, cable, broadcaster, and associations.

Communications Information Sharing and Analysis Center

In 2000, the NCC was designated the ISAC for the communications sector per the guidance of the 1998 Presidential Decision Directive 63, *Protecting America's Critical Infrastructures.* This directive encouraged the private sector to establish ISACs to "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information." As part of the ISAC mission, information regarding threats, vulnerabilities, intrusions and anomalies is collected from the communications industry, Government and other sources and then analyzed with the goal of averting or mitigating impacts on the communications infrastructure.

Major ISAC Activities in 2006:

- Continued development and orchestration of cross-sector forum discussions with other ISACs for the purpose of identifying interdependencies and cross-sector vulnerabilities;

- Participated in NCC/Industry conference calls to identify assets and communications conditions for area(s) impacted by Hurricane Wilma;

- Staged generators, ice, food, fuel, water and personnel for quick response to restoring communications impacted by Hurricane Wilma;

- Worked with NCC to address issues with access and fuel as related to restoring communications in area impacted by Hurricane Wilma; and

- Participated with NCS in exercises designed to test ability of Federal Government and private Industry to respond to Incidents of National Significance. These exercises included:

  - Cyber Storm (February 6–10);

  - Blue Cascades (March 1–2);

  - DHS Grants and Training Hurricane Tabletop Exercises (May 3–June 21);

  - ESF-2 Training Workshop (May 20-26); and

  - Forward Challenge/TOPOFF (June 19–22).

Operational Programs

Shared Resources High Frequency Radio Program

The SHAred RESources (SHARES) High Frequency (HF) Radio Program is a key element of the developing NS/EP infrastructure. SHARES provides the Federal emergency response community with a single, interagency emergency message handling system for the transmission of NS/EP information. It brings together existing high frequency radio resources of Federal and federally affiliated organizations to include telecommunications industry and critical infrastructure providers when normal communications are destroyed or unavailable.

The SHARES HF Interagency Working Group, consisting of 154 members representing 110 organizations, provides guidance and direction for the SHARES network to provide the Federal community a forum for addressing issues affecting HF radio. This body conducts three nationwide readiness exercises each calendar year. The overall exercise objectives are to provide personnel training on operating procedures and various message formats, expand SHARES awareness within the Federal emergency response community and assess the interoperability of new HF technologies.

During FY 2006, SHARES was activated to a heightened state of readiness in support of Hurricane Wilma on October 24, 2005, as well as Tropical Storm Ernesto on August 29-30, 2006. In addition, SHARES conducted nationwide SHARES exercises on April 19 and October 4, 2006. The April 19th exercise designated as "Howling Wind," had radio participation by 54 Federal SHARES stations and 231 federally affiliated SHARES stations. The October 4th exercise, designated as "Operation Messenger," had over 550 participants.

Telecommunications Service Priority Program

The TSP Program, established by a FCC R and O dated November 17, 1988, provides the regulatory, administrative, and operational framework for the priority provisioning and restoration of qualified NS/EP telecommunications services. The FCC authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments.

Currently there are over 109,000 total active TSP assignments in support of NS/EP communications. During FY 2006, over 32,000 TSP codes were added, changed or revoked. Additionally, the TSP user base increased by approximately 128 new organizations bringing the total number of organizations with active TSP codes to over 680.

Network Security Information Exchange Activities

The NSIE was established in 1991 at the recommendation of the President's NSTAC to establish a industry-Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. In FY 2006, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including corporate patch management, the threat management process, and the effects of extreme events such as widespread power outages, pandemics or terrorist attacks on the telecommunications network. During FY 2006, the NSIEs participated in several conference calls to provide immediate assistance to NSIE member organizations when urgent security concerns arose. The NSIEs also produced a white paper on peer-to-peer communications and a document pertaining to the security issues of the next generation networks, titled *Security Implications of Next Generation Networks (NGN)*.

The NSIEs also engage in international outreach activities. NSIE representatives worked closely with British Telecom to assist with the establishment of a UK

NSIE in 2003. Following the eighty-third meeting (May 2005) of the NSIEs in Ottawa, Canada, Industry Canada established an NSIE-like entity in Canada (Canadian NSIE). A joint meeting of the UK, Canadian, and U.S. NSIEs is planned for Spring 2007.

Alerting and Coordination Network

The ACN was designed to provide a survivable emergency communications network connecting critical telecommunications service providers' network operations and/or emergency operation centers with key federal entities. The ACN reached a technical and contractual program milestone in 2006 that prompted the NCS to take a fresh look at the legacy technical requirements and current architecture. During 2007, the NCS will initiate implementation of new ACN capabilities and technical architecture.

Contingency Planning Branch

In FY 2006, the Contingency Planning Branch was created to provide a greater focus on the development of doctrine and operational plans within the CIP division. This branch translates these plans into tools and learning aids to effectively assimilate key concepts, roles and responsibilities to ECT members. As the NCS' regional presence grows in the coming years, the CP Branch will provide guidance and oversight to the Regional Communications Coordinators in each of the 10 Federal regions.

Contingency Planning

CP focuses on contingency communications planning and has primary responsibility for development and publication of the ESF-2-Communications Operations Plan (OPLAN), the NCS Continuity of Operations (COOP) Plan, the COOP Multi-Year Strategy and Program Management Plan (MYSMP), and numerous communications support documents.

The OPLAN augments the ESF-2 Communications Annex to the NRP. The OPLAN defines the organizational structures that form when ESF-2 is activated to support an Incident of National Significance and outlines the roles and responsibilities of all ESF-2 supporting agencies under the NRP and the *National Plan for Telecommunications Support in Non-Wartime Emergencies.* In FY 2006, the first version of the OPLAN was approved with inputs from all ESF-2 stakeholders. Version IV of the OPLAN is currently under review by the HSC's Policy Coordination Committee.

The COOP plan identifies the NCS mission essential tasks that must be performed to continue the NCS mission from an alternate location if its primary facilities become uninhabitable for a prolonged period of time. The plan identifies the personnel required to perform these functions and additional elements associated with relocation. The MYSMP is the essential document that defines the NCS roadmap for developing a viable COOP capability over the next 5 years. The MYSMP identifies resource and budget requirements that will enable NCS to achieve an effective, proven COOP capability and provides a schedule for completion of required actions.

Preparedness Tools

CP is responsible for the development of job aids to translate National plans (such as, NRP, Joint Field Office Standard Operating Procedures (SOP), ESF-2 OPLAN) into specific tasks for ECT members. These tools are designed to reduce inefficiency by providing information on specific positions so that any official could perform the tasks associated with that position.

In addition to these job aids, CP produces SOPs to provide direction, improve communication, reduce training time and enhance work consistency. SOPs are general guidelines promulgated by CP to promote a cohesive approach to responding to an incident of national significance.

Regional Infrastructure

As a result of the CIP Division's examination of Hurricane Katrina response, the requirement for a more robust regional presence was identified. To satisfy this requirement, the division developed a plan to staff two full-time NCS team members at each Federal region. These team members, a GS-15 Regional Communications Coordinator (RCC) and a GS-13 Deputy RCC, will report to the CP Branch Chief. While this plan is in its infancy, the division has taken concrete steps to realize this goal.

During FY 2006, contractor personnel have been assigned to Federal regions IV (Atlanta, GA), VI (Denton, TX), and VIII (Denver, CO) to serve as RCCs. During FY 2007 and FY 2008, CP intends replace these contractor staff with permanent Federal employees and well as staff the remaining RCCs and all Deputy RCCs throughout the country. RCCs conduct regional emergency communications conferences; attend emergency response planning conferences; participate in national, regional and local exercises; aid national, regional and local officials in planning for incidents of national significance; and establish and strengthen relationships with Federal agencies, State and local officials and private industry.

In FY 2006, the Region VI and IV RCCs participated in drafting the Gulf Coast Emergency Communications Plan, focused on identifying and mitigating communications vulnerabilities for coastal counties/parishes in Louisiana, Mississippi, and Alabama. In the event of a disaster, the NCS' ECTs will be responsible for the execution of these emergency communications plans.

Operational Analysis Branch

The OA Branch 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. In FY 2006, the OA Branch focused on improving the quality, comprehensiveness and timeliness of telecommunication analytic products. Initiatives conducted during FY 2006 include:

Analysis Response Team

The increasing demand for complex, real-time analyses during emergency response operations highlighted a need for a coordinated analytic response across several entities of the NCS and Federal government. In response to that need, the OA Branch established the Analysis Response Team (ART) in FY 2006. The ART brings together representatives from the OA Branch, the NCC Watch, the NCS Technology and Standards Division, and the FCC. Each participant brings a unique set of knowledge, skills and data that jointly contribute to a comprehensive analysis of the telecommunications infrastructure. During an emergency response event, the ART will be activated to work on-site at the NCS to meet the operational needs of the NCC Manager. During this report period, the ART developed and exercised standard operating procedures and pre-formatted report templates which will be applied for all assessments.

Regional Characterization

In an effort to improve the ability to quickly and accurately provide critical telecommunication assessments, especially during an emergency response operation, the OA Branch initiated a series of in-depth regional characterizations of the telecommunications infrastructure throughout the country. The goal of these characterizations is to establish and document a comprehensive understanding of the communication services supporting NS/EP missions in high-risk areas prior to an emergency event. This significantly reduces the preliminary research and data gathering time normally associated with any analysis.

As part of these characterizations, the OA Branch is coordinating with key NS/EP stakeholders to better understand their specific communication services and engineered architectures supporting their critical missions. The results of these studies are incorporated into the NCS analytical tools and models used to support telecommunication assessments. During FY 2006, the OA Branch initiated characterization studies in the metropolitan areas of San Francisco, Miami, and Philadelphia. In addition, the OA Branch assisted the communication planning efforts in the Gulf Coast Region by conducting a high level baseline analysis of the entire state of Louisiana, and more detailed analyses of seven high-risk Louisiana parishes and four high-risk counties in Mississippi.

State and Local Requests for Critical Telecommunications Information

With an increased occurrence of natural disasters and the threat of additional terrorist activity, State and local entities have a need for critical infrastructure information to support their emergency planning initiatives. During FY 2006, the OA Branch coordinated with the NCC's industry members to develop and implement a process for the NCS to serve as the focal point for addressing State and local emergency planner's requests for sensitive telecommunication information within their jurisdictions. During this reporting period, the OA Branch responded to requests from the States of Washington and Michigan, and the city of Houston. In addition, the OA Branch worked closely with the DHS's Protected Critical Infrastructure Information (PCII) Program Office to initiate the establishment of an NCS PCII officer which will allow the NCS to receive, process and protect, via the PCII authority, information related to requests for sensitive telecommunications data.

Prioritization of Telecommunications Assets

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 degree of vulnerability resulting from a physical attack on the Nation's critical infrastructures. In addition, Homeland Security Presidential Directive 7 (HSPD-7) *Critical Infrastructure Identification, Prioritization, and Protection* establishes a national policy for identifying, prioritizing and protecting critical infrastructure assets. During FY 2005, the OA Branch initiated analysis to prioritize telecommunications assets in relation to consequences described in HSPD-7. During FY 2006, the OA Branch expanded upon that methodology by incorporating an economic metric to evaluate potential economic impacts associated with the loss of portions of the telecommunications infrastructure. Using data that estimates the gross domestic product (GDP), the OA Branch prioritized telecommunications assets based on the amount of GDP potentially supported at each location housing telecommunications assets. These results will be integrated with analyses of other aspects of the HSPD-7 consequences to develop a composite listing of important telecommunication assets.

Undersea Cable Analysis

The United States relies heavily on the undersea cable system for international communications. The dependence of the Government communications on these international seabed networks, along with worldwide integration and linking of economies, has raised the concern that the destruction or damage to submarine cable facilities could severely impact the U.S. economy and national security. As a result, the Government is seeking to improve the resiliency of the undersea cable communications infrastructure as well as better prepare for service disruptions resulting from multiple cable failure scenarios. To this end, the OA Branch participated in a multi-agency working group led by the NSC. Each department and agency was asked to review four scenarios related to loss of service from major switching facilities, cable landing stations, and deepwater cables. Each department and agency identified their roles and responsibilities, then recommended plans and procedures to prevent, respond to, and mitigate known undersea cable threats and vulnerabilities. The working group identified potential follow on actions, designed to minimize disruption of international communications, and finalized a set of recommendations and resource requirements.

Training and Exercise Branch

The TE Branch is responsible for ensuring a cadre of skilled civilian and military reservist personnel are ready to provide emergency response support during crises and emergencies. During FY 2006, the TE Branch successfully planned, coordinated and performed the following activities:

Emergency Response Training Seminars

Emergency response training seminars are intended to increase awareness of the mission and capabilities of the NCS; explain the NCS' role as the primary agency for ESF-2 within the NRP; and emphasize the best use of industry and Government communications resources. During FY 2006, seminars were presented to private industry and Federal, State and local government emergency planners and operators in Federal Region III (Mid-Atlantic) (Philadelphia) and Federal Region V (Great Lakes) (Chicago). This training program reached a combined audience of approximately 135 attendees.

NCS Individual Mobilization Augmentee Program

The NCS continued its Individual Mobilization Augmentee (IMA) Program, which provides a valuable resource of skilled Army Reserve personnel to augment telecommunications response activities. This program provides the NCS with a surge capability to deploy and react to a myriad of situations associated with ESF-2 operations. Some 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 IMAs may be activated and deployed to assist the NCS staff, or they may deploy to regional locations to assist during disaster response and planning.

During FY 2006, the NCS IMAs supported the response operations after Hurricanes Katrina and Rita by providing personnel at six locations (Washington, DC, Austin, Baton Rouge, New Orleans, Jackson, and Atlanta). During the long-term recovery phase, selected IMAs accepted continuous duty obligations in excess of 100 days. In response to the increased frequency and duration of duty deployments, the NCS IMA Unit increased its personnel strength to the current roster of 15 officers. The newer members received a two-day orientation and training session at the NCS which included a description of the NCS and its role under the NRP. The IMAs received briefings about the 2005 hurricane season; key NCS programs that provide communications services to assist the emergency planner and responder; the IMA training program; and relationships and coordination between the industry and Government on telecommunications matters. The augmentees also received a tour of the NCC and the FEMA-National Response Coordination Center.

ESF-2 Training

The response events of the 2005 Hurricane Season clearly demonstrated that the NCS' traditional ESF resources were inadequate to address the emergency response needs of a catastrophic event the magnitude of

Hurricane Katrina. Consequently, the ESF-2 Training and Response Improvement Program was initiated to address the deficiencies highlighted during Hurricane Katrina. The ESF-2 Training and Exercise program was modified to improve ESF-2 staff member's proficiencies with the revised ESF-2 plans, procedures and operational support systems, as well as reinforce their roles and responsibilities as outlined in ESF-2 Operational Plans.

From May 20-26, 2006, the NCS conducted a training event for 130 attendees dedicated to supporting ESF-2 during periods of crisis. The training, conducted at Homestead Air Reserve Base, Florida, focused on preparing attendees for the 2006 hurricane season.

During the classroom training, instructors from the telecommunications industry, FCC, FEMA, and DHS presented instruction in the following areas:

- ESF-2 operating procedures;
- Automated information management tools;
- Communications assessment techniques;
- Logistics and procurement procedures;
- Telecommunications fundamentals;
- NCS priority programs; and
- Communications equipment.

Attendees were given tours of the local dial central office in Homestead Florida, the Miami/Dade County Emergency Management Agency Operations Center and the Miami/Dade County 9-1-1 call center. The week culminated in a command post exercise in which attendees applied the knowledge gained throughout the week by playing their actual ECT roles in a hurricane response scenario.

ESF-2 Exercises

In preparation for the 2006 hurricane season, the DHS sponsored multiple exercises to assess the capabilities of Federal, State and local Governments and private industry to respond to incidents of national significance.
The NCS partnered with NCSD to plan and conduct Exercise CYBER STORM 05, which assessed the Federal Government's ability to respond to an Internet attack. NCS personnel also participated in the planning and execution of the following inter-agency events:

- Five DHS Grants and Training hurricane tabletop exercises (Regions I, II, III, IV, VI);
- Exercise TOP OFFICIALS 4; and
- FORWARD CHALLENGE 06.

Additionally, ESF-2 personnel participated in the following exercises that were sponsored by regional or state emergency management organizations:

- BLUE CASCADES IV (Region X);
- Louisiana Emergency Evacuation Exercise (Region VI); and
- Regional COOP exercises.

GSA demonstrated its continuing commitment to the ESF-2 mission by providing a significant number of personnel to perform team leadership roles during the above listed exercises.

PLANS AND RESOURCES

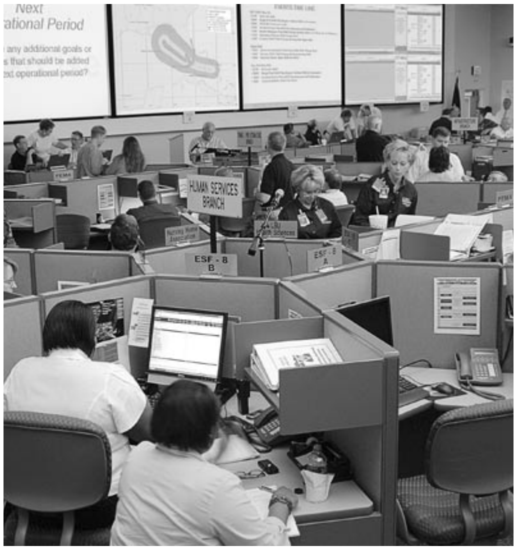
The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, manpower allocations, and other human capital related matters. The Plans and Resources Division exercises authority 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 Execution System (PPBE) 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 business plans, performance plans, future year homeland security planning documentation, advanced acquisition plans, and budgetary expertise to strategic planning efforts.

The Planning Team, through the implementation of the strategic and performance plans, comprehensively evaluates organizational performance and effectiveness. The OMNCS develops 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 PPBE-related documentation for the OMNCS, including documentation for program objective memoranda, budget estimates, the President's Congressional Justification 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 and strategies, 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

President Ronald Reagan—through E.O. 12472 established the NCS Committee of Principals (COP) in 1984 to provide advice and recommendations on NS/EP telecommunications to the Executive Office of the President (EOP). The President designates the COP membership, which is composed of senior-level officials representing 23 Federal departments and agencies with telecommunications facilities or services significant to NS/EP activities.

As an interagency forum, the COP serves as a means for the member departments and agencies to exchange ideas, coordinate interagency activity, and form recommendations on current and emerging telecommunications issues to be delivered directly to the Manager of the NCS, the Secretary of Homeland Security, and the President. Each COP Principal provides the position of its parent organization on NS/EP issues as well as comments and recommendations on current and prospective NCS programs to the NCS; the HSC; the NSC; the OMB; the OSTP; and the Executive Agent. Additionally, the COP performs any other duties that may be assigned by the President or his authorized designee.

The COP meets at least twice each year, as provided for in NCS Manual 1-2-1, *Bylaws of the National Communications System Committee of Principals*. COP meetings provide members with an opportunity to engage in high-level discussions to determine effective policies and activities on matters of importance to NS/EP telecommunications.

In FY 2006, the COP engaged in several efforts designed to improve the Nation's NS/EP telecommunications posture. Specifically, the committee received briefings from the OMNCS on the damage sustained by the communications infrastructure and the performance of the priority communications services during Hurricanes Katrina, Rita and Wilma. In addition, the COP conducted a detailed discussion on the activities undertaken within each member department and agency in preparation for the 2006 hurricane season and responded to a call for volunteers to commit surge support to the OMNCS in the execution of ESF-2—Communications responsibilities. In addition, the COP provided comments on the development of the ESF-2 Operations Plan as well as the NCCC Terms of Reference document. Members also participated in a briefing on the use of route diversity as a means to achieve network resiliency in situations such as catastrophic hurricanes. At the request of the EOP, COP members provided comments on draft NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities.* Furthermore, the COP also reviewed the recommendations made to the President by the NSTAC in May 2006 and provided the EOP with the NCS member departments and agencies perspective on those recommendations for consideration during its subsequent review. Finally, the COP oversaw and directed the activities of its two active working groups—the CCWG and the Priority Services Working Group (PSWG) —which are further explained below.

Continuity Communications Working Group and the Continuity Communications Architecture Program Office

In May 2006, the COP reconstituted the CCWG to oversee the activities of the Program Office. The Program Office is charged with developing a Continuity Communications (CC) FEA and Framework to enable FEB departments and agencies to perform their PMEFs and NEFs under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

In April 2006, the Program Office provided a program plan to the CCWG, which outlined the office's primary mission. To accomplish this mission, the Program Office has undertaken three primary tasks: (1) the production of draft NCS Manual 3-10-1 *Minimum Requirements for Continuity Communications Capabilities User Manual* to accompany NCS Directive 3-10; (2) the continuation of departments and agencies NEF/PMEF efforts, including an analysis of the ability of departments and agencies to perform their PMEFs using current communications capabilities under all conditions; and (3) the research of collaborative and mobile solutions that can be used to further enhance continuity communications.

Draft NCS Manual 3-10-1 provides detailed communications services descriptions, mandatory operational standards, and interoperability requirements for continuity communications capabilities within FEB departments and agencies headquarters and alternate/COO facilities. The Manual serves as a guide to achieve full compliance with draft NCS Directive 3-10 by outlining the requirements to meet each type of essential communications. The minimum communications requirements are assigned by category as defined in Federal Preparedness Circular 60, *Continuity of the Executive Branch of the Federal Government during National Security Emergencies,* which is currently being revised. The FEB departments and agencies are assigned to one of four categories commensurate with their responsibilities in response to national security emergency conditions. Category I departments and agencies are assigned the highest level of emergency response responsibility, while Category IV departments and agencies have the lowest level of emergency response responsibility.

Under the NEF/PMEF analysis activities, the Program Office will review the specific information technology (IT)/ communications infrastructures supporting each departments and agencies PMEF to identify any operational gaps that would prevent departments and agencies from performing their PMEFs. To accomplish this activity, the Program Office is in the initial phases of developing a:

- CCA Metamodel to define the "As-Is" and "To- Be" CC architectures across three major components: environment/situation (including the scenarios under which the departments and agencies must operate); operations/business (including what the departments and agencies must do in any given scenario); and infrastructure (including the facilities, communications systems, IT systems and other capabilities the departments and agencies use to accomplish their priority mission functions);

- CCA data input toolset to gather the departments and agencies infrastructure data needed to perform an assessment of an organization's readiness. The toolset will be operationalized and tested prior to the onset of the official data gathering effort; and

- Departments and agencies data collection process that will be comprehensive and as minimally invasive as possible so as not to overburden the departments and agencies as they provide the requested CCA data.

Additionally, the Program Office will work with OSTP and the Science and Technology Policy Institute,[12] to begin to normalize departments and agencies PMEFs and Secondary Mission Essential Functions.

The Program Office's collaborative and mobile solutions research effort will study existing departments and agencies solutions for potential FEB-wide implementation, including COTS and GOTS solutions.

Priority Services Working Group

Established in December 2003, the PSWG's scope of work called for the group to undertake four activities: (1) an evaluation of the NCS' GETS, TSP, and WPS; (2) an examination of priority service outreach efforts; (3) an assessment of cost issues; and (4) an analysis of the potential impact of future technologies on priority services programs. The group's initial study examined TSP according to the four tenets of its scope of work.

During FY 2006, the PSWG incorporated edits from the TSP Oversight Committee to its draft report and recommendations. The working group then submitted its *Final Report on the Telecommunications Service Priority Program* to the COP for its review and approval on June 9, 2006. The report will be forwarded to the DHS and the EOP once approved by the COP.

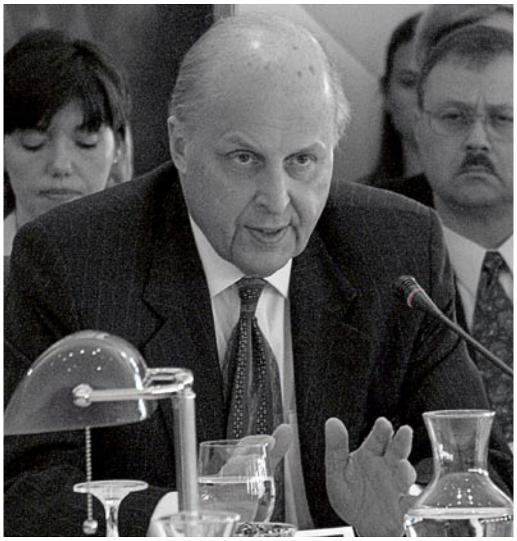
Moving forward, the working group plans to examine GETS and WPS according to the four tenets of its scope of work, and make recommendations regarding strategies to improve the visibility and participation levels of both priority service programs.

Council of Representatives

The Council of Representatives (COR), the permanent subordinate working body of the COP, met in August 2006 to receive briefings from members of the NSTAC's Industry Executive Subcommittee (IES). The IES members provided an overview of recent NSTAC correspondence with the President on three important topics related to NS/EP telecommunications—NGN; emergency communications and interoperability; and the NCC. During the session, COR members engaged in a dialogue with IES members on the NSTAC's specific Presidential recommendations, the potential impact these recommendations will have on NS/EP telecommunications, and the establishment of a process through which the COP and COR can socialize NSTAC recommendations within the broader Federal NS/EP community. The COR also received a briefing from the OMNCS on existing alert and warning notification lists and discussed methods for ensuring that COP and COR members are formally alerted to events of national significance, both natural and man-made.

The President's National Security Telecommunications Advisory Committee

E.O. 12382, *President's National Security Telecommunications Advisory Committee,* established the President's NSTAC in September 1982. The NSTAC is a Presidentially-appointed advisory committee consisting of no more than 30 industry chief executives from major communications, network service provider, information technology, finance, and aerospace companies.



Ambassador John Negroponte, the Director of the Office of National Intelligence, addresses questions and concerns by members of the President's National Security Telecommunications Advisory Committee during their Executive Session held in Washington May 9. *(Photo by Robert Flores, Defense Information Systems Agency)*

The NSTAC held its 29th Annual Meeting on May 10, 2006, in Washington, D.C., at which time the NSTAC Principals and senior Government officials reviewed the activities of the past cycle and discussed emerging issues for consideration during the NSTAC XXX Cycle. The NSTAC also met quarterly via conference call. Topics discussed included network convergence, telecommunications and electric power interdependency, and emergency communications and interoperability.

Industry Executive Subcommittee

During FY 2006, the NSTAC's IES continued to identify communications issues critical to NS/EP activities for consideration by its subgroups. The NSTAC addressed a variety of issues, including: the provisioning of NS/EP services over the NGN; international implications of the NGN; emergency communications and interoperability; telecommunications and electric power interdependency; the evolving role of the NCC; NSTAC outreach efforts; research and development (R&D) issues; global infrastructure resiliency; and legislative and regulatory issues. Specific subgroup activities and the results of their analysis, work, and recommendations to the President are discussed further below.

The IES also received several briefings during the year to inform its activities, including:

- an overview of U.S. military disaster recovery activities,
- a briefing on the U.S. Northern Command's (USNORTHCOM) Ardent Sentry Exercise,
- an update on the ATIS's National Diversity Assurance Initiative from the Federal Reserve Board,
- a briefing on the NCSD's Cyber Storm Exercise,
- an overview of the Public Safety and Homeland Security Bureau from the FCC, and
- a briefing on the North American Aerospace Defense Command (NORAD) USNORTHCOM plan for communications interoperability.

Next Generation Networks

Throughout FY 2006, the NSTAC, through its NGN Task Force (NGNTF), continued to examine NS/EP requirements for and emerging threats to the NGN. Following the submission of its *Near Term Recommendations Report* in March 2005, the committee undertook an extensive long-term tasking, creating working groups with deep subject matter expert involvement to thoroughly address the following five fundamental issue areas: (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. Ultimately, the committee, based upon the work of the task force, agreed upon nine recommendations, the implementation of which would support the ability of the NGN to meet NS/EP functional requirements while also providing greater capabilities to NS/EP users.

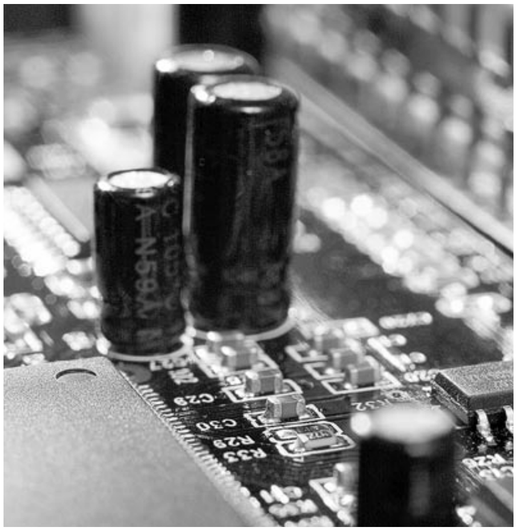
The NSTAC offered the following recommendations to the President in April 2006 in its *Report to the President on Next Generation Networks:*

- **Identity Management.** Direct the OMB, the Department of Commerce (DOC), and DHS to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos," allows federation between the Government and commercial domains, and supports use of Government issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy;

- **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services.** Direct OSTP, with support from the collective NCS agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be an industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs that would foster NS/EP capabilities within the NGN, including initiatives concerning:

  – A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and

  – NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IP version 6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IP security for authentication and confidentiality;



- **Research and Development.** In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and DOD to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers;

- **Technology Lifecycle Assurance and Trusted Technology.** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities;

- **Resilient Alternate Communications.** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged, or diminished access to the communications infrastructure;

- **Agreements, Standards, Policy, and Regulations.** Direct DHS, DOS, and DOC (including NIST and the NTIA) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally distributed NGN environment;

- **Incident Management on the NGN.** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the NCC, for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program;

- **International Policy.** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non U.S. companies in NS/EP incident response in the U.S.; and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment; and

- **First Responders.** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

The NSTAC sunset the NGNTF in June 2006.

National Coordinating Center

Throughout FY 2006, the NSTAC, through its NCC Task Force (NCCTF), continued to investigate the long-term direction of the NCC, including but not limited to: (1) where the NCC should be in one year, three years, and five years; (2) how the NCC should continue to partner with Government; (3) how the NCC should be structured; and (4) how the new DHS Sector Coordinating Council approach could impact the NCC.

The committee deliberated on numerous issues, focusing its discussions on the NCC's organizational structure, information sharing and analysis, leadership, incident management and response, and international mutual aid. To gain additional insight into incident management, and information sharing practices in particular, the NCCTF co-hosted an all-day incident management subject matter expert Meeting with the NGNTF on August 30, 2005. The committee also incorporated lessons learned from Hurricane Katrina and insights from the White House report on Hurricane Katrina in making recommendations on improved coordination between industry and Government.

Based on the analysis conducted by the NCCTF, the NSTAC recommended that the President:

- Direct the Secretary of Homeland Security, the Director of the OSTP, the Secretary of Defense, and other ESF-2 Federal support agencies to develop and implement policies and procedures with respect to: (1) managing and escalating requests from the NCC, and (2) the delineation of authorities and responsibilities when ESF-2 is invoked;
- Direct the OSTP and the HSC to join with the Communications Sector Coordinating Council (CSCC) and the IT Sector Coordinating Council to support an industry-led task force with the primary goal of planning a regional communications and information technology coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and information technology coordinating capability that can serve all regions of the Nation. The task force should primarily be made up of industry representatives, as well as Federal, State, and local Government representatives;
- Direct the Secretary of Homeland Security to expand the NCC to include both communications and IT companies and organizations. This would be a cross sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies;
- Direct the Secretary of Homeland Security to engage the private sector in CIP activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information;

- Direct the Secretary of Homeland Security to improve the ESF-2 Emergency Response Training and Exercise program, with a focus on enhancing coordination among industry members and Federal, State, and local responders during incidents of national significance. This program should focus on sector interdependencies for both physical and cyber threats, and would aim to produce actionable results. Industry must be involved from the earliest planning stages;

- Encourage the Secretary of Homeland Security to improve the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the private sector in the NRP, aligning communications and cyber operations centers, and enhancing relationships with international computer emergency readiness teams; and

- Direct the Secretary of Homeland Security and other Government stakeholders to examine the value received from the NCC relationship and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission.

To further these recommendations, the committee developed a roadmap of action items for the NCC to assist it in evolving to address new issues and challenges over the next five years. The NCCTF remains active to conduct further NCC analysis on an ad hoc basis per the direction of the NSTAC Principals.

Telecommunications and Electric Power Interdependencies

Throughout FY 2006, the NSTAC, through its Telecommunications and Electric Power Interdependency Task Force (TEPITF), continued to examine the NS/EP implications associated with the significant interdependencies between the telecommunications and electric power sectors. The analytic efforts conducted by the TEPITF included the participation of a significant number of companies from both the U.S. and Canadian telecommunications and electric power sectors as well as representatives from other bodies such as Industry Canada, the Institute of Electrical and Electronics Engineers, the NCS, and National laboratories.

The NSTAC tasked the TEPITF to evaluate how sector interdependencies will affect the future of the telecommunications network. The effort was subsequently divided into two work streams: the first examined the people and processes involved in national emergency communication and restoration; the second will examine the technological implications of future events.

In January 2006, the NSTAC finalized its *People and Processes: Current State of Telecommunications and Electric Power Interdependencies Report* in which the Committee recommended that the President direct his departments and agencies to:

- Define and establish the term Emergency Responder within the NRP and other appropriate plans, guidance, directives, and statutes, including other local, State and Federal Government emergency plans;

- Ensure key response personnel of critical infrastructure owners and operators in the telecommunications and electric power sectors be designated as emergency responders;

- Include fuel supply, security, site access, and other required logistical support to critical telecommunications and electric power infrastructures as part of the Emergency Responder planning process to ensure priority restoration to critical telecommunications and electric power;

- Foster and promote effective emergency coordination structures to ensure reliable and robust communication between the two sectors and local, regional, State, and Federal governments;

  - Review examples of proven priority restoration models at the State and regional levels. Encourage States and metropolitan regions without effective models to improve and update their existing frameworks;

  - Encourage effective information sharing models at the local/regional Emergency Responder level, both in advance of a natural disaster and during the emergency restoration period. When developing these models, liability issues should be considered.

The committee is currently focusing on the second work stream, exploring a working definition for a long-term outage and reviewing the possible interdependency implications of a long-term outage. Based on its analysis and conclusions, the NSTAC plans to develop its long-term report and recommendations in the fall of 2006.

Emergency Communications and Interoperability

In the wake of the devastating 2005 hurricane season and as a result of the discussion conducted during the December 8, 2005, NSTAC Principals' Hurricane Katrina Response Working Group Meeting, the committee determined the need to provide recommendations to the President on short-term interoperability solutions for responders in advance of the 2006 hurricane season. Furthermore, the committee also agreed on the need to conduct a long-term study that: (1) examines the impact on emergency communications in the aftermath of a catastrophic event that significantly damages the fixed telecommunications infrastructure; (2) investigates how a complete suite of communications technologies, including wireline, terrestrial wireless, broadcast, and satellite communications, should be integrated into the Federal Government's emergency communications planning to more effectively support NS/EP activities; and (3) identifies rapidly deployable interoperability solutions and recommend a strategic direction for the future that can assure a more survivable and interoperable nationwide communications architecture for responders. Additional consideration will be given to the need to develop recommendations on how to educate the Federal Governments departments and agencies, State and Local Governments, first responder communities, and emergency responder communities on technologies currently available to meet their NS/EP communications needs.

To accomplish the required analysis, the committee established the Emergency Communications and Interoperability Task Force. Based upon the task force's initial investigations, the NSTAC provided short-term recommendations in its *Letter to the President on Emergency Communications and Interoperability* in April 2006, which outlined emergency communications and interoperability issues and identified immediately applicable actions to improve responder communications capabilities. The NSTAC recommended that the President direct DHS to:

- Establish a uniform protocol working with Federal, State, and local Government organizations that can dynamically identify their emergency management and coordinators' contact information, especially during times when regular contact information is changed due to event situations, and a capability to share that information with DHS;

- Accelerate efforts to create an initial deployable communications capability for the Gulf Coast region in accordance with Recommendation #37 of the February 2006 White House report, The *Federal Response to Hurricane Katrina: Lessons Learned* (Lessons Learned Report); and

- Formally integrate the NCS' NS/EP priority programs into the *National Emergency Communications Strategy* pursuant to Recommendation #34 of the Lessons Learned Report.

Additionally, the NSTAC recommended that the President direct the NTIA to work in conjunction with the FCC to streamline the authorization process for use of Federal incident response frequencies by the larger non-Federal Government emergency response community.

The NSTAC expects to finalize its long term analysis by the end of 2006.

International

At the NSTAC XXIX Meeting on May 10, 2006, the NSTAC Principals agreed that the international concerns raised during the NGN examination warranted further investigation during the NSTAC XXX cycle. The NSTAC conducted its issue scoping activities in June 2006 during which the committee hosted four subject matter expert meetings, eliciting expertise from industry and Government with experience in the areas of policy development, international relations, operational control (such as cyber incident response), standards and protocol development, intelligence, and internationally significant infrastructure.

Based on the findings from the subject matter expert meetings and the unanimous opinion of the Principals, the NSTAC determined that an International Task Force should be established to assist the Principals in further examining international operational and policy framework concerns related to NS/EP services on the global network. Issues for initial consideration include: (1) International network security environment and related incident response capabilities; (2) Analysis of existing and proposed international policy frameworks; and (3) Advancing U.S. leadership in emerging international network security issues, including security standards activities and adequacy of industry involvement.

The task force commenced its investigation in September 2006. The committee plans to send a near term report to the President in the fall of 2006 and expects its long term examination to extend into late 2007.

Cellular Shutdown

As a direct result of the bombings that took place in the London transportation system in July 2005, U.S. authorities initiated the shutdown of cellular network services in the Lincoln, Holland, Queens, and Brooklyn Battery Tunnels. The Federal Government based this precautionary measure on the suspicion that similar attacks might also be perpetrated in the tunnels leading to and from New York City. Though the decision was rooted in vital security concerns, the resulting situation, undertaken without prior notice to wireless carriers or the public, created disorder for both Government and the private sector at a time when use of the communications infrastructure was most needed. Shortly following these activities, the NCC hosted a teleconference to discuss the need to develop a process for determining if and when cellular shutdown activities should be undertaken in the future in light of the serious impact these efforts could have had, not only on access by the public to emergency communications services during these situations but also on public trust in the communications infrastructure in general.

These actions highlighted, within the NSTAC community, the need for a process to ensure that future similar decisions meet the Nation's security goals and ensure the protection of critical infrastructures. Consequently, the NSTAC established a Principal-level task force which worked throughout the fall of 2005 to formulate recommendations to effect efficient coordinated action between industry and Government in times of national emergency. To facilitate more coordinated action, the NSTAC recommended that the President direct his departments and agencies to:

- Work to implement a simple process, building upon existing processes, with DHS/NCS coordination enabling the Government to speak with one voice, provide decision makers with relevant information, and provide wireless carriers with Government-authenticated decisions for implementation; and

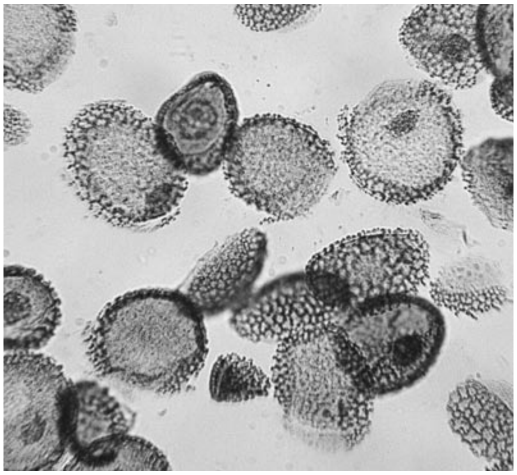
- Achieve rapid implementation through the Homeland Security Advisor of each State, in conjunction with the NCS and the Office of State and Local Government Coordination, DHS.

The working group concluded its activities upon NSTAC approval of the *Letter to the President on Cellular Shutdown* in January 2006.

Global Infrastructure Resiliency

In June 2006, the NSC requested the assistance of the NSTAC in conducting an expedited examination of the global resiliency of the telecommunications infrastructure. To accomplish the tasking, the committee established the Global Infrastructure Resiliency Working Group. The NSTAC plans to submit its report to the NSC in October 2006.

Influenza Pandemic



On June 15, 2006, Mr. Earl Nye, National Infrastructure Advisory Council (NIAC) Chair and Chairman of TXU, sent a letter to Mr. F. Duane Ackerman, Chief Executive Officer of BellSouth and Chair of the NSTAC, requesting assistance from the committee on a study related to the impact of pandemic influenza on the Nation's infrastructure. The study was the result of a joint request to the NIAC from Secretary of Homeland Security Michael Chertoff and Secretary of Health and Human Services Michael Leavitt to assist the Government in establishing priorities for determining critical services that must be maintained during an influenza pandemic. Per the request of the NIAC, the NSTAC appointed two IES representatives to represent the telecommunications sector on the working group tasked with conducting the research and analysis to accomplish the task. The NIAC plans to submit its report to the President on priorities during pandemics in October 2006.

Research and Development

During FY 2006, the Research and Development Task Force (RDTF) continued to pursue issues identified at the October 2004 Research and Development Exchange (RDX) Workshop and conducted its first ever international RDX Workshop. The task force focused its efforts on exploring mechanisms for R&D collaboration on NS/EP communications, examining the issue of authentication and identity management, and assessing the need for further study on the NS/EP implications of these issues by the NSTAC.

In July 2005, the RDTF continued to learn about R&D-related cooperative efforts across the Federal Government through presentations from the National Coordination Office for Networking and Information Technology R&D and the DOD on authentication and identity management initiatives underway within the Department. In June 2006, the task force received briefings from the Homeland Security Institute and the DHS Science and Technology Directorate on collaborative R&D efforts, including the *National Plan for Research and Development in Support of Critical Infrastructure Protection*.

On September 21-22, 2006, the RDTF conducted its seventh RDX workshop with the theme *International Collaboration on Cyber Security Research and Development: Leveraging Global Partnerships for the Security of Free Nations: an All Sector Preparedness and Response*. The workshop, the first to be held internationally in Ottawa, Ontario, Canada, focused on the need for international collaboration to enhance NS/EP communications. Mr. John Grimes, Assistant Secretary of Defense, Networks and Information Integration, and Chief Information Officer, DOD; and Ms. Patricia Sauvé-McCuan, Canada's Assistant Deputy Minister, Information Management, Department of National Defence, presented keynote addresses during the opening plenary session and moderated the concluding plenary

The Rotunda at the Ronald Reagan Building and International Trade Center housed the 29th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) on May 10. *(Photo by Robert Flores, Defense Information Systems Agency)* session, working with breakout session leaders to identify issues of importance for further investigation and study.

During the event, participants heard from leaders in industry and Government during plenary sessions, and actively participated in breakout sessions, which focused on the following five issues associated with the focus of the workshop's theme—international Internet governance, global-scale identity management, collaborative mechanisms for network security protocol R&D, cross-border and cross-sector challenges, and wireless and mobile ad hoc applications. From these sessions, six major findings regarding international collaboration on cyber security research and development emerged:

- Technologies and mechanisms to enable trust and build communities of interest are needed.

- International collaboration is essential for successful cyber security R&D initiatives.

- To advance cyber security research, leaders and practitioners must make investment decisions based on cost benefit analyses.

- To maintain the current security posture and improve future preparedness and response, NS/EP requirements must be embedded in new technologies and methodologies.

- Dynamic leadership and common frameworks are critical to achieve real progress in cyber security R&D.

- Strengthened education, awareness, and training programs increase the effectiveness of R&D partnerships and programs.

Legislative and Regulatory Issues

On January 31, 2006, the Committee completed its examination of the NS/EP issues many telecommunications infrastructure providers encountered during public and private sector response to Hurricane Katrina. During the October 13, 2005, Principals' Conference Call and the December 8, 2005, Principals' Hurricane Katrina Response Working Group Meeting in Washington, D.C., the NSTAC Principals discussed their companies' challenges when trying to restore telecommunications infrastructure damaged during the hurricane. They determined that telecommunications infrastructure restoration efforts were delayed when Federal officials interpreted laws and regulations in a manner that prevented telecommunications infrastructure providers from receiving the Federal support needed for their efforts. The Principals also concluded that were telecommunications infrastructure providers to be granted access to non-monetary Federal assistance including prioritized access to restricted areas, fuel, water, power, billeting, and workforce and asset security, response efforts could have been more efficient. The Principals subsequently tasked the Legislative and Regulatory Task Force (LRTF) with examining the NS/EP issues associated with telecommunications infrastructure restoration after Hurricane Katrina.

To ensure optimal future disaster response coordination between telecommunications infrastructure providers and Federal, State, local, and tribal Government, the NSTAC recommended that, no later than June 1, 2006, the President establish and codify the term, "Emergency Responder (Private Sector)" to include telecommunications infrastructure providers and ensure non-monetary assistance, including accessing restricted areas and obtaining fuel, water, power, billeting, and workforce and asset security, to them by:

- Directing DHS to modify the NRP and its Emergency Support Functions to designate telecommunications infrastructure providers as "Emergency Responders (Private Sector)" and to establish protocols and procedures for the way in which Federal, State, local, and tribal Governments should work with telecommunications infrastructure providers before, during, and after a national disaster;

- Issuing appropriate Presidential guidance to define "Emergency Responders (Private Sector)" under the *Robert T. Stafford Disaster Relief and Emergency Assistance* (Stafford) Act and other authorities as appropriate, to align with the broadened definition of "national defense" in the 2003 amendments to the *Defense Production Act* (DPA). Specifically, the guidance should make clear that key response personnel of critical telecommunications infrastructure owners and operators should be defined as "Emergency Responders (Private Sector)" and should receive non monetary Federal assistance under the Stafford Act; and

- Directing the Secretary of Homeland Security to work with Congress to align the Stafford Act and other appropriate legislative authorities with the DPA by codifying the designation of private sector telecommunications infrastructure providers as "Emergency Responders (Private Sector)" and by codifying the official interpretation that for-profit telecommunications infrastructure providers should receive Federal assistance.

Continuing with its examination of the NS/EP issues associated with the response to Hurricane Katrina, the committee, through the LRTF, analyzed the NS/EP communications

recommendations included in the Senate, House of Representatives, and the White House reports on Federal Government response to the 2006 hurricane season. The task force developed a list of NS/EP communications concerns to share with the IES.

The committee continued to examine NS/EP concerns associated with implementation of the *Support Anti-terrorism by Fostering Effective Technologies* (SAFETY) Act. The task force received a briefing from Ms. Wendy Howe, Office of SAFETY Act Implementation, DHS, on the Department's efforts to revise the SAFETY Act regulations and application kit. The LRTF agreed to continue to examine the issue of SAFETY Act implementation.

The committee concluded its examination of NS/EP issues associated with proposed amendments to the DPA and E.O. 12919, *National Defense Industrial Resources Preparedness,* which resulted from an Interagency Review of the DPA intended to update the DPA to include homeland security. The LRTF sent a thank you letter to the Interagency Group tasked to develop recommendations to amend the DPA and E.O. 12919. The letter expressed gratitude for the Interagency Group's commitment to remain engaged with the LRTF on the DPA amendment process and included the August 23, 2005, LRTF meeting summary highlighting the task force's concerns with the DPA and some proposed amendments.

Finally, the committee continued to address the implications of various legislation affecting NS/EP communications. Specifically, the LRTF examined H.R. 285, *Department of Homeland Security Cybersecurity Enhancement Act* of 2006; H.R. 6, *Energy Policy Act* of 2005; S. 1753, *Warning Alert and Response Network Act*; and telecommunications reform bills in both chambers of Congress.

NSTAC Outreach

The NSTAC Outreach Task Force (NOTF) operates to foster the exchange of information between key NSTAC stakeholders from both industry and Government on telecommunications-related NS/EP activities, on behalf of the Principals. The NOTF is tasked to: (1) raise the awareness of the NSTAC across industry, the Federal Government, 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 2006 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);
- Meeting with Admiral Timothy Keating, NORAD, and other representatives from NORAD and USNORTHCOM;
- Meeting with U.S. Air Force Lieutenant General Charles Croom, Jr., Director, Defense Information Systems Agency, and Director, Joint Task Force–Global Network Operations;

- Participating in several conferences to raise the awareness of the NSTAC, including:

  - The U.S. Telecom Association's Telecom 2005 Conference;

  - The 2006 Committee on National Security Systems Conference;

  - The Critical Infrastructure Resilience Conference; and

  - The DHS' SAFECOM Conference.

- Conducting the NSTAC Principals' Orientation in conjunction with the NSTAC XXIX Meeting.

HSPD-7 Coordinating Councils

The CSCC and the Communications Government Coordinating Council (CGCC) were established in the late spring 2005, to facilitate inclusive coordination of the policy development and infrastructure-protection planning within the sector. During their first year of operations, the CSCC and CGCC worked jointly on finalizing and implementing the Communications Sector Specific Plan, an annex of the NIPP. Other activities will include: broad-based planning; development of suggested practices and evolution of these practices over time to best-practice standards; promulgation of programs and plans; and development of requirements for effective information sharing, R&D, and cross-sector coordination.

The CSCC has also been involved in other activities such as the development of a regional coordinating capability to coordinate sector response activities during major events. In addition, several members of the council have also become involved in the Federal pandemic flu planning groups. Continuing through FY 2007, the CSCC will continue working on outreach to cable and broadcasting companies/trade associations.

The CGCC also will provide comments on other national preparedness-related plans.

NCS Issuance System

The NCS Issuance System, as outlined in NCS Directive 1-1, *National Communications System Issuance System*, and issued under the authority of E.O. 12472 is comprised of documents that establish, implement, guide, describe, or explain the NCS' organizational responsibilities, authorities, policies, and procedures. It includes directives, circulars, manuals, handbooks, notices, and OMNCS office orders. Directives, circulars, and manuals are binding on all NCS member organizations, as well as any other affected Federal entity.

Status of Issuances or Revisions Pending during FY 2006

The issuances listed below are currently being reviewed within the EOP, following the incorporation of edits from the NSC by the OMNCS. Following EOP review, these issuances will progress for signature to the Assistant to the President for Science and Technology and the Director of OMB:

- NCS Directive 1-1, *National Communications System Issuance System;*

- NCS Directive 1-2, *National Communications System Membership;* and

- NCS Manual 1-2-1, *National Communications System Committee of Principals By-laws.*

The following issuances are currently in development:

- Draft NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* (In coordination at EOP prior to consideration by the Assistant to the President for National Security, the NCS Executive Agent, the NCS Manager, and the NCS COP);

- NCS Manual 3-10-1, *Required Minimum Continuity Communications Capabilities;*

- NCS Handbook 3-10-1, *National Communications System Backup Dial Tone Project—Abridged Route Diversity Methodology Procedure;*

- NCS Directive 3-11, *Government Emergency Telecommunications Service;*

- NCS Manual 3-11-1, *Government Emergency Telecommunications Service Manual; and*

- NCS Directive 3-12, *Wireless Priority Service.*

The following issuances were revised as recommended by the NCS COP through its PSWG Administrative Changes Report for Top-Level National Communications System Priority Services Guidance:

- NCS Directive 3-1, *Telecommunications Service Priority* (Currently awaiting review and edification from OSTP); and

- NCS Directive 3-3, *Shared Resources (SHARES) High Frequency Radio Program* (Returned to internal coordination process for review and coordination recommended as a result of Hurricane Katrina After Action Report).

NCS Communications and External Affairs

The NCS answers inquiries 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 Preparedness Directorate to ensure that the Department approves all requests for interviews and information about the NCS.

Inquiries generally focused on the NCS emergency preparedness programs and their role with the DHS. Others focused on NSTAC, the NCC and its Communications ISAC; WPS, GETS, and TSP programs; the SHARES HF Radio 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 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.

The NCS Program Manager for Communications serves on a variety of DHS public affairs and external affairs committees. NCS is actively involved in the DHS Internal Communications Committee (including the DHS Intranet Subcommittee), the DHS Web Content and Design Committee, and the DHS Branding Committee. In addition, the NCS participates in all meetings of the DHS Preparedness Directorate and the Infrastructure Protection Branch dealing with external affairs activities.

Even though information services for the NCS are located on two different computer networks (DHS and Defense Information Systems Agency), the NCS continues to keep its employees informed and DHS internal communications issues. Those assigned to DHS facilities receive much of their DHS information through the "DHS-ALL" distribution maintained by the Department. This includes the weekly "DHS Today," press releases and fact sheets. However, the remaining NCS members (nearly 65 percent) at the DISA compound cannot access DHS Online and must still rely on forwarded information sent by the NCS Program Manager for Communications.

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

Outreach

The NCS continues to spearhead an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences. NCS representatives attend and participate in Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and critical infrastructure protection. Since the inclusion of the NCS in DHS in March 2003, there have been numerous opportunities for NCS leaders to

Department of Homeland Security Assistant Secretary for Infrastructure Protection Bob Stephan (left) listens as BellSouth Chairman and Chief Executive Officer F. Duane Ackerman addresses members of the President's National Security Telecommunications Advisory Committee (NSTAC) during their May 10 Business Session. Ackerman is the NSTAC Chair. *(Photo by Robert Flores, Defense Information Systems Agency)* 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.

Web Sites

The NCS Web Site (http://www.ncs.gov) provides information on the NCS and NSTAC (http://www.ncs.gov/nstac/nstac.html). The site contains NCS and NSTAC history, information about NCS programs and NSTAC activities, and online versions of NCS and NSTAC publications. The NCS also continues to work with DHS as the Department upgrades its own public site, as well as DHS Interactive (extranet) and DHSOnline (intranet).

Footnotes

[1] Federal Communications Commission Releases, STATISTICS OF COMMUNICATIONS COMMON CARRIERS, November 2005, http://www.fcc.gov.wcb/iatd/socc.html.

[2] Telcordia LERGTM Routing Guide.

[3] Telcordia GR-512 Reliability.

[4] Telcordia LERG Routing Guide.

[5] CTIA Semi-Annual Wireless Industry Survey, 2006 http://files.ctia.org/img/survey/2005_endyear/slides/EndYear_4.jpg.

[6] NSC Minutes from October 5, 2001 Meeting on Selected NS/EP Telecommunications Projects, Oct 9, 2001.

[7] Major areas impacted include, Denver and the western 3/4 of Colorado, Minneapolis/St. Paul, Sacramento and northeastern California, North and South Carolina, central Pennsylvania, Nevada (excluding Las Vegas), southwestern and northeastern Oregon, and southeastern Washington (state).

[8] The Honeynet project is a non-profit, volunteer, research organization dedicated to improving the security of the Internet. www.honeynet.org

[9] Dr. John H. Marburger III, Director Office of Science and Technology Policy, briefing to Enduring Constitutional Government Coordinating Council, September 27, 2005.

[10] David W. Howe, "Background Paper on Essential Functions Concept and Implementation and Recommended Guidelines for Submitting Department/Agency Priority Mission Essential Functions Information," January 10, 2005.

[11] The focus of the CCA effort is on the FEA BRM, DRM, SRM, and TRM. There is no explicit connection between the FEA PRM and the metamodel at this time.

[12] The Science and Technology Policy Institute is a federally funded research and development center that provides analytic support to the White House Office of Science and Technology policy.

IV

NS/EP Telecommunications Support and Activities of Member Organizations

DEPARTMENT OF STATE (DOS)

NS/EP Telecommunications Mission

Interagency Collaboration

The Department is committed to the enhancement of inter-agency communications and collaboration. 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 Intelink-Sensitive But Unclassified (SBU) (formerly known as the Open Source Information System) and Secret Internet Protocol Router Network (SIPRNet). State coordinates with other agencies through the Inter-Agency Collaboration Working Group chaired by the Deputy chief information officer for Business, Planning and Customer Service.

The Department has expanded greatly the publication of classified reporting on SIPRNet; through the Classified Homepage Program and the Net Centric Diplomacy initiatives, more than 200 embassies and bureaus publish to SIPRNet on web pages linked from the Department's gateway site at http://www.state.sgov.gov. The Department is also moving ahead to improve communications and collaboration among agencies via Intelink-SBU, 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 Intelink-SBU network, including consular data, administrative data, and information on State Department regulations and administration of embassy activities. In addition, the Department uses web log technology provided by Intelink-SBU to underpin more than a dozen communities of practice based on country, regional or functional interests.

The Department and the Agency for International Development 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. We are participating in each other's information technology (IT) Capital Planning and Investment processes and developing joint Office of Management and Budget Exhibit 300 submissions for major IT projects.

eDiplomacy

The Office of eDiplomacy aims to enhance the Department's leadership in formulating and implementing American foreign policy by promoting innovative technologies and effective knowledge management practices and initiatives domestically and overseas. Many of its programs are directly relevant to implementing Secretary of State Condoleezza Rice's vision for Transformational Diplomacy. The office oversees the ongoing extension of the accuracy and coverage of the enterprise search engine that it initially deployed in 2005. eDiplomacy has been the lead advocate for expansion of the Virtual Presence Post initiative, a new approach that combines traditional diplomatic outreach with web-based information to enable our overseas missions to systematically engage people in cities and regions where the United States does not have a permanent physical presence. eDiplomacy also has designed, launched and managed the initiative to foster use of online communities of practice to improve interagency knowledge-sharing and collaboration. The office champions the end user in information technology decision-making, including such developments as remote computing, teleworking, and satellite imagery and geospatial information systems. eDiplomacy is working to provide the means for Department personnel to use web logs and "wikis" as new tools to collaborate within State and with the Department's foreign affairs partners. The office also oversees the Department's Classified Homepage Program.

Secure Voice Program

The Department continues its Operations and Maintenance phase of the Secure Terminal Equipment (STE) program in FY 2006. All Secure Telephone Units have been recalled from the field for destruction or transfer to the National Security Agency. The Department currently has 4928 STE units deployed worldwide. The Department continues to evaluate newly introduced Secure Voice technology. Secure Voice is a constantly changing evolution covering everything from interoperability issues, configuration

DEPARTMENT OF STATE (DOS) - *continued*

management, key issues, etc. affecting all regions of the world. One of the most immediate issues on the horizon is Voice over IP (VoIP). Commercial telephone companies have already started to re-direct voice services to public network VoIP connections. This is causing severe and adverse affect on our secure voice capabilities. In an effort to provide solutions to these issues, the Secure Voice Program has formed a Secure Voice Products Community of Interest Group (SVP-COI) to address the technical and other factors associated therewith.

Anti-Virus Program

The Department's Anti-Virus program has intercepted and destroyed over 3,610,563 virus attacks in the calendar year 2006 to date. More than 35,318,497 pieces of spam have been stopped in addition. 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 unknowingly introduction of malicious codes, nearly 20,872 Anti Virus software CDs have been provided to the 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 Department of State IT infrastructure.

Communication Security (COMSEC) Modernization

The Department is continuing its effort to modernize its national security level encryption systems by using the National Security Agency (NSA) certified Inline Network Encryption (INE) devices, (including, KG-235s, KG-75s, and KG-175s). These new devices replace our aging serial based encryption systems with internet protocol based systems that will provide new higher capacity, robust network designs that leverage traditional Government owned, leased circuits, and the Internet infrastructure. In addition to supporting the Department's SMART and Internet Virtual Private Network programs, the INEs will provide the Department a gateway into in the Department of Defense (DOD) sponsored Global Information Grid providing state of the art real time interagency secure communications of classified information. The INE devices have been provisioned to every Diplomatic Mission certified to process classified information. Next generation INE devices are currently undergoing testing as part of the ClassNet redesign to further enhance the Department's domestic network and integrate it fully into the Intelligence Community resources to ensure rapid reliable exchange of information.

The Department has implemented the NSA mandated Electronic Key Management System. The Department's primary communications hub, Beltsville Management Center, has been completely converted from paper based to electronic COMSEC keying material. In addition, electronic keying material has been deployed to all foreign missions in the European region and is being successfully utilized to encrypt their command and control circuitry. The migration over the next year to full electronic keying material distribution over the existing Department of State (DOS) network infrastructure will provide the capability to distribute keying material in near real time without the security risks and time associated with using the Diplomatic courier system.

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 Diplomatic Security and Information Resource Management Bureaus, have issued over 28,095 intelligent Smartcard IDs that are being used for both physical access and logical PKI functions on the Department's SBU systems. PKI hardware and software has been installed on over 14,000 domestic workstations, and over 14,000 workstations overseas. Projected completion of deployment is planned by the end of FY 2007. The FPKIPA has cross-certified the Department's X.500 directory-based PKI and allowed it to connect to the Federal Bridge Certificate Authority at the high assurance level. This gives the Department's current 28,000+ (43,000 at full deployment) PKI users the ability to share digitally signed and/or encrypted SBU information rapidly in a secure manner, with 10 Government

DEPARTMENT OF STATE (DOS) - *continued*

agencies, the State of Illinois, and several non-government entities and certificate providers, through the use of PKI digital certificates. The Department also uses PKI to secure its websites, mobile code updates, patches to applications, and to access a growing number of applications. Currently (in addition to its internal uses), 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 103 locations around the country. BCIS estimates PKI services provided by the Department have saved taxpayers conservatively over $700,000 annually. The PKI program, in coordination with the Consular Affairs Bureau, has integrated PKI into the congressionally mandated electronic intelligent passport also known as the Machine Readable Travel Document program. This system digitally signs passport information using the Department's PKI to ensure the official issued information can be verified and has not been altered in real time at the Nation's ports of entry. In the FY 2006 timeframe, this system will support the production capacity of 7 to 10 million U.S. passports a year. The Department is implementing the Biometric Logical Access Development and Execution (BLADE) program, a biometric access application that is coupled with the Department's PKI. This program will improve system security by enhancing user authentication, and will enable a limited single sign-on capability for several PKI-enabled desktop applications, including network logon. This solution eliminates the need for users to remember passwords; instead using their fingerprint biometric to authenticate to their DOS Smart ID card for access to their personal PKI certificates. Biometric logon has begun domestically in several offices and is currently in use in 16 overseas posts. BLADE will be an ongoing component of the overseas deployment efforts.

Secure Video and Data Collaboration

The Secure Video and Data Collaboration (SVDC) program provides secret-high videoconferencing services to the Department of State. The success of this growing program continues to prove itself through the increasing customer-base, usage levels, and measurable cost savings. Additionally, the considerable reduction of risk to personnel, incurred by limiting the need to travel, is a particularly strong achievement of this program. The SVDC Program Office is staffed 5x24, providing program management and customer support for conference scheduling, configuration, interagency coordination and technical assistance. The SVDC program now supports diverse interagency videoconferencing capabilities with DOD through networking partnerships with Defense Information Systems Agency, U. S. European Command, U.S. Southern Command, and U.S. Pacific Command, as well as with other DOD area commands. Most recently we have established technologies in our program that facilitate point-to-point conferencing abilities allowing customers in both agencies to direct dial and expedite videoconference establishment. Currently, SVDC capabilities have been extended to 90% of our European and African embassies and consulates. Implementation domestically, in South and Central America, and Asia is rapidly increasing on a weekly basis. The SVDC Program Office continues to explore opportunities to expand and to improve the technologies and capabilities of this program.

Domestic Radio Program

The Department of State's domestic radio program supports twenty-four Bureau of Diplomatic Security Service field offices. These offices are engaged in law-enforcement and protection activities and are mandated by the Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399). The DOS has recently completed an upgrade all of domestic Land Mobile Radio systems to comply with the new National Telecommunications and Information Administration narrow-banding requirements. The DOS's Radio Program office is currently developing a project plan for the migration of all domestic Land Mobile Radio systems from Data Encryption Standard (DES) to Advance Encryption Standard (AES) before the National Institute of Standards and Technology (NIST) DES de-certification date in May 2007.

DEPARTMENT OF STATE (DOS) - *continued*

Overseas Radio Programs

In support of the mandates in the *Diplomatic Security and Antiterrorism Act of* 1986 (P.L. 99-399) and National Security Decision Directive-38, the DOS owns and operates Land Mobile Radio (LMR) and High Frequency radio systems at two hundred and sixty overseas United Stats diplomatic missions. These systems are designed to support citizen services, security, and emergency activities of the individual diplomatic missions. The DOS's Radio Program office is currently developing a project plan for the migration of all overseas LMR systems from DES to AES before the NIST DES de-certification date in May 2007.

Global IT Modernization (GITM) 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 (LANs) 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 to keep pace with new business requirements, not just replacement of existing 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.

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 United States of America as a member of the World stage. The essential functions of the Treasury Department requiring national security and emergency preparedness (NS/EP) and Telecommunications Service Priority program service are summarized as follows:

- Promote prosperous U.S. and World economics;
- Promote a stable U.S. and World economy;
- Manage the U.S. Government's finances effectively;
- Maintain, manage and preserve the economic and financial management institutions of the United States, including all monetary, credit, and financial systems;
- Serve as one of the principal economic advisors to the President;
- Perform international economic and monetary control as it pertains to the well-being of the Nation;
- Manufacture currency, coins, and stamps; and
- 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 (OCIO). The OCIO provides oversight and management of NS/EP support activities and the National Communications System (NCS) liaison. The OCIO 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 OCIO is also a member of the Federal Chief Information Officers 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 OCIO 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 include:

Treasury Communications System (TCS)

The Treasury Communications System (TCS), the Treasury Department's nation-wide business communications networking infrastructure, continues to provide critical telecommunications services to Treasury Department Headquarters and its associated Bureaus. TCS is one of the largest secure, encrypted networks within the Federal Government today.

Security Operations Center (TCS-SOC)

For fiscal year (FY) 2006, the TCS Security Operation Center (SOC) staff continues to pursue cyber security initiatives with a defense in depth focus. Following FY 2005's deployment of network intrusion detection systems into critical Wide Area Network chokepoints, significant sensor tuning and expanded network segment monitoring coverage has been established using the existing array of network sensors. Further efficiency tuning of the TCS Security Information Management (SIM) ensures appropriate security events are escalated and triaged effectively. Due to these developed efficiencies and economies of scale, the TCS Network Sensor count was reduced

DEPARTMENT OF THE TREASURY (TREAS) - *continued*

from 26 to 17, allowing other sensors to be staged for failure support or redeployment at other unmonitored network points. TCS Security also is currently monitoring 20 critical systems directly with Host based Intrusion Detection.

To further ensure incident events are properly handled and to ensure appropriate situational awareness, a TCS vulnerability Management System (VMS) was designed and deployed. The VMS, built within an enterprise framework, allows TCS security staff to review and assign responsibility from the results of Nessus vulnerability scans, and allows approving officials to accept business case and false positive vulnerabilities as part of the tracking system. The resultant list of bonafide vulnerabilities is then leveraged with the deployed SIM system to correlate active network vulnerabilities with detected security incidents to help assess the incident impact and facilitate further escalation.

TCS continues to define and refine it existing procedures, policies, and infrastructure in the security monitoring and incident response field, and TCS Security staff are providing full network security monitoring and reporting support to the Office of the Controller of the Currency and the Bureau of Public Debt. Additional agencies include the Departmental Offices, Community Development Financial Institution, and Treasury HRConnect.

From the government level, TCS Security staff has forged an operational bond with the Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT) team. This alliance yields numerous security operations benefits to TCS, as well as facilitated the deployment of DHS's Interagency EINSTEIN program on behalf of the Department of Treasury. EINSTEIN is a high level network traffic flow analysis tool used by TCS Security and US-CERT to identify anomalous and potentially malicious traffic flow across the Internet boundary.

Certification and Accreditation

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 assurances 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 2006, 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 created C&A packages for other Bureaus and agencies including: the Treasury Human Resources, the Treasury Intranet, the Treasury Enterprise VPN, and the ProSight system used to support Treasury-wide capital planning and investment control, the Secure Extranet Gateway, the Business DNA project, the Federal Credit Reporting Service (FCRS), the Metis System, and the Treasury Enterprise Directory Services (TEDS) X.500 system.

Currently, TCS' Security Assurance Program is in the process of certifying and accrediting the Treasury Executive Office of Asset Forfeiture project, the Trusted Agent Federal Information Security Management Act of 2002 (FISMA) reporting system, the V-One VPN solution, the Secure Extranet Gateway, and the Treasury Self Administration Service. Since C&A packages expire after three years, work will also soon begin on the re-certification of the TCS infrastructure in order to maintain continuous accreditation status. There are also three-year re-certifications in progress on the FCRS, and the TEDS. Additionally there is one re-certification in progress on the ProSight pilot project due to major modifications.

The Certification team has currently completed working on a Treasury-wide Security Requirements Compliance Matrix (SRCM) as a standard that was developed from the latest National Institute for Standards and Technology (NIST) guidelines, including the 800-53 Recommended Security Controls for Federal Information Systems, and all of the Treasury Policies including the TD P 85-01. Since the NIST 800-53 recommends different levels of controls based on security categorization (System Low, System Moderate, and System High) from the Federal Information Processing Standards Publication 199 process, three different SRCM documents are being developed.

The Certification team has also completed yearly updates in compliance with the FISMA requirements for the TCS including the TCS System Security Plan, Personnel and Physical Security Plan, TCS Risk Assessment, and TCS Self assessment in accordance with NIST 800-26.

The Certification team is also in the process of performing an annual audit of the Treasury Public Key Infrastructure (PKI) system. The system is being audited for compliance with RFC 2559 standard for Certificate Policy, Certification Practices Statement, and the actual implementation of these policies.

Digital Telecommunications Switching System (DTS2)

IT Security

To carry out their wide ranging responsibilities, employees and managers of the U.S. Department of the Treasury have access to a complex telecommunications infrastructure that provides local capabilities to Treasury sites in the Washington, D.C. area, including sites in suburban Maryland and Northern Virginia, and physical interfaces to other telecommunications programs and services. To have this access to Treasury's complex telecommunication, the Digital Telecommunications Switching System 2 (DTS2) network provides voice, data, and video services via analog, Integrated Services Digital Network (ISDN) Basic Rate Interface and ISDN Primary Rate Interface service to the DTS2 user community. The various business and law enforcement functions within Treasury depend on the confidentiality, integrity, and availability of these systems and their data.

Treasury relies on its information and communications infrastructure, including DTS2, to accomplish its mission in a secure, cost effective manner. The information transmitted and generated by DTS2, and the DTS2-specific information in Verizon's operations, administration, maintenance, and provisioning support systems, are considered Sensitive But Unclassified. The Department developed the DTS2 Security Program to meet the security requirements and technical guidance set forth in the following:

- Public Laws;
- Office of Management and Budget guidance;
- Government Accountability Office;
- National Institute of Standards and Technology Special Publications;
- Department of the Treasury Directives;
- DTS2-specific policies and procedures set forth in the DTS2 System Security; and
- Authorization Agreement and its appendices.

The DTS2 network met Treasury's requirements for the Authority to Operate in December 2003. DTS2's System Security Plan defines actions for which Treasury is responsible and provides the overarching DTS2 security framework and objectives. The DTS2 System Security Authorization Agreement and its appendices describe security measures that are in place, or that the DTS2 Program Management Office and Verizon plan to implement, to ensure the confidentiality, integrity, and availability of DTS2 services and to fulfill contract requirements (including Government requirements such as FISMA, OMB A-130, and guidance from the 800 series of NIST Special Publications). Verizon's documents complement the DTS2 Shared Service Provider (SSP) by describing how Verizon implements Treasury's DTS2 security framework and achieve the Department's security objectives for the DTS2 network.

[1] U.S. Department of Treasury, Missions, Goals and Results. Available online: http://www.treasury.gov/gpra.

DEPARTMENT OF THE TREASURY (TREAS) - *continued*

Treasury Emergency Management Center Capability

As part of Treasury's Continuity of Operations Plan (COOP), Treasury Headquarters established Emergency Management Centers (EMC) for responding and reacting to crises, disasters and emergencies. The local EMC is a "hot site", and has equipment running and ready for operation. A second EMC is located within the Department of the Treasury's primary COOP location; this is a cold site. These sites are fully integrated with the Treasury's communications system network operations facilities for ensuring continuous operations of the Treasury Department in a crisis or emergency. Currently a search is underway for a newer, larger, more capable local EMC. This center will be improved and modernized around changes in the Treasury Department's operating principles and practices and the associated information technology systems for enhancing their business management information systems. Both Treasury EMC's (local and COOP) are capable of secure voice, facsimile, and SIPRNet communications as well as unclassified voice, facsimile, and local area network operations.

The continuity of operations requirements for the Treasury Communications System have been fully coordinated and synchronized with the plans and programs operating under the Treasury Department's Office of Emergency Preparedness. The issuance of Government Emergency Telecommunications Services (GETS) cards continued to increase in FY 2006. All Successors to the Secretary of the Treasury now have Wireless Priority Service (WPS) on their cellular telephones. The acquisition of a new expanded the Treasury Emergency Management/Operations Center within the greater Washington, D.C./ metropolitan area is expected to further strengthen Treasury's emergency preparedness posture. Key operational functions and capabilities that will be expanded in fiscal years 2006/2007 are:

- A larger, modernized Department of Treasury local EMC with associated system monitoring and management tools;

- Additional contingency office space for senior Treasury Department leadership and their core emergency staff equipped with secure and unclassified equipment;

- Additional contingency communications capability. Treasury will install, test, and implement a High Frequency Radio Network in support of Federal Preparedness Circular 65 requirement for emergency back up communications. HF radios will be procured and installed at Treasury Headquarters, Treasury headquarter COOP site, all Bureau COOP sites and selected bureau headquarter locations. This network will facilitate communications between Treasury headquarters and Bureau COOP sites at the secure level, as well as between Treasury headquarters COOP site and Federal Emergency Management Agency at the Top Secret level;

- Additional GETS Cards/Personal Identification Numbers will be obtained and pre-positioned at all Department of the Treasury Alternate Operating Facilities and EMC's so that cards can be transferred to Treasury staff in order to respond to immediate crisis;

- WPS phone acquisition for the senior staff of Department of the Treasury Bureaus;

- Secure and non-secure Video Teleconferencing capability for the Primary and Alternate Treasury Headquarter COOP site;

- Treasury is in the process of acquiring fixed-station Satellite communications (Unclassified Voice, Secure Voice, and Secure Facsimile) for its primary COOP site. Treasury plans to equip its newer, expanded EMC with the same capability as soon as it is occupied and operational; and

- Full installation, testing, and use of E-Team (an unclassified event tracking system) in Treasury's EMC's and Bureau locations. Treasury Headquarters and Bureau Emergency personnel have been trained utilizing

E-Team during the exercise, Forward Challenge-2006.

Support for the Federal PKI

The Department of Treasury continues to provide first-class technical, operational and leadership support in the development and use of an interoperable government-wide PKI to permit electronic transactions across Treasury and over the Internet in a secure and trusted environment.

Treasury's enterprise PKI system is capable of issuing digital certificates to over 150,000 Treasury contractors and employees, and to date has had active participation by 11 of its 12 Bureaus. For this reason, Treasury's PKI will be a critical component in the Department's Personal Identity Verification (PIV) system, as required by the Homeland Security Presidential Directive-12). Indeed, in FY 2006 significant progress has been made to modify the current PKI architecture to prepare for necessary and imminent changes in support of this solution.

During FY 2006, the Federal Identity Credentialing Committee has formally inducted Treasury into the Federal PKI SSP program. The induction, which marks several years of collaboration and effort between Treasury and Federal organizations, formally allows the Department to offer its digital credential services to partnering agencies to reduce its ongoing operations, policy and management costs by sharing its PKI resources. This has proven to be highly successful—the National Aeronautics and Space Administration, as Treasury's first SSP customer, has publicly praised Treasury's PKI personnel and resources. Treasury is actively seeking future business engagements with other agencies, and will continue its efforts to do so over the next fiscal year.

Treasury continues its business relationship with the Federal Bridge Certification Authority to conduct trusted business with member agencies through a common PKI architecture. During FY 2006, Treasury has leveraged this trust model to conduct interagency business with the Department of Homeland Security. Efforts to further utilize this trust architecture are expected to increase over the next fiscal year.

Treasury has expanded its current resources to meet forecasted demand and address requirements such as those brought about by the Department's involvement in the E-Authentication Federation and PIV, as described above. For example, Treasury organizations in charge of PKI governance and maintenance have established a staging environment for its mission-critical Certification Authority hosts, to enable the Department to more effectively prepare for upcoming infrastructure changes.

Treasury continues its efforts with the General Services Administration as part of the E-Authentication Federation program, and is working actively with its trading partners in the financial community to ensure business is conducted seamlessly and securely.

Public Safety/Law Enforcement Wireless Activities

The Department of the Treasury's Wireless Programs Office (WPO) serves as a centralized, enterprise approach to managing wireless technologies throughout the Department. The WPO has been successful in increasing its presence throughout the Department and across other Federal entities. The WPO continues to efficiently maintain Treasury's spectral assets, participate in the Integrated Wireless Network (IWN) Program, and assist Treasury Bureaus in upgrading their land mobile radio (LMR) equipment in order to meet the narrowband and AES related mandates.

Treasury continues to participate in the Interdepartment Radio Advisory Committee (IRAC) and other Federal committees (including the Federal Partnership for Interoperable Communications. Having a presence at the IRAC ensures that Treasury's spectral assets are managed appropriately to meet the department's spectrum needs for wireless public safety and law enforcement communications. In addition, to further increase Treasury's spectrum efficiency, Treasury is actively continuing efforts for timely compliance with the National Telecommunications and Information Administration narrowband mandate as well as participating in activities related

DEPARTMENT OF THE TREASURY (TREAS) - *continued*

to the Presidential Determination on spectrum management.

Treasury has also increased participation within the IWN Program, which is a partnership with the Department of Justice, Department of Homeland Security, and Treasury, to implement a joint law enforcement voice and data network that will meet the mission-critical requirements of the Federal departments involved. This joint effort will provide cost and operational efficiencies across Treasury as well as significantly enhance interoperable communications among law enforcement agencies. Treasury will continue to participate in this joint effort to ensure that Treasury remains abreast the rapidly evolving wireless technologies and standards and to address public safety and law enforcement activities in collaboration with other Federal law enforcement agencies.

To participate in the IWN and to meet federal mandates, the WPO has assisted several Bureaus (including, Bureau of Engraving and Printing, U.S. Mint) in obtaining new state-of-the-art LMR equipment to support their security and law enforcement missions around their facilities. Additionally, the upgraded equipment enables the Bureaus to connect into the IWN in the future for emergency response.

Once completed, these enhancements and modernization initiatives 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, 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, National Security Agency, provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications; and

- Execute the functions listed in Section 3(1) of E.O. 12472.

Telecommunications Staff Organization

DOD includes the Office of the Secretary of Defense (OASD), 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 Office of the Secretary of Defense are the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense [ASD (HD)] and the ASD for NII.

Current/Ongoing NS/EP Telecommunications Activities

Critical Infrastructure Protection

The Deputy Secretary of Defense issued DOD Directive 3020.40 (Defense Critical Infrastructure Program), dated August 19, 2005., DODD 3020.40 assigns responsibilities to Department of Defense components for the identification, prioritization and where appropriate, protection of DOD and non-DOD networked assets essential to project, support, and sustain military operations worldwide. The ASD (HD) serves as the principal senior advisor to the Secretary of Defense on all matters related to the execution of Defense Industrial Base (DIB) Sector Specific Agency (SSA) responsibilities assigned under Homeland Security Presidential Directive-7 (Critical Infrastructure Identification, Prioritization, and Protection). The ASD (HD) represents the DOD on all Critical Infrastructure Protection (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 this capacity, the ASD (HD) has established a Defense Industrial Base Government Coordinating Committee and encouraged the establishment of a Private Sector Coordinating Committee to provide effective coordination of DIB sector policy, security strategies and coordination across government. These bodies bring together diverse Federal, state and local, as well as private sector, interest in order to identify and develop collaborative strategies that advance critical infrastructure protection. The Department, under HSPD 7, has established Critical Infrastructure Protection-Mission Assurance Assessment teams, composed of the Defense Contract Management Agency Industrial Analysis Center (DCMA-IAC) and National Guard Bureau to conduct and facilitate vulnerability assessments on the DIB. These assessments, whether conducted or facilitated are done in accordance with established DCIP standards and benchmarks. In addition, awareness teams, composed of DCMA-IAC, National Guard Bureau (NGB), DHS, Federal Bureau of Investigation, local law enforcement, and first responders have been established to bring greater awareness to CIP. The Department is drafting its DIB Sector Specific Plan, a collaborative plan with industry, for execution of DIB SSA responsibilities, as required by the National Infrastructure Protection Plan, for delivery to the White House by December 31, 2006.

Defense Continuity and Crisis Management

The Defense Continuity and Crisis Management office, within the ASD

DEPARTMENT OF DEFENSE (DOD) - *continued*

for HD, contributed to the following NS/EP activities:

- National Response Plan (NRP): The Department of Defense supported the planning effort and proactively participated in the development of the current version of the Emergency Support Function-2 Operations Plan as an integral supplement of the NRP.

- Katrina After Action. DOD acted upon the recommendations of the House Report on Hurricane Katrina, The White House Federal Response To Hurricane Katrina, and the Government Accountability Office reports. The Department developed milestones and expedited the development of detailed plans and exercises to fully account for the unique capabilities and support that the military is likely to provide to civil authorities in response to the full range of domestic disasters, including catastrophes. Specifically, DOD has published the Defense Support to Civil Authorities (DSCA) Standing Execute Order, which authorizes the commanders of U.S. Northern Command (USNORTHCOM), U.S. Pacific Command, and U.S. Southern Command to prepare DOD assets in order to be ready to deploy in support of civil authorities in response to natural disasters. DOD DSCA operations fully exploit NCS NS/EP programs such as the Governments Emergency Telecommunications Service, the Wireless Priority System, and the Telecommunications Service Priority Program.

- Louisiana Gulf Coast Communications Planning. OASD (HD) and USNORTHCOM supported a planning effort chartered by DHS, under the leadership, of the, Principal Federal Officer Gulf Coast Region and Deputy for Gulf Coast Development. The Federal Government, working with regional, State, and local partners developed a comprehensive, integrated Federal, State, and local communications plan for the Louisiana High Risk Gulf Coast Community. The Plan integrated a Federal, State and local approach to ensure effective communications, coordination and delivery prior to a tropical storm or hurricane.

Net-Centric Operating Environment

In 2006, ASD NII with the Joint Staff J6 continued Net Centric Operating Environment planning to deliver needed Global Information Grid (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. Key efforts include development of the DOD Information Sharing Strategy, initiatives with other Departments and Agencies to interconnect networks for classified and unclassified information sharing, and development of cyber security policies.

Joint Task Force-Global Network Operations

Joint Task Force-Global Network Operations leads and directs continuous Enterprise Services Management/Network Management, Information Assurance/Computer and Network Defense, throughout the GIG. JTF-GNO provides Situational Awareness (SA) of the GIG through the Network Common Operational Picture. The JTF-GNO provides command and control through a tiered hierarchy of NetOps Centers working together to assure Global Decision Superiority by maintaining near real-time SA, end-to-end management, and dynamic DOD network defense.

National Command and Coordination Capability

DOD supported the Department of Homeland Security by leading a working group to define the National Command and Coordination Capability (NCCC).

Initial NCCC constructs were developed through the Nuclear Command and Control System Committee of Principals activities under the authority of the National Security Presidential Directive (NSPD)-28, *Nuclear Weapons Command, Control, Safety, and Security*. The National Command Capability Transitional Working

Group led by DOD performed preliminary vulnerability analyses and developed initial strategy documents. The NCCC is the enabling command, control, and coordination capability among the Federal, state, tribal, international, territorial, insular area, local governmental levels, non-government organizations, and the private sector. It is the means to command, control, and coordinate land-aerospace-sea operations among the above organizations to achieve national objectives through all emergencies and contingency situations.

Joint CONUS Communications Support Environment

As a key component to DOD's homeland security mission set and a key link to the State and local governments, the NGB in cooperation with USNORTHCOM, is developing Joint CONUS Communications Support Environment (JCCSE) to provide valuable communications support to Federal, State, and territorial, local tribal and private-sector response efforts JCCSE provides a distributed capability that enables collaboration, information sharing, and interoperability that promotes effective interagency operations. The intent of JCCSE is to "optimize DOD preparedness to support Homeland Defense and DSCA mission requirements. The NGB has coordinated with DHS to leverage DHS' primary information sharing capability, the Homeland Security Information Network, to collaborate and facilitate operational effectiveness and share information with DHS and local authorities.

Information Sharing for Civil-Military Operations

The ASD(NII)/DOD CIO and U.S. Joint Forces Command, in consultation with other Combatant Commands, the Services, Defense Agencies and the Joint Staff, are developing an internet-accessible virtual environment for the exchange of unclassified information across the civil-military boundary associated with Stability, Security, Transition, and Reconstruction Operations or international Humanitarian Assistance and Disaster Relief operations. U.S.-Joint Forces Command has created an initial instantiation of this capability as HARMONIEWeb.org. HARMONIE will provide web-based services and collaborative tools through a dynamic portal. This environment will enable the Department to harmonize better its operations with other U.S. Departments and Agencies, foreign governments and security forces, International Organizations, Non-Governmental Organizations, and members of the Private Sector.

The Committee on National Security systems

DOD is the Executive Agent for the Committee on National Security Systems (CNSS), which is the policy making body for all issues concerning the security of national security systems for the Federal Government. It promotes the security of these systems by providing a forum for policy discussions, setting national policy, and promulgating direction, operational procedure, and guidance through the CNSS issuance system.

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.

Scope of Services

The Department centralizes its NS/EP responsibilities in the Justice Management Division for all department components except the Federal Bureau of Investigation (FBI). The Department's Components include the Bureau of Alcohol, Tobacco, Firearms and Explosives, Bureau of Prisons, Drug Enforcement Administration, Executive United States Attorneys, United States Marshals Service (USMS). The Department is currently transitioning to the Justice Unified Telecommunications Network (JUTNet) from several legacy networks including the Justice Consolidated Network, the Washington Metropolitan Area Network, and the Treasury Network. Transition to JUTNet is scheduled for completion by the end of the calendar year 2006. The FBI maintains separate secure network facilities.

Telecommunications Staff Organization

The Deputy Chief Information Officer, Operations Services Staff (OSS) operates and manages DOJ's current consolidated data transport network, law enforcement message processing system and the 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 such as the Defense Message System, Justice Automated Message System and the Joint Worldwide Intelligence Communications System. The FBI continues to administer their communication security program. The Drug Enforcement Administration and USMS utilize JUTNet but provide their own administrative services around the network.

Current/Ongoing NS/EP Telecommunications Activities

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

- The Deputy Chief Information Officer, Policy and Planning Staff provides representation for DOJ on the National Communications System's (NCS) Committee of Principals (COP);
- OSS provides representation for DOJ on the Council of Representatives;
- An OSS representative serves on the Telecommunications Service Priority (TSP) Oversight Committee;
- DOJ continues its active participation in the NCS activities of the 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 NS/EP support in their normal duties (such as remote security alarm sensing; 9-1-1 and enhanced 9-1-1 services in several Midwestern states; and for environmental and emergency response services for cleanup of waste at clandestine drug laboratories); and
- Additionally, the department is an active participant in the Government Emergency Telecommunications Service Program, the Wireless Priority Service Program, TSP, 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. The Department of the Interior (DOI) and the United States Department of Agriculture co-manage the National Interagency Fire Center (NIFC) in Boise, Idaho. It is the Nation's primary emergency support resource for all-risk hazards management. NIFC provides emergency land mobile radio (LMR), satellite, and weather tracking systems from multiple radio caches strategically located throughout the United States to support wildland fire and national security and emergency preparedness (NS/EP) activities under Emergency Support Function-2 (ESF-2). Operations are conducted in close cooperation with State, local, other federal, and tribal government emergency support activities.

Current/Ongoing NS/EP Telecommunications Activities

DOI mission critical long distance voice and data communications is primarily provided by Verizon via the General Services Administration's (GSA) FTS2001 contract. We are in process of consolidating of our 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.

The transition of DOI's wideband LMR systems to the National Telecommunications and Information Administration mandated narrowband operation is a continuing high priority. We are recompeting our second multi-vendor, multi-year contract to supply Project 25 (P25) standard narrowband radios and supporting infrastructure to all Federal agencies, providing lower-cost standardized interoperable P25 radios. We participate in the e-Gov SAFECOM program which promotes public safety radio system interoperability.

DOI Key Officials, emergency coordinators, and telecommunications managers have Government Emergency Telecommunications Service Cards for long distance emergency telephone communications and cellular phones with Wireless Priority Service. Secure Terminal Equipment secure telephones are used to support DOI national security programs and high frequency backup radio links are used to augment DOI emergency relocation site communications. Critical circuits on the DOI network have received Telecommunications Service Priority designation.

DOI Significant Accomplishments

We are currently preparing to sign separate memorandum of understanding with the states of Montana and Wyoming for cooperative proportional partnerships in their statewide P25 compliant LMR systems. Additionally, we are in process of reviewing potential partnerships in Oregon, Alaska, Idaho and Wisconsin, and are updating our partnership agreement with South Dakota. These agreements significantly improve interoperability between federal, state, local and tribal public safety radio users.

DOI is in the final phase of establishing a joint DOI, Department of Homeland Security and National Institute of Standards and Technology funded Telecommunications Service Center (TSC). The TSC will provide a laboratory component level and holistic plan for determining manufacturer's radio equipment compliances with P25 standards and ability to work in support of incident command scenarios and systems. The land mobile radio industry is very supportive of this effort with multiple vendors providing baseline user, infrastructure, dispatch and encryption equipment for testing.

The Department's consolidated Enterprise Services Network (ESN) deployment is nearing completion. This included completion of agency intranet and Internet access points of presence, multi protocol label switching deployment, and transferring all network devices to managed services. DOI received and reviewed the National Communications System provided FTS2001 Traffic Analysis as part of the ongoing effort to provide critical infrastructure analyses for the Committee of Principals. The findings of this excellent analysis are being considered for the DOI ESN project.

UNITED STATES 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 leadership on food, agriculture, natural resources, and related issues based on sound public policy, the best available science, and efficient management.

NS/EP Telecommunications Activities

As a result of Hurricane Katrina, the use of specific communications equipment and services increased dramatically within the Department in 2005. USDA fielded Wireless Priority Service (WPS) handsets that provide priority cellular network access to individuals in NS/EP leadership positions. During the aftermath of Hurricane Katrina, the National Finance Center employees used these WPS phones to make outgoing calls in support of the USDA mission.

WPS and Government Emergency Telecommunications Service (GETS) requests were filled to support USDA Continuity of Operations (COOP). During post hurricane Katrina and Rita recovery efforts, GETS cards proved particularly effective for the USDA Emergency Operations Center as Watch officers used these services to contact personnel assigned to mission critical facilities.

To better prepare USDA to respond to future disasters, departmental policy (Departmental Notice 3300-20) was published to ensure that the USDA agencies are engaged in the National Communications System's (NCS) Telecommunications Service Priority (TSP) program. The USDA Office of the Chief Information Officer's (OCIO) Telecommunications Services and Operations continues to work closely with COOP Planning Staff to meet Departmental information technology requirements. During fiscal year (FY) 2005, emphasis was placed on the identification of TSP requirements and OCIO is now in the process of implementing TSP circuits in these critical locations.

Activities planned for FY 2006 include:

- Identify new communications requirements between key NS/EP designated sites;
- Designate key field personnel to serve as TSP representatives for each USDA agency; and,
- Provide TSP training to the representatives.

NS/EP Partnership Activities

The USDA is responsible for performing multiple Emergency Support Functions (ESF) under the National Response Plan (NRP). Within the ESF structure the USDA is able to provide support to the states and other Federal agencies during declared disasters and emergencies under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act), as well as non-Stafford Act incidents. In carrying out NRP Emergency Support Functions, USDA personnel follow telecommunications guidelines established for major wild land fire suppression that are published in a National Mobilization Guide by the National Interagency Coordination Center (NICC). The NICC resides within the National Interagency Fire Center (NIFC) in Boise, Idaho. The Guide provides administrative procedures for mobilization of radio equipment, the assignment of communications personnel, the allocation of communications resources, levels of authority for shipping equipment to a site, the assignment of communications frequency managers to complex incidents, and equipment transfer and replacement during an incident. Trained personnel include a National Communications Duty Officer (CDO), Geographic Area Frequency Managers, Communication Coordinators, and Incident Communication Unit Leaders, who coordinate with NICC, the Geographic Area, and the National Incident Radio Suport Cache (NIRSC) CDO on all telecommunication issues.

In the aftermath of Hurricanes Katrina and Rita, USDA delivered radios as part of the ongoing role in the NRP to 500 Federal Air Marshals at the New Orleans Airport, who were without any

UNITED STATES DEPARTMENT OF AGRICULTURE (USDA) - *continued*

communications capability when they arrived. The New Orleans Fire Department was given a USDA repeater to maintain communications with fire fighting helicopters, and USDA technicians established a network so that Environmental Protection Agency personnel could be in contact as they perform fieldwork in southern Louisiana.

As one of the oldest agencies in the Federal Government the USDA has evolved in conjunction with its role in the NRP. The USDA Forest Service participates in a formal National Multi-Agency Coordinating Group and has a major role in the FY 2005 preparedness strategy that addresses joint operations for fire fighting and law enforcement.

The NIFC maintains a NIRSC consisting of preconfigured mobile communications systems. NIRSC is a National Resource composed of multi-channel radio systems available for complex incident communications. Each system is comprised of multiple kits with items such as command radios, logistics radios, and repeaters ready for shipment and to key Geographic Areas where they are pre-positioned for emergency use.

When a Presidential Disaster Declaration was issued on August 29, 2005, the NRP was activated. As requested by the Federal Emergency Management Agency, the Forest Service assisted in providing logistical support such as managing base camps for field hospitals, receiving and distributing equipment and relief supplies, managing the care, feeding and logistical support of thousands of relief workers and volunteers, for the elderly and infirm, and for other persons unable to evacuate using whatever communications tools were available.

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

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; and,
- 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.

Agencies operating within the Department of Commerce include the Bureau of Industry and Security, Economic and Statistics Administration, Bureau of Census, Bureau of Economic Analysis, Economic Development Administration, International Trade Administration, Minority Business Development Agency, National Oceanic and Atmospheric Administration, National Telecommunications and Information Administration, Patent and Trademark Office, Technology Administration, National Institute of Standards and Technology, and National Technical Information Service.

The Department continues to support the efforts of various cross governmental organizations including the National Communications System (NCS) Committee of Principals and the Committee of Representatives, the National Cyber Response Coordination Group, the Critical Infrastructure Protection Policy Coordination Committee, and various Contingency of Operations Planning committees and forums.

Telecommunciations Staff Organization

The DOC manages its telecommunications through the Office of the Chief Information Officer's throughout the Operating Unit agencies, with varying telecommunications technologies services including Voice over Internet Protocol (VoIP), Private Branch Exchange and other agency managed telecommunications services.

Current/Ongoing NS/EP Telecommunications Activities

The following current/ongoing DOC activities support national security and emergency preparedness objectives:

- The DOC is actively involved in Homeland Security initiatives and efforts to enhance preparedness with the necessary information technology equipment, software and hardware upgrades. Its headquarters in Washington, D.C. has implemented a new Emergency Broadcast System (EBS) that can send pre-recorded or ad hoc messages to every VoIP 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.

DEPARTMENT OF COMMERCE (DOC) - *continued*

- To enhance our Continuity of Operation Planning, the Employee Notification System was successfully piloted within the HCHB during the first half of calendar year 2005, is fully operational today, and was tested during the recent Forward Challenge TTX. The system automatically notifies all identified employees using any of several available means (such as, telephone, cell phone, pager, email) within a reasonable period of time. Notifications are based on grouping structures and other criteria. Employees are able to report their status and availability for duty, as well as enter and update their own contact information.

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 promote the support and use of NCS services and programs, especially in light of recent hurricane disasters 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 United States 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 (NS/EP) telecommunications systems.

Current/Ongoing NS/EP Telecommunications Activities

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; and
- Communications on Public Health issues with Non-Governmental Organizations.

Current emphasis is on providing a consolidated approach for the delivery of integrated Information Technology and communications systems to support the Department's mission for the protection of the health and welfare of the American public. An area of focus for the Department continues to be provisioning of information technology (IT) infrastructure that allows bidirectional communications regardless of atmospheric or terrain restrictions. In addition, emphasis has been placed on the interoperability of systems that can communicate with all of the Federal, State, local and tribal partners involved in the support of the Departments primary Emergency Support Function-8 response. With the further definition being provided by the National Communications System and other organizations, the Department is rapidly moving toward standardization of IT related resources for its continuity of operations and continuity of government functions and is working towards compliance with both the SAFECOM and Disaster Management initiatives. Additionally, HHS is developing a standardized approach across the Department for the administration and deployment of Wireless Priority Service, Government Emergency Telecommunications System cards and Telecommunications Service Priority in support of critical National Security, Public Health and Financial systems.

In an effort to increase the ability for global surveillance of health issues affecting the American public, the Department of Health and Human Services has established collaborative relationships with health organizations around the world to ensure rapid identification and treatment of health threats. 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.

Over the next year, HHS will take advantage of inventory studies in support of our General Services Administration Networx Transition Planning to re-evaluate the status of infrastructure to assure protection of critical telecommunications access facilities and redundant/diverse access availability for disaster recovery purposes.

DEPARTMENT OF TRANSPORTATION (DOT)

NS/EP Telecommunications Mission

The Department's mission as outlined in the Department of Transportation (DOT) Strategic Plan, asserts that the Department will "serve the United States by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people." Due to the tragic events on September 11, 2001, the entire Department has been engaged in the evaluation and implementation of enhancements to the safety and security of the Nation's transportation systems. The Department is developing new strategies and contingencies to deal with increased threats and vulnerabilities. The recognition of the vital role that telecommunications plays in providing for safety and security that the public has come to expect from the Nation's transportation systems has enabled the Department to further increase its ability to respond to and counter new threats as they arise.

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. Today, multinational manufacturers receive materials from international suppliers, transport 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 commodity 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 communications 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 the National Communications System's (NCS) Committee of Principals and Council of Representatives, the President's National Security Telecommunications and Advisory Committee, and actively supports NCS national security and emergency preparedness activities and programs. DOT provides a member of the chief information officer's staff who, as a representative, ensures that program information as provided by NCS is properly disseminated throughout the agency and the resulting benefits realized.

Government Emergency Telecommunications Service

The Department of Transportation continues to be involved with the Government Emergency Telecommunications System (GETS). The GETS calling cards are assigned to Regional Emergency Transportation Coordinators and Representatives to be used during emergency situations. This capability was successfully put to use during the Hurricane Katrina disaster.

DEPARTMENT OF TRANSPORTATION (DOT) - *continued*

DOT was able to keep in ready contact with volunteers sent to the region to offer support. The Department continues its sponsorship of Federal, State, local Government and the private sector in entering the program. The GETS card is vital to these groups to support continuity of operations and receive priority service.

Other Emergency Support

DOT participated in the Forward Challenge 2006 exercise sponsored by the Federal Emergency Management Agency (FEMA). In following the direction of FEMA, DOT submitted scenarios to be used in the event directly related to its operational mission. The information gleaned from the data gathered was distributed to all interested parties and resulted in an affirmative response and approach to the continuity of government in an emergency situation.

Disaster Area Evacuation Improvements

DOT is assessing the existing DOT-led Evacuation Liaison Team for potential improvements. In addition, DOT has modified the existing DOT Emergency Response Team to include a pre-identified Evacuations Event Team (including interagency partners) that link with the Evacuation Liaison Team, the Emergency Support Function-1 component to monitor and make recommendations as they relate to evacuations. This team is activated several days before landfall and make reports and recommendations to the DOT Incident Management Team regarding evacuation planning and execution. DOT has initiated discussions with many of its transportation industry association partners to develop methods through which even more transportation resources could be acquired faster, and applied more effectively. DOT continues to engage in discussions with key non-transportation partners who play key roles in the success of evacuations, such as the American Red Cross, whose role in identifying and activating shelters to which evacuees are taken is critical to rapid movement of those persons to safety. DOT has engaged in intensive planning for evacuation of southern Louisiana, possibly the nation's most vulnerable area, due to the devastation it experienced during the 2005 hurricane season. DOT is focusing on capabilities that will make it possible to support evacuations more effectively, such as assuring accurate tracking of and communication with evacuation vehicles. These were major problems during Hurricane Katrina due to the destruction of the wireless communications system in the disaster area. DOT is working with FEMA and other disaster response partners on improving the procedures through which evacuation actions can be authorized, such as "pre-scripting" the predictable assignments.

Finally, the DOT will be moving to a new headquarters in 2007. Planning for the Information Technology infrastructure has been ongoing and will take advantage of the NCS Route Diversity Program offerings. Employing the key concepts of redundancy, resiliency and diversity to control the communications network is key to the Department of Transportation.

DEPARTMENT OF ENERGY (DOE)

NS/EP Telecommunications Mission

DOE Headquarters Networks

The Department of Energy (DOE) migrated its wide area network (WAN), the DOE Corporate Network (DOEnet), from a hub and spoke asynchronous transfer mode design to an Internet Protocol (IP) multi protocol label switching-based any-to-any topology and replaced all of the network hardware resulting in a more stable and secure networking environment. All data transmitted across the WAN is now protected with IPSEC 256-bit AES encryption using Dynamic Multi-point Vertical Positioning Mast (VPM) configurations. All DOEnet circuits have Telecommunications Service Priority Restoration assignments. Completed the metropolitan Sonet Ring for the DOE Headquarters Network and further improved fault-tolerance by adding a redundant, physically diverse Internet path from Germantown to Philadelphia. DOE Headquarters successfully tested its network contingency and disaster recovery capabilities in June 2006 through tabletop and other exercises. Government Emergency Telecommunication Service (GETS) and Wireless Priority Service (WPS) cards were vital to the Operation of the Strategic Petroleum Reserve during Hurricane Katrina. For the most recent quarter, the number of GETS/WPS test calls increased by 35 percent.

Richland Operations Office (RL)

RL is implementing a digital trunked two-way radio system to improve utilization of licensed spectrum and interoperability for the Hanford Patrol, Fire and Emergency Preparedness. RL is also deploying an integrated, instantaneous, emergency alerting system that utilizes phones, radios, pagers, AM radio stations, reader boards, Tone Alert Radios, and pop-up messages on desktop computers to meet Federal mandates.

Chicago Operations Office (CH)

All CH Laboratories completed the very high frequency migration to narrow band technology.

Argonne National Laboratory (ANL)

ANL in coordination with the State of Illinois, has connected to a new statewide narrow band 800 megahertz (MHz) digital trunked system for interoperability between government and public safety agencies. Operations are to begin in December of 2006.

Lawrence Berkeley National Laboratory (LBNL)

Completed the installation of a ultra high frequency Digital Trunked Repeater Site to tie into the LBNL Trunked Radio System. This provides LBNL with radio coverage over most of the Bay Area using digital technology compatible with public safety and Department of Homeland Security and greatly enhances the two-way radio coverage throughout the laboratory.

Savannah River Operations Office (SR)

New radio systems were installed at the Tritium facilities with encryption capabilities providing communications through the facilities in the event of an emergency. New radios and Centracom console upgrades were installed for the U.S. Forest Service facilities providing continuity of operations capabilities.

The Kansas City Plant (KCP)

KCP entered into a frequency sharing agreement with the Division of Fire Safety of the Missouri Department of Public Safety in fiscal year 2006, which documents the methodology for coordinating mutual emergency aid activities among various agencies.

Oak Ridge Office (ORO)

ORO continues to move all reservation radio users over to the Wide Area Radio System currently with 3200 users. The site is broadcasting a 460 MHz mutual aid channel for communications between DOE security, emergency management, and local city, county, and state law enforcement and emergency services agencies enhancing interoperability.

National Energy Technology Laboratory (NETL)

The Morgantown, West Virginia, facility installed a SHAred RESources program High Frequency Radio system.

Rocky Mountain Oilfield Testing Center (RMOTC)

RMOTC installed a back-up phone system tied into the Midwest, Wyoming, NPR-3 phone system for emergency communications. All Federal Manager's have been issued GETS cards to support emergency response/preparedness.

DEPARTMENT OF VETERANS AFFAIRS (VA)

NS/EP Telecommunications Mission

Wide Area Networking

The Department of Veterans Affairs (VA) is optimizing its corporate wide area network (WAN) under the Telecommunications Modernization Project (TMP). In 2004 and 2005, the TMP WAN was extended beyond the existing core and distribution layer into a regional access architecture that provides standardized and consolidated network management and security. An alternate Network and Security Operations Center and WAN application integration services were also established during that timeframe. In 2006, TMP will address rapidly growing capacity and functionality requirements to serve significant new and changed applications that serve VA's missions.

Network capacity and performance of the One-VA network is managed by the Engineering and Capacity Planning team. Over the past year, various enterprise wide programs and technologies have resulted in an 85% increase in backbone bandwidth. To maintain Service Level Agreements, network performance metrics are reviewed on a monthly basis and new bandwidth is provisioned when sustained usage exceeds 75%.

Projections over the next two years indicate that due to various new Veteran health and benefits applications, major modifications to the present One-VA backbone architecture must be implemented within the next fiscal year in order to provide adequate backbone performance. The engineering team has developed a Multi-Protocol Label Switching (MPLS) solution to replace the legacy Asynchronous Transfer Mode (ATM) backbone technology. In addition, to provide adequate Continuity of Operations functionality, a second Federal telecommunications service carrier will provide redundant MPLS service to all backbone locations. This change will effectively double the available capacity of the backbone, decrease long distance induced latency, and provide carrier diversity to all backbone components.

As new applications and technologies are introduced on the One-VA network, it is critical that these projects be engineered properly to function over the One-VA wide area network. Over the past year, the N&IMS engineering team has implemented an admission control process that verifies the functionality of these new applications, and alerts the developers to problems early during the engineering and migration cycle, greatly reducing the risk of application failure as projects migrate to production.

The One-VA Networks Operations Center and Gateway management team have continued to extend the capabilities and enhanced security of the backbone and firewall infrastructure to meet security requirements while maintaining remote access to users outside the One-VA network. This remote access includes various Virtual Private Network (VPN) and Business Partner Gateways (BPG), such as Department of Defense (DOD), necessary for support of various Veteran related health and benefits services. In addition, the gateway team has migrated all SMTP mail users off the legacy gateways to the four new core gateways on the One-VA backbone.

Actions, Progress and Resolution Date

2001-2006 – Telecommunications Modernization Project was approved and executed, resulting in a common network backbone across the VA.

Key Points

- Responding to increasing demands for bandwidth and performance enhancements on the One-VA backbone, the N&IMS team is deploying a diverse carrier, MPLS solution, to replace the single carrier ATM backbone.

- Quality of Service engineering changes has been instituted to segregate and prioritize different classes of applications in order to guarantee network availability during periods of excessive traffic congestion.

- Network capacity growth was approximately 85% in fiscal year 2006.

- Enterprise Telemedicine projects, such as the Ploytrauma Telemedicine Network, have been integrated into a centralized Video Teleconferencing management architecture.

DEPARTMENT OF VETERANS AFFAIRS (VA) - *continued*

- Veterans Benefits Administration legacy frame relay network has been migrated to the One-VA Enterprise network.

- Internal encryption capabilities have been implemented between the VA Internet gateways and specific internal VA sites.

- Enterprise Mail Transfer Agents have been installed within each of the four VA Internet Gateways with Anti-Virus (AV) and Anti-Spam capabilities. Prior to this installation, AV and anti-spam was handled by the individual administrations with varying success. This solution helps prevent malicious and unsolicited traffic from entering the VA network, resulting in bandwidth preservation and improved security.

- Migrated access of all externally facing web servers to the VA Internet Gateways.

- Installed new outbound web solution in all four VA Internet Gateways to include caching, new AV provider and content filtering software.

- Installed an additional T-3 circuit at all four VA Internet Gateways for carrier redundancy and additional capacity.

- VA Domain Name System servers were installed at all four gateways, which provide external resolution and caching of internal va.gov records. The Network Operations Center assumed administrative responsibility for the external va.gov domain.

- Configured several new site-to-site VPN and BPG solutions to allow security connectivity between VA and trusted business partners.

VA Nationwide Teleconferencing System (VANTS)

VANTS provides 24 X 7 audio and video teleconferencing services for business meetings, program planning sessions, distance learning, interviews and hearings. VANTS customers include VA employees, emergency personnel, state officials, hospitals, universities and other federal government agencies, including DOD. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 Kilobit per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 1,512 audio ports for voice teleconferencing.

Frequency Management Automation

To expedite the engineering of new radio frequency assignments, VA uses the latest frequency management software, Spectrum XXI. VA has joined the National Telecommunications and Information Administration in proving the viability of a Government-wide, classified data exchange to update the Government Master File of Radio Frequency Authorizations in real time over the public switched telephone network.

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 (MXU) at geographically dispersed locations to allow the handsets to dial directly into VA facilities via the satellite network. The MXU's also provide VA facilities access to the satelite network without having to go outside of their buildings under adverse conditions. Many of the handsets are also equipped with approved Type I communications security devices to support secure voice communications.

VA Trans-America Radio Program (TARP)

The VA has begun development of a functional Department-wide High-Frequency (HF) emergency radio system that can provide end to end communications between all VA sites. This system is designed to provide, in phases, operable backbone emergency HF communications to include voice, data ALE/non-ALE (short message, long message, fax, e-mail, and bridging to telephone), and both secure and non-secure modes of communications with NVIS capabilities for short range and multiple capabilities to manipulate antenna propagation for long range.

This system will be compatible with Federal Emergency Management Agency, National Communications System, and capabilities wherever possible.

DEPARTMENT OF HOMELAND SECURITY (DHS)

NS/EP Telecommunications Mission

To serve the nation and execute the national security and emergency preparedness (NS/EP) telecommunications mission, the Department of Homeland Security (DHS) engages in critical initiatives that are improving communications capabilities across all levels of government. DHS is designing, implementing, and managing communications systems that enable secure and reliable information sharing during NS/EP activities and is also developing partnerships with Federal, State, local and tribal governments and private entities to ensure communications are in place and operational during significant incidents.

Current/Ongoing NS/EP Telecommunications Activities

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

DHS Wireless Management Office

The DHS Wireless Management Office (WMO) supports the NS/EP mission by leading a unified effort for a DHS-wide integrated wireless enterprise to ensure DHS and other government users have wireless capabilities needed during significant events and crises. The WMO leads initiatives to improve communications for homeland security and emergency preparedness and works to ensure comprehensive planning, coordination, and deployment of critical communications resources and equipment are in place for law enforcement and key government staff.

In fiscal year (FY) 2006, the WMO's NS/EP accomplishments included:

- Provided tactical wireless communications coordination support and equipment following Hurricanes Katrina and Rita and procured tactical communications equipment for the National Operations Center and the Federal Emergency Management Agency (FEMA) Mobile Emergency Response System in preparation for the 2006 hurricane season;

- Supported FEMA Regions IV and VI in development of regional and state hurricane communications plans including development and execution of training and exercises;

- Provided tactical communications support at the Joint Field Office in Baton Rouge, Louisiana;

- Enhanced and expanded the Integrated Wireless Network (IWN) in the Seattle-Blaine, Washington area and began development of an IWN system design for the Southwest border area though coordination with the Secure Border Initiative to meet NS/EP Federal user requirements;

- Initiated the Gulf Coast Project to upgrade and modernize DHS tactical communications systems in the region in partnership with Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE) and Transportation Security Administration (TSA);

- Upgraded CBP, ICE, TSA, U.S. Secret Service, and FEMA equipment based upon the Mission-Essential Technical Baseline established to identify and remedy critical wireless communication needs; and

- Developed frequency management plans for critical law enforcement and gulf coast operations and streamlined DHS-wide spectrum management operations.

SAFECOM

SAFECOM, a communications program of the Department of Homeland Security's Office for Interoperability and Compatibility under the Science and Technology Directorate, works with the emergency response community and Federal partners to develop solutions to address communications interoperability challenges. With these partners, SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to Federal, State, local, and tribal emergency response agencies.

SAFECOM is committed to developing tools—best practices, methodologies, and templates—that serve immediate, critical emergency response needs.

DEPARTMENT OF HOMELAND SECURITY (DHS) - *continued*

In FY 2006, SAFECOM's accomplishments included:

- Published the Statewide Communications Interoperability Planning Methodology, a step-by-step planning guide for developing a locally driven statewide strategic plan, setting the foundation for interoperable communications;
- Conducted the Regional Communications Interoperability Pilots which are initiatives coordinated on the ground to assist implementation of statewide planning processes which will result in models and tools for all 50 states;
- Led RapidCom 1 which included initiatives in 10 high-threat urban areas to establish emergency communications at the command level within 1 hour of an event; SAFECOM provided policy guidance, facilitated table top exercises, and supported governance bodies;
- Developed SAFECOM Grant Guidance to encourage states to develop and adhere to statewide interoperability plans when purchasing equipment using Federal funds;
- Published the Public Safety Architecture Framework Volumes I and II. This Framework helps emergency response agencies map system requirements and identify system gaps;
- Published the Statement of Requirements, Volume I, v.1.0 and v1.1, which provides equipment specifications to manufacturers for emergency responders' communications needs; and
- Established the National Interoperability Baseline Methodology. The National Interoperability Baseline is a survey that will provide a quantitative assessment of the capacity for emergency response interoperable communications.

High Speed Operational Connectivity Program (Hi-SOC)

The Hi-SOC Program provides the underlying network infrastructure to support TSA's mission objectives. The program includes establishing Local Area Network connections in an airport and Wide Area Network connections between the airport and the TSA Hosting Center, along with intelligent phones and standardized desktop/laptop computer configurations.

Transferring 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 potential. These threat mitigation applications include Threat Image Projection System, Electronic Surveillance System, Performance and Results Information System, and U.S. Visitor and Immigrant Status Indicator Technology among others.

National Incident Response Unit/Technical Maintenance Facility

The National Incident Response Unit/Technical Maintenance Facility (NIRU/TMF) provides rapid deployment support of radio equipment and personnel for emergency response and large event activities. This includes two-way radio support for 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 law enforcement duties and enhanced officer safety.

NIRU/TMF provided the following NS/EP support during FY 2006:

- Distributed mobile and portable radio assets and associated equipment to ICE offices nationwide;
- Loaned portable radios to ICE components for use during short-term operations;
- Provided radio equipment and programming support for the presidential election and inauguration; and
- Provided radio equipment, programming, training, and personnel

DEPARTMENT OF HOMELAND SECURITY (DHS) - *continued*

support for Hurricanes Katrina and Rita.

Customs and Border Protection, Office of Information and Technology

CBP, Office of Information and Technology (OIT) operates very high frequency (VHF) and high frequency (HF) radio networks, CBP communications centers, CBP dispatch centers, and various border security systems, such as seismic sensors and remote video cameras. Although CBP OIT does not have a statutory responsibility for ensuring national communications during crises, assets maintained by CBP OIT 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 HF radio program.

During FY 2006, CBP was partially funded to begin modernization of its existing VHF land mobile radio network with the primary focus on the Southwest border of the country and other locales. Modernization will provide for interoperability among CBP users, DHS, and in certain locales, among state and local law enforcement officials.

DHS One Network (One Net)

Established in FY 2005, DHS One Net is a general support system, providing wide-area communications for the service-wide DHS sensitive, but unclassified, environment. One Net provides continuous monitoring of network activity to detect, analyze, report, contain, and remediate 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. The Infrastructure Transformation Program/Chief Information Officer Council (CIOC) is planning the transformation of the Data Communication Network to the next generation One Net.

In FY 2006 the One Net Integrated Project Team stood up the One Net Network Operations Center (NOC) and Security Operations Center and launched the conversion of ICEnet and the TSA network to OneNet. Component network conversions continue until completion in FY 2008 and include the Homeland Security Data Network (HSDN) to OneNet Transport Transition, which utilizes the ability for separation of networks inherent in Multi Protocol Label Switching to provision logically completely separate sensitivity levels over the same transport platform.

National Operations Center

The NOC (formerly the Homeland Security Operations Center), collects and disseminates threat information to 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 NOC is to create a real-time snapshot of the nation's threat environment at any moment to help detect, deter, and prevent terrorist acts. The NOC uses a number of communications technologies to communicate and share NS/EP and threat information. Efforts include:

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

- Application of imagery capability by cross-referencing informational data against geospatial data that pinpoints images down to an exact location using satellite technology.

Homeland Security Data Network

In FY 2006, DHS continued deployment of the HSDN to 56 government sites, providing a unified system and program that enables the sharing and protection secret-level data between its Federal partners. 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.

Integration of Crisis-Related Communications Functions and Customers

DHS began a Department-wide initiative using Project Matrix, an IAIP Homeland Security Presidential Directive-7 methodology to identify DHS component

DEPARTMENT OF HOMELAND SECURITY (DHS) - *continued*

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

- Modern, efficient, and interoperable to support intelligence collection and distribution requirements;

- High-volume and timely for open-source collection; and

- Quick-reacting in support of crises and special operational requirements wherever needed.

Telecommunications Staff Organization

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

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

Current/Ongoing Telecommunications Activities

The following CIA activities support NS/EP objectives:

- Active participation in the National Communications System activities of the Committee of Principals/Council of Representatives

- Continued support of the Government Emergency Telecommunication Services, the Federal Telecommunications Standards Committee, and the Telecommunications Service Priority System.

We are actively transitioning our legacy secure telephone units to the new Secure Terminal Equipment.

We have an active program to add secure video teleconferencing to our desktops.

CIA Significant Accomplishments

Continued to develop a cadre of professional personnel prepared to meet operation, technical, and system management requirements of state-of-the-art telecommunications and automated information systems.

Provided enhanced telecommunications services between the CIA, other U.S. Government organizations, and the U.S. military services.

Continued support to Defense Message System objectives and architecture.

We have added redundancy and eliminated single points of failure for our commercial and secure voice networks.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP Telecommunications Mission

The mission of the Federal Emergency Management Agency (FEMA) is to reduce the loss of life and property and protect the nation's critical infrastructure from man-made and natural hazards through a comprehensive program of mitigation, planning, response and recovery. FEMA helps the nation address communications network disruptions, manages federal response and recovery efforts following any national incident and serves as the nation's portal for emergency management information. FEMA evaluates and adopts new telecommunications technologies to ensure that government agencies can accomplish their missions effectively.

Current/Ongoing NS/EP Telecommunications Activities

FEMA helps communities face the threat of terrorism and respond to all types of hazards. FEMA establishes working relationships with state and local first responder and public safety communications organizations. In addition, FEMA:

- Plans for, provides, operates and maintains information technology (IT) and telecommunications services and facilities as part of the National Emergency Management Information System (NEMIS);
- Designs and develops emergency networks and information systems;
- Provides communications support to State and local officials to help disseminate warnings of risks and hazards;
- Accumulates and assesses damage information;
- Deploys telecommunications and IT assets to incident areas and coordinates Telecommunications Service Priority and other requests for communication service and connectivity; and
- Coordinates the assignment and use of all Federal radio frequencies at an incident site.

Significant Achievements

FEMA was directly involved in the standardization of a Common Alerting Protocol was for use by public television, cellular phones, pagers, and satellites to improve the existing public Emergency Alerting System.

NEMIS supported 107 disaster and emergency declarations. NEMIS was upgraded and web-enabled so disaster victims could apply for assistance using the Internet.

Interactive voice response service was added to the FEMA telephone network to enable disaster victims to check the status of their applications. Telephone messages were sent to disaster victims to confirm receipt of their substantiating materials. FEMA's data network bandwidth was increased to OC-3 to meet unprecedented load and relieve saturation. Improved security features were added to communications networks joining Federal Continuity of Operations sites.

Mobile Emergency Response Support enhancements included the rapid buildout of communications and office equipment, and the addition of 30 new vehicles to the mobile disaster recovery fleet.

The FEMA National Radio System multiphase upgrade project started in fiscal year (FY) 2005. Engineering, design and acquisition of hardware and software resources for architectural upgrade of a network control station and two remote stations were performed in FY 2006.

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 Commanders, 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 seven functionally aligned divisions, and a Director's Action Group that includes a Programs and Budget element.

Significant Accomplishments

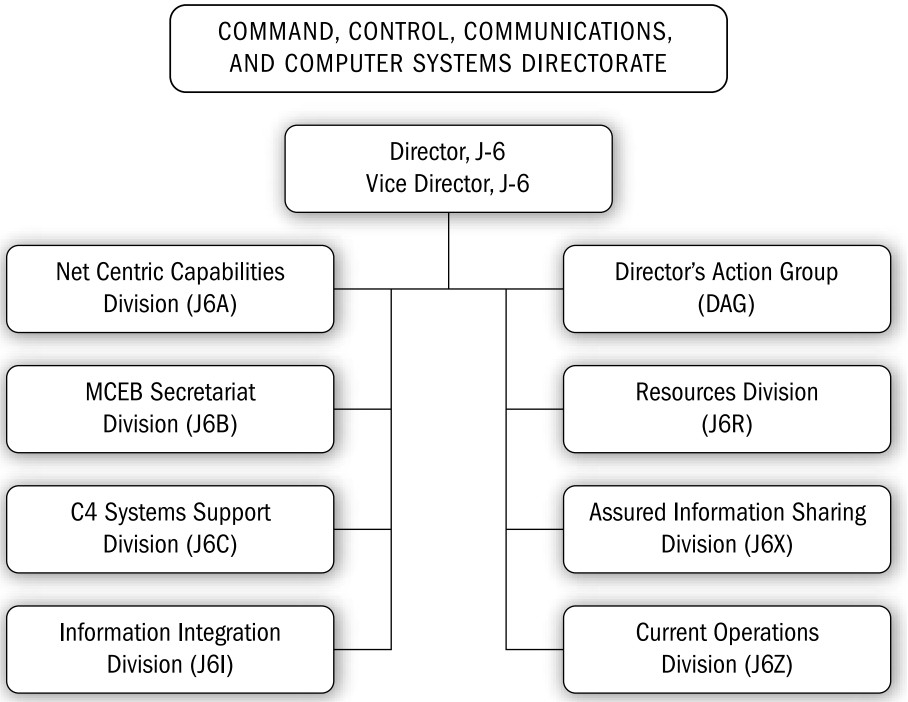
(Refer to DOD Section)

Current/Ongoing NS/EP Telecommunications Activities

(Refer to DOD Section)

Pending Issues

(Refer to DOD Section)


COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE
Director, J-6
Vice Director, J-6
Net Centric Capabilities Division (J6A)
MCEB Secretariat Division (J6B)
C4 Systems Support Division (J6C)
Information Integration Division (J6I)
Director's Action Group (DAG)
Resources Division (J6R)
Assured Information Sharing Division (J6X)
Current Operations Division (J6Z)

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 Acquisition Service (FAS) 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 national security and emergency preparedness (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.O. 12656, *Assignment of Emergency Preparedness Responsibilities*;

- Office of Science and Technology Policy (OSTP): *National Plan for Telecommunications Support in Non-Wartime Emergencies*; and

- National Response Plan.

Current/Ongoing NS/EP Telecommunications Activities

GSA/FAS 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.

FAS helps client agencies develop solutions for customers using a variety of contracts. FAS 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 Department of Homeland Security, National Communications System (NCS) and Executive Office of the President, OSTP 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/FAS 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 Public Key Infrastructure services to assist Federal agencies in meeting the requirements of the *Government Paperwork Elimination Act*.

Significant Accomplishments

- GSA FAS deployed 12 NCS Regional Emergency/Federal Emergency Communications Coordinators from almost all the regions to staff the Regional Response Coordinating Centers, the Joint Field Offices, and State Emergency Operations Centers in FEMA Regions 4 and 6. All 12 served for a duration of several weeks, some continuously, some returning for a second tour.

- Provided support on Continuity Of Operations Plan and NS/EP exercises throughout the country and provided telecommunications support to FEMA as required for numerous disasters.

- Reactivated the FAS participation in the National Defense Executive Reserve which is a program for recruiting and training experienced business executives and other civilian personnel to serve in key government positions during periods of national emergency. Reservist will augment the FAS staff of Federal departments and agencies when organizations must rapidly mobilize to respond to national security emergencies.

GENERAL SERVICES ADMINISTRATION (GSA) - *continued*

- Supported activities of the Committee on National Security Systems.

GSA/FAS continues to provide vendors and agencies information regarding all FAS services, including disaster support, contingency planning, and continuity of operations services through the GSA home page (http://www.gsa.gov).

National Aeronautics and Space Administration (NASA)

NS/EP Telecommunications Mission

The National Aeronautics and Space Administration (NASA) 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 Space Operations Mission Directorate 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 and manage NASA resources 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.

NS/EP Telecommunications Assets

NISN supports both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency, its contractor and research partners, and International Space Partners.

NASA Space Network is a constellation of geostationary Tracking and Data Relay Satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft and other supported customer satellites.

NASA Deep Space Network 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.

Significant Accomplishments

- Provided a NASA employee detailee to the NCS;
- Actively participated in the NCS Continuity Communications Architecture Development;
- Increased the number of NASA employee Government Emergency Telecommunications Service card holders;
- Participated in Sharers Exercises from multiple conus dispersed NASA facilities; and
- Participate in the Telecommunications Service Priority System.

NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP Telecommunications Mission

The Nuclear Regulatory Commission (NRC) is responsible for ensuring adequate protection of the public health and safety, the common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the United States. Activities licensed and regulated by the Commission include commercial nuclear power reactors; non-power 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 national security and emergency preparedness (NS/EP) telecommunications provide for highly reliable connectivity between the NRC emergency operations center, operating nuclear power plant control rooms, various emergency operations facilities, and regional incident response centers. This connectivity provides a means for 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 continues to support the National Communications System's (NCS) NS/EP programs and remains active in NCS Committee of Principals and Council of Representatives activities. The systems and programs used in support of NS/EP telecommunication include Emergency Telecommunications System, Satellite Phones, Wireless Priority Service (WPS), Government Emergency Telecommunications System (GETS), Critical Warning Infrastructure Network (CWIN), Secure Communications and Secure Video Teleconferencing System.

Presently, forty-two (42) U.S. nuclear plants use ETS with Telecommunications Service Priority through FTS 2001 and twenty-three plants use private corporate systems. Satellite phones are used by headquarters, regions, and federal inspectors at every U.S. nuclear power plant. WPS is used on cell phones assigned to key agency staff and members of the NRC incident response organization. GETS is used by agency staff to enhance access to long distance service. A CWIN terminal and telephone is maintained in the Headquarters Operations Center. Secure communications is maintained between the agency and licensed nuclear facilities and Secure Video Teleconferencing is used in the Headquarters Operations Center and at all of the NRC Regional Incident Response Centers. The NRC continues to conduct quarterly testing of GETS, Satellite phones and WPS and presently, many of the communication systems used in the NRC Headquarters Operations Center are being replaced or upgraded.

Significant Accomplishments

- New Executive Team Briefing system installed;
- WPS program successfully implemented; and
- Additional satellite phones deployed.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP Telecommunications Mission

The National Telecommunications and Information Administration's (NTIA) national security and emergency preparedness (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 spectrum policy for the 21st century in response to the President's Spectrum Policy Initiative of May 2003. OSM developed a Federal Strategic Spectrum Plan using information from Federal Department Strategic Spectrum Needs Plans. Part of the OSM vision is to use information technology to automate the spectrum management business processes and to be more effective and efficient in all Federal spectrum use including NS/EP applications. Specific examples of activities in this regard include the following:

- Using an OSM Enterprise Architecture Council to develop information technology requirements of the Federal spectrum management community and an implementation plan to satisfy those requirements.

- Continuing efforts under a memorandum of agreement with the Federal Communications Commission and the Department of Defense's Joint Spectrum Center to leverage available resources in developing common spectrum management systems and approaches as appropriate.

- Continuing to plan and implement, using a phased approach, a series of Federal spectrum management system improvements.

- Continuing 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 is continuing to:

- Serve as a non-resident member of the National Communications System's (NCS) National Coordinating Center for Telecommunications (NCC) – Information Sharing and Analysis Center (ISAC).

- Participate in various NS/EP support activities relative to national emergency management and continuity of government as well as agency continuity of operations.

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

- Serve as Co-Chair of the Government Emergency Telecommunications Service (GETS)/Wireless Priority Service (WPS) User Council, participate in Council endeavors, and provide GETS/WPS user authorizations to all new NTIA emergency employees.

- Serve as a Government member of the NCS Telecommunications Service Priority Oversight Committee.

- Participate in 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.

- Participate in the NCS SHAred RESources (SHARES) High Frequency (HF) Coordination Network and in NCS SHARES HF Interoperability Working Group activities.

Significant Accomplishments

- Fully supported the NCS relative to the National Response Plan Emergency

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) - *continued*

Support Function (ESF-2), Communications.

- Served as lead agency in developing the Frequency Management Appendix to the ESF-2 Operations Plan.

- Supported the ESF-2 Training Event in May 2006 with five NTIA personnel participating.

- Assisted in developing the Interim National Emergency Communications (NEC) Strategy as a member of the Interim NEC Strategy Working Group.

- Spearheaded an effort to streamline the procedures for authorizing use of Federal incident response frequencies to achieve interoperability between Federal and non-federal emergency response personnel.

- Conducted interagency frequency management portion of Exercise FORWARD CHALLENGE 2006.

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

NATIONAL SECURITY AGENCY (NSA)

NS/EP Telecommunications Mission

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

Information Technology and Information Assurance

Within NSA, several organizations share responsibility in supporting NS/EP related activities: National Information Assurance Research Laboratory (NIARL), information assurance (IA) worldwide enterprise, and Information Technology Directorate (ITD).

- The NIARL conducts and sponsors research in the technologies and techniques needed to secure U.S. national security systems, to include cryptography, high-confidence software and systems, authentication, high speed security solutions, secure wireless multimedia, secure operating systems and network management, privilege management, and controlled sharing.

- The IA enterprise teams across academia, industry, and Government to provide IA solutions to keep U.S. national security systems safe from harm. This mission involves detecting, reporting, and responding to cyber threats, as well as making encryption codes to securely pass information among systems. It includes embedding IA measures directly into the Department of Defense's emerging Global Information Grid (GIG); building secure audio and video communications equipment; making tamper protection products; providing trusted microelectronics products; testing the security of systems; providing operational security assistance; as well as evaluating commercial software and hardware against nationally set standards.

- The ITD plans and operates the telecommunications systems and networks that link NSA elements worldwide, as well as provide connectivity to other Government services.

In accordance with its National Security Systems Manager responsibilities under National Security Directive 42, NSA IA products and services also are 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 close working relationships with the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), and other entities with information assurance responsibilities.

Current/Ongoing NS/EP Telecommunications Activities

NSA Commercial Solutions Center for NS/EP Telecommunications

- The NSA Commercial Solutions Center (NCSC) was established to collaborate with industry and Government. This collaboration involves the design, development, procurement, and deployment of commercial technology and IA-enabled end products, devices/components, specifications, and guidance needed to enable of the capability areas of the IA component of the GIG. A significant mission element of the NCSC is to create a collaborative environment with commercial Information Technology firms to foster solutions to national security problem sets.

NSA Threat Operations Center for NS/EP Telecommunications

- The NSA Threat Operations Center (NTOC) provides real-time global network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity directed against U.S. national security systems and to enable U.S. Computer Network Operations. NTOC activities includes the discovery and reporting of malicious network behavior; identification and provision of mitigation and response action options; network intrusion analyses; and ensuring appropriate procedures, oversight, and compliance are known

NATIONAL SECURITY AGENCY (NSA) - *continued*

and implemented throughout U.S. national security systems.

Cryptographic Modernization Initiative Supporting NS/EP Telecommunications

- The Cryptographic Modernization Initiative is a DOD-directed/NSA-led effort to transform and modernize IA capabilities for the 21st century. The initiative coordinates and oversees modernization of DOD IA capabilities by replacing an aging cryptographic product inventory, meeting increased interoperability needs, keeping pace with the evolution of information technology, and achieving objectives needed to enable the information assurance component of the DOD GIG architecture.

- Achieved two major milestones: Assessment of Type 1 Cryptographic Inventory, January 2005, which lists all known cryptographic devices; and issuance of 11 Cryptographic Decertification messages signed by the NSA Director of IA in September 2005.

Electronic Key Management System for NS/EP Telecommunications Systems

- 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 will continues to provide the primary means for distribution of electronic key (both conventional and public key certificates) intended for classified applications.

- Continued development of EKMS Tier 2 Local COMSEC Management Software Version 5.1, which unifies baselines into a single Tier 2 baseline.

- Upgrade EKMS Communications—Both Secret Internet Protocol Router Network (SIPRNET) and initial Non-Classified Internet Protocol Router Network capabilities were completely and integrated to the message server. SIPRNET Tier Pilot accounts were established and Tier 2 customers have seen a substantial improvement in performance in receiving their key and message from the message server

- Provide Coalition Re-key Guard software and hardware release to correct System Integration and Test issues uncovered. System ready to begin Developmental Test and Evaluation testing. Deployment scheduled for September 2006, which will provide re-key services to War-fighter coalition partners.

- Awarded a contract to fix operational discrepancies associated with Card Loader User Application Software, software used to load Secure Terminal Equipment key material in the field and enabling much quicker receipt/use of key for the War-fighter requiring secure voice.

High Assurance Internet Protocol Encryption

- The first generation of 100 megabits per second and 1 gigabit per second inline network High Assurance Internet Protocol Encryptors (HAIPE) have been deployed to secure the high speed transport pipes. Work continues on the development of higher speed implementations at 10 and 40 Gbps and beyond as well as migrating the entire HAIPE product line to support Internet Protocol version 6 by 2008.

Security Assessments Supporting NS/EP Telecommunications

- 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.

IA Services Supporting NS/EP Telecommunications

- NSA continues to provide a variety of IA services. In 2005, NSA issued the following IA guidance documents for use by industry and the Government: Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF; Center for Internet Security Benchmark for Oracle 9i/10g, Version 2.0; and Center for Internet Security Exchange Server 2003 Benchmark, Version 1.0.

NATIONAL SECURITY AGENCY (NSA) - *continued*

- A Defense Advanced Research Projects Agency employee was honored with the NSA 2005 Rowlett Individual Excellence Award for breakthrough research into cyber defense to include technology that automatically quarantines computer-based worms, limiting their migration and restoring the user's computer to its pre-infected state within minutes. This individual achievement award is given annually to the individual within a Government organization making the most significant contribution to improving his/her element's information systems security posture, IA readiness, or the conduct of defensive information operations (DIO).

- The United States Naval Academy took top honors over each of the five U.S. service academies (Army, Air Force, Coast Guard, and Merchant Marine) in the 2005 Cyber Defense Exercise (CDX), a one-of-a-kind training tool to prepare the students to protect and defend the nation's critical information systems. The CDX is just one example of NSA's educational outreach.

- NSA and DHS continue their joint management of the National Centers of Academic Excellence in IA Education by approving the addition of eight more universities. Additionally, NSA/DHS approved the re-applications of seven other universities.

- NSA and NIST jointly announced the public availability of the Extensible Configuration Checklist Description Format (XCCDF). NSA and NIST collaborated with industry to develop the XCCDF specification to promote the use, standardization, and sharing of effective security checklists. XCCDF is vendor-neutral, and provides a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, thereby fostering a more widespread application of good security practices.

NSA/CSS Threat Operations Center

- The NSA/CSS Threat Operations Center (NTOC) provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique, tailored, time-critical and term reporting based on NTOC'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.

Defensive Information Operations Assessments/Monitoring

- Defensive Information Operations provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique leadership and technical expertise in the areas of operations, community coordination, policy, as well as analysis and reporting which was uniquely tailored to NSA's ability to detect, react, warn, and respond to intrusions into U.S. Government cyber networks. DIO assessments provided a unique look at U.S. government systems, operations, personnel, and current technology enabling the protection and defense of information and information systems and to promote and maintain Operations Security (OPSEC) principles worldwide. Monitoring of U.S. Government communications assisted in the identification of information that may have been exploitable by adversaries and provided advice to mitigate that risk.

Global Information Grid

- NSA's Enterprise IA Architecture and Systems Engineering office, in partnership with the GIG community, leads the effort to define the enterprise level IA strategies, guidance, standards, policies, systems requirements and technologies necessary to realize DOD's net-centric GIG vision. While the office's principal focus is in supporting the DOD's GIG, its work is broadly applicable to net-centric enterprise efforts across the Intelligence Community (IC), DHS, Information Sharing Environment (ISE) and other federal Information Technology (IT) enterprise efforts. These national security communities require the development of an assured global

NATIONAL SECURITY AGENCY (NSA) - *continued*

national security IT enterprise to transform the way they operate, communicate and use information to accomplish their missions. NSA's IA support will help ensure that communications, information sharing and infrastructure availability are not barriers to the Nation's security.

Vulnerability Analysis and Operations Assessments/Monitoring

- The Vulnerability Analysis and Operations/Group (VAO) provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique leadership and technical expertise in the areas of operations, technology analysis, community coordination, policy, as well as analysis and reporting which was uniquely tailored to NSA's ability to detect, react, warn, and respond to intrusions into U.S. Government cyber networks. VAO performed near real time vulnerability analysis and assisted key customers in mitigating intrusions and restoring network trust. Through close partnership with DOD and National customers, this group provided operational, crisis, and exercise planning to ensure that CNO activities and response promoted good actionable defense measure, thus enabling offensive missions. The group's assessments provided a unique look at U.S. Government systems, operations, personnel, and current technology, enabling the protection and defense of information and information systems while promoting and maintaining OPSEC principles worldwide. VAO monitoring of U.S. Government communications assisted in the identification of information that may have been exploitable by adversaries and led to the development of measures to mitigate that risk. This expert operational analysis and guidance is sustained through state-of-the-art technology evaluations covering a wide range of communication components, network appliances, and software applications.

United States Postal Service (USPS)

NS/EP Telecommunications Mission

The Postal Service delivers to every household and business in the United States. Every American has access to our products and services and pays the same postage rate for First-Class® Mail service regardless of geographic location. We:

- Deliver 212 billion pieces of mail to over 144 million homes, businesses and Post Office boxes in virtually every state, city, and town in the country, including Puerto Rico, Guam, the American Virgin Islands and American Samoa.
- Handle more than 44% of the world's card and letter mail volume—delivering more mail to more addresses and to a larger geographic area than any other postal service in the world.
- Serve over 7.5 million customers daily at more than 37,000 Post Offices™. And 1,450 of our Post Offices now stay open later.
- Provide stamps at:
  - More than 27,800 vending machines;
  - Nearly 25,400 commercial retail outlets;
  - Nearly 15,300 banking and credit union ATMs; and
  - 2,500 Automated Postal Centers®.
- Have an annual operating revenue of nearly $70 billion.
- Employ more than 700,000 career employees, who communicate with each other on the world's largest intranet.
- Pay more than $2 billion in salaries and benefits every two weeks.

Information Technology (IT) is dedicated to helping the Postal Service improve service and operations through technology. In the telecommunications area, IT has equipped key personnel with the tools necessary to continue operations in the event of national/local emergencies or disasters. IT has employed National Communications System tools and offerings such as the Government Telecommunications System (GETS) and Wireless Priority Service (WPS) to many key personnel in order to maintain vital communications and services to the public.

IT has also upgraded all of the Postal Services Large Private Branch Exchange (PBX) Telephone Systems throughout the country. IT has also refreshed many Key Telephone Systems at smaller Postal Service facilities throughout the country.

The Postal Service has not been assigned any specific national security and emergency preparedness telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the Postal Service designs, engineers and develops telecommunication systems, services and solutions to support day to day organizational, administrative and operational mission requirements.

Significant Accomplishments

Upgrading the Telecommunications Infrastructure (Voice)

After the extensive improvements to the Postal Service Data Network in fiscal year (FY) 2005, the Postal Service moved to upgrade the voice communications network throughout the country. The two major types of telephone systems, PBX and Key Telephone Systems were targeted for improvements.

Private Branch Exchange Telephone System (PBX)

The Postal Service standard PBX is a Nortel. There are various models that are equipped throughout the larger offices within the system. Options 11, 61 and 81 are the models that are deployed and were targeted for upgrading.

The upgrading of these systems included the latest vintage software as offered by Nortel along with improvements in hardware and adjunct systems. All PBX's have integrated voice mail, Uninterruptible Power Supplies, administrative terminal access and call accounting.

Furthermore the upgrade effort included hardware and software for these systems to operate in a Voice over

United States Postal Service (USPS) - *continued*

Internet Protocol environment. Presently these systems are operating with conventional Digital Primary Rate Interface trunks for commercial and within network calling.

In FY 2006, the Postal Service upgraded 518 PBX's.

Key Telephone Systems

The Postal Service standard Key System is an Avaya. These systems are sized depending on the amount of handset required by the facility. Each system is equipped with one cordless telephone to offer mobility for the supervisor. Some systems have voice mail and Uninterruptible Power Systems.

These systems are connected into the Public Switched Network via conventional telephone lines from the Local Exchange Carriers.

In FY 2006, the Postal Service refreshed a total of 167 Key Telephone Systems

PBX Security

All PBX's in the U.S. Postal Service have been configured to limit the amount of access local personnel have to make changes to the system. The PBX's are locked down to not allow trunk to trunk transfers which can open the systems up to hackers. The PBX's are also monitored for calling patterns that are unusual that would indicate fraudulent or criminal activity maybe occurring.

All PBX's are monitored at a Central Network Operations Center so that any alarms or malfunctions can be acted on immediately. In addition, Postal executives are advised in real time about the state of these PBX's so that pro-active plans maybe issued to advise employees and business partners of any outage or malfunction.

Government Telecommunications Service (GETS)

During FY 2006 an effort was made to deploy GETS accounts to Postal executives and key personnel responsible for Continuance Of Operations duties. These accounts are to provide emergent landline communications when telephone systems experience congestion due to local or national situations. There are more than 650 GETS accounts assigned to Postal employees.

Wireless Priority Service (WPS)

In conjunction with the GETS deployment, WPS activations have been assigned to key members of the Postal Service in order to provide emergent communications in cases where cell towers become congested due to local or national situations. There are more than 75 WPS accounts assigned to Postal employees.

FEDERAL RESERVE BOARD (FRB)

NS/EP Telecommunications Mission

The Federal Reserve Board's (FRB) 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 Associate Director 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 National Communications System's (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) Federal Deposit Insurance Corporation (FDIC) 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.

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 (such as 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, and other qualifying financial service utilities;

FEDERAL RESERVE BOARD (FRB) - *continued*

- 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; and
- Circuits used by the World Bank to ensure continuity of operations.

By the end of this fiscal year, there will be approximately 4,600 active TSP assignments including circuits directly sponsored by the FRB as well as those circuits administered for the SEC, OCC, CFTC, NCUA, FDIC 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 55 institutions.

During the last fiscal year, the FRB continued to participate in the evolution of the WPS program. The FRB has sponsored approximately 30 institutions for WPS.

National Diversity Assurance Initiative

In 2005 and early 2006, the National Diversity Assurance Initiative, led by the Alliance for Telecommunications Industry Solutions Chief Information Officer Council and the Federal Reserve Board, evaluated the problem inherent in assuring physical diversity of NS/EP financial service circuits in a multi-carrier environment. At the completion of the Assessment Phase, the team concluded that end-to-end multi-carrier circuit diversity assurance currently cannot be conducted in a scalable manner. The cost and level of manual effort required were comparable to the assessment step and demonstrated that an ongoing program for end-to-end multi-carrier circuit diversity assurance, as it exists today, cannot be offered as a widely available commercially viable product. The team recommended a follow-up effort to determine more accurately the requirements for providing an automated end-to-end diversity assurance solution in a multi-carrier environment. As a first step, a small-scale effort could be undertaken to leverage the findings of the Initiative to scope the objectives and requirements for providing an end-to-end diversity assurance solution in a multi-carrier environment.

The FRB has developed contingency plans to continue the operation of the NS/EP priority telecommunications programs in the event of a pandemic flu outbreak. The plan incorporates the training and equipping of staff located in disparate regions of the country.

Federal Communications Commission (FCC)

NS/EP Telecommunications Mission

The Federal Communications Commission's (FCC) national security and emergency preparedness responsibilities include the following:

- Developing policies that promote access to effective communications services in emergency situations by public safety, health, defense, and other emergency personnel, as well as all consumers in need;

- Evaluating and strengthening measures for protecting the Nation's critical communications infrastructure;

- Facilitating rapid restoration of the United States communications infrastructure and facilities after disruption by any cause;

- Participation in international organizations and conferences to coordinate protection of the global communications infrastructure; and

- Coordination with industry and other federal, state, tribal, and local agencies on matters of public safety, homeland security, and disaster management.

Current/Ongoing NS/EP Telecommunications Activities

- On March 17, 2006, the FCC voted unanimously to establish a Public Safety and Homeland Security Bureau. The new Bureau is designed to provide a more efficient, effective, and responsive organizational structure to address public safety, homeland security, national security, emergency management and preparedness, disaster management, and other related issues. The new Bureau was launched on September 26, 2006.

- In January of 2006, Chairman Kevin J. Martin, established the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel). The Katrina Panel examined the impact of Hurricane Katrina on all sectors of the telecommunications and media infrastructure in the areas affected by Hurricane Katrina, including public safety communications systems. The Katrina Panel made recommendations to the FCC on June 12, 2006, regarding ways to improve disaster preparedness, network reliability, and communications among first responders such as police, fire fighters, and emergency medical personnel. On June 19, 2006, the FCC released a notice of proposed rulemaking seeking comment on the Katrina Panel's findings and recommendations.

- On March 17, 2006 the FCC adopted an Eighth Notice of Proposed Rulemaking (Notice) that seeks comment on whether certain channels within the 24 Megahertz (MHz) of spectrum in the 700 MHz band allocated for public safety use should be modified to accommodate broadband communications. The 700 MHz public safety spectrum is currently being used bwy television broadcasters during the digital television (DTV) transition but will become available for use by public safety agencies by February 18, 2009, (as mandated by Congress) when the DTV transition is completed. The Notice asks commenters to update the record regarding wideband interoperability and the Scalable Adaptive Modulation standard in light of proposals to accommodate broadband communications.

- On April 26, 2006, the FCC adopted a Second Report and Order and Memorandum Opinion and Order (Order) that addresses several issues regarding implementation of the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. The primary goal of the Order is to ensure that Law Enforcement Agencies have all of the resources that CALEA authorizes to combat crime and support homeland security, particularly with regard to facilities-based broadband Internet access providers and interconnected voice over Internet protocol providers. The Order balances the needs of Law Enforcement with the competing aims of encouraging the development of new communications services and technologies and protecting customer privacy.

- On December 19, 2005, the FCC issued a Report to Congress pursuant to

FEDERAL COMMUNICATIONS COMMISSION (FCC) - *continued*

Public Law No. 108-458 that examines, in light of Hurricanes Katrina, Rita, and Wilma, the spectrum needs of traditional public safety entities and other critical first responders. The Report also considers proposals to enhance public safety interoperability, particularly broadband interoperability, ranging from the deployment of a nationwide, interoperable network to more easily achievable solutions that employ widely available commercial technologies.

- Through its Part 4 Network Outage reporting rules, the FCC continues to monitor the reliability of the nation's telecommunications infrastructure, including critical facilities. This work has led to the identification of a number of areas for attention that FCC staff has worked collaboratively with industry to address through forums like the Alliance for Telecommunications Industry Solutions Network Reliability Steering Committee.

Significant Accomplishments

- The FCC took a number of initiatives to support relief and communications efforts related to Hurricanes Katrina, Rita, and Wilma, including: outreach to all segments of the communications industry to determine requirements and assets for rapid recovery of essential communications services; grant of more than one hundred special temporary authorizations and temporary frequency assignments for wireline, wireless, satellite, and broadcasters to expedite recovery of communications services; and provision of over $200 million in universal service funding for reestablishment of communications services in the disaster area.

- Senior FCC staff members chaired or participated in committees and working groups chartered by the U.S. Department of Homeland Security and its functioning entities, such as the Federal Emergency Management Agency and the National Communications System (NCS).

- The FCC maintained its oversight of the Telecommunications Service Priority (TSP) and Wireless Priority Service (WPS) programs and worked with the NCS to address outstanding issues. Earlier this year, a working group chaired by a senior FCC staff member submitted a report to the NCS Committee of Principals on how to improve the TSP program. The FCC reviewed TSP and WPS enrollment figures and sought ways to increase both visibility of and enrollment in the two programs. Of note, the FCC sponsors state and local 9-1-1 Call Centers (Public Service Answering Points or PSAPs) for entry into the TSP. Senior FCC staff members are working with officials from New York to facilitate a large-scale TSP enrollment.

- FCC staff members met with Federal, State, local, and tribal Governments, along with industry and non-governmental organizations, to discuss Public Safety Communications topics, including operable and interoperable communications, spectrum availability and management, emergency preparedness, Emergency Support Function-2, Emergency Alert System, TSP, WPS, and CALEA.

A

Acronyms

A

NCS RELATED ACRONYMS

A

ACH	Automated Clearing House
ACN	Alerting and Coordinating Network
ACR	Alternate Carrier Routing
AGCS	AG Communications Systems
AIN	Advanced Intelligence Network
AgPRS	Agriculture Public Safety Radio System
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
ASD (HD)	Assistant Secretary of Defense for Homeland Defense
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
ASIP	Assistant Secretary for Infrastructure Protection
ATG	Advanced Technology Group

B

BCIS	Bureau of Citizenship and Immigration Services
BDT	Backup Dial Tone

C

C4	Command, Control, Communications and Computer Systems
C&A	Certification and Accreditation
CALEA	Communications Assistance for Law Enforcement Act
CBP	Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear
CC	Continuity Communications
CCPC	Civil Communications Planning Committee
CCWG	Continuity Communications Working Group
CDMA	Code Division Multiple Access
CDX	Cyber Defense Exercise
CEP	Civil Emergency Planning

CEPTAG	Civil Emergency Planning Telecommunications Advisory Group
CFTC	Commodoties and Futures Trading Commission
CFWG	Critical Facilities Working Group
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CLS	Continuous Linked Settlement
COG	Continuity of Government
COMSEC	Communications Security
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives (III-39)
COR	Central Office of Records (IV-38)
CSC	Computer Sciences Corporation
CSCC	Communications Sector Coordinating Council
CTCP	Canadian Telecommunications Cyber Protection
CTIA	Cellular Telecommunications and Internet Association
CY	Calendar Year

D

DHS	Department of Homeland Security
DIO	Defense Information Operations
DISA	Defense Information Systems Agency
DISALAN	Defense Information Systems Agency Local Area Network
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
DPA	Defense Production Act
DTS	Diplomatic Telecommunications Service
DTS2	Digital Telecommunications Switching System

E

E9-1-1	Enhanced 9-1-1
EA	Enterprise Architecture
EAP	Extensible Authentication Protocol
EBS	Emergency Broadcasting System
ECN	Emergency Communications Network
EDW	Enterprise Data Warehouse
EIP	Enterprise Information Portal

EKMS	Electronic Key Management System
EMP	Electromagnetic Pulse
E.O.	Executive Order
EOC	Emergency Operations Center
EOP	Executive Office of the President
EOT	Emergency Operations Team
EPS	Electronic Production System
ERLink	Emergency Response Link
ESF-2	Emergency Support Function #2
ESOC	Enterprise Server Operation Center
ESWG	End-to-End Services Working Group
ETS	Emergency Telecommunications System

F

FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEA	Federal Enterprise Architecture
FEB	Federal Executive Branch
FEMA	Federal Emergency Management Agency
FPKIPA	Federal Public Key Infrastructure Policy Authority
FNARS	FEMA National Radio System
FOC	Full Operational Capability
FPC	Federal Preparedness Circular
FRB	Federal Reserve Board
FTS	Federal Technology Service
FTS2001	Federal Telecommunications System 2001
FY	Fiscal Year

G

GETS	Government Emergency Telecommunications Service
GIG	Global Information Grid
GITM	Global IT Modernization
GN	Ground Network
GPRA	Government Performance and Results Act
GPS	Global Positioning System
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
HPC	High Probability of Completion
HPM	High Power Microwave
HQ	Headquarters
HSC	Homeland Security Council
HSCL	Homeland Security Communication Link

HSDN	Homeland Security Data Network
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
HSRP	Hot Standby Routing Protocol
HSTL	Homeland Security Telephone Link

I

IA	Information Assurance
IAIP	Information Analysis and Infrastructure Protection
IAM	Initial Address Message
IC	Integration Contractor
IEEE	Institute of Electrical and Electronic Engineers
IES	Industry Executive Subcommittee
IG	Inspector General
IMA	Individual Mobilization Augmentee
IMWG	Incident Management Working Group
INCCO	Interagency National Coordinating Center Office
INE	Inline Network Encryption
IP	Internet Protocol
IR	Industry Requirements
IRS	Internal Revenue Service
ISAC	Telecommunications Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
ITD	Information Technology Directorate
IWN	Integrated Wireless Network
I-WPS	Immediate Wireless Priority Service
IXC	Interexchange Carrier

J

J6	Command, Control, Communications, and Computer Systems Directorate
JS	Joint Staff
JTRB	Joint Telecommunications Resources Board

L

LAN	Local Area Network
LEC	Local Exchange Carrier
LCMS	Local Communications Security Management Software
LMD	Local Management Device
LMR	Land Mobile Radio
LRTF	Legislative and Regulatory Task Force

M

MHD	Magneto Hydro Dynamics
MSRC	Media Security and Reliability Council

N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCCTF	National Coordinating Center Task Force
NCS	National Communications System
NCSC	NSA Commercial Solutions Center
NCSD	National Cyber Security Division
NCUA	National Credit Union Administration
NDAC	Network Design and Analysis Capability
NEMIS	National Emergency Management Information System
NGN	Next Generation Networks
NGNTF	Next Generation Network Task Force
NGPS	Next Generation Priority Service
NIARL	National Information Assurance Research Laboratory
NICC	National Infrastructure Coordination Center
NIIF	Network Interconnection Interoperability Forum
NIPP	National Infrastructure Protection Plan
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
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
NTOC	NSA Threat Operations Center
NTRWG	Near Term Recommendations Working Group

O

OA	Operatonal Analysis
OC	Oversight Committee
OCC	Office of Comptroller of Currency
OCIO	Office of the Chief Information Officer's
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OSD	Office of the Secretary of Defense
OSIS	Open Source Information System
OSM	Office of Spectrum Management
OSSS	One-Stop Shop Service
OSS	Operations Services Systems
OSTP	Office of Science and Technology Policy
OTS	Office of Thrift Supervision

P

PAS	Priority Access Service
PBX	Private Branch Exchange
PDD	Presidential Decision Directive
PKI	Public Key Infrastructure
PN	Public Network
POTS	Plain Old Telephone Service
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

S

S&T	Science and Technology
SAFECOM	Wireless Public Safety Interoperable Communications Program
SAFETY Act	Support Anti-Terrorism by Fostering Effective Technologies Act
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified

SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SCIP	Statewide Communications Interoperability Planning
SEC	Securities and Exchange Commission
SHARES	Shared Resources High Frequency Radio Network
SIPRNET	Secure Internet Protocol Router Network
SITREP	Situation Report
SMART	State Messaging and Archive Retrieval Toolset
SPP	Security and Prosperity Partnership
SS7	Signaling System 7
SSA	Sector Specific Agency
SSAA	System Security Authorization Agreement
SSP	Sector Specific Plan
STE	Secure Terminal Equipment System
STU III	Secure Telephone Units, Third Generation
SURWG	Scenarios and User Requirements Working Group
SVDC	Secure Video and Data Collaboration

T

TAL	Technology Assessment Laboratory
TATF	Trusted Access Task Force
TCS	Treasury Communications System
TCO	Tactical Communications Organization
TEDE	Telecommunications Electromagnetic Disruptive Effects
TEPITF	Telecommunications and Electric Power Interdependency Task Force
TGCC	Telecommunications Government Coordination Council
TIB	Technical Information Bulletin
TMN	Telecommunications Management Network
TMP	Telecommunications Modernization Project
TOP	Technology Operations Program
TOPOFF	Top Officials Exercise
TSA	Transportation Security Administration
TSO	Telecommunications Services and Operations
TSP	Telecommunications Service Priority

U

UCC	Universal Computing Connectivity
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
USDA	United States Department of Agriculture

USG	United States Government
USPS	United States Postal Service
USS	United States Ship

V

VA	Department of Veterans Affairs
VANTS	Veterans Affairs Nationwide Teleconferencing System
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VTMWG	Vulnerabilities and Threat Modeling Working Group

W

WAN	Wide Area Network
WARN	Washington Area Radio Network
WG-P	Postal Working Group
WG-T	Telecommunications Working Group
WMO	Wireless Management Office
WPS	Wireless Priority Service Response Team

X

XCCDF	Extensible Configuration Checklist Description Format
XTE	Experimental Testbed Environment