Fiscal Year 2007 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 National Communications System (NCS) is approaching another milestone in its service to our country—its 45th anniversary on August 21, 2008. From the Cuban Missile Crisis and Cold War diplomacy to 21st century terrorism and the unpredictable manner of Mother Nature, the NCS continues to thrive as the leader in emergency communications solutions. In addition, the NCS continues its response to evolving technology advancements and changes in emergency preparedness operations. These changes define how the NCS accomplishes its mission to endure as a prominent leader in securing the Nation's communications systems.

During the past 18 months, three primary factors shaped the NCS mission. In the wake of the tragic 2005 hurricane season, the NCS reviewed and strengthened its essential communications coordinating efforts—specifically for the Federal Government emergency response and recovery events. Simultaneously, the NCS worked to realign itself within Government-based on policy changes from within the Department of Homeland Security and changes mandated by Congress in April 2007. These changes allow the NCS and DHS to better collaborate with other Federal, State and local organizations in advancing the Nation's national security and emergency preparedness (NS/EP) posture. Finally, as the convergence of wireless, wireline, and Internet protocol networks into the next generation network (NGN) reshapes the technology landscape, the NCS redefined the way it meets its NS/EP communications requirements. By meeting these and other challenges, the NCS strives to initiate and uphold innovative approaches to telecommunications response, recovery, and coordination through its unique industry/Government partnerships.

Emergency preparedness has been the core of the NCS mission, and the organization has undertaken a wide range of initiatives to ensure reliable commercial communications services for the Nation. We work to answer the needs of Federal, State, local and tribal governments, and critical first responders in the severest of situations affecting the American people. In the past year, the NCS initiated significant efforts to expand the National Response Plan's (NRP) Emergency Support Function 2 (ESF-2) communications capabilities regarding emergency communications. This included conducting a large-scale training exercise in New Orleans last June, and establishing regional communications coordinators who began daily interaction with State and local personnel in advance of the 2007 hurricane season. The NCS continues to provide support to the ESF-2 support team and capabilities, obtaining experience and resources from its departments and agencies, while implementing innovative solutions to assist in the NCS mission.

The NCS remains involved in revising the NRP in its transition to a National Response Framework (NRF)—specifically toward the emergency support function portions, but also in support of the plan's International Annex that aims to further promote the extensive international collaboration the NCS already fosters. In that vein, we continue our long-standing relationship with the North Atlantic Treaty Organization on civil emergency planning and critical infrastructure protection issues through the Civil Communications Planning Committee. Additionally, the Network Security Information Exchanges (NSIE)—comprised of government and industry communications experts—held a trilateral meeting in March 2007 involving NSIEs from the United Kingdom, Canada, and the Unites States. This forum resulted in broadening international collaboration on network security issues. The NCS' far-reaching international associations—such as the International Telecommunication Union—ensure the U.S. Government maintains a voice in the intercontinental NS/EP communications arena.

The NCS and its numerous industry partners finalized the Communications Sector Specific Plan (SSP), a vital annex to the National Infrastructure Protection Plan. Over the past year, the NCS led the Communications Sector Coordinating Council to initiate implementation of the much anticipated plan; created the SSP Implementation Working Group to define the current communications architecture; and developed an essential National Sector Risk Assessment methodology. The NCS also devoted significant resources to ensuring that critical priority communications services continue to function as the underlying networks of these programs evolve into the NGN. The demonstrated importance of continuity of communications services

for critical personnel encourages the NCS to persist in developing and advancing the Government's disaster response capabilities as technology evolves.

The Department of Homeland Security Appropriations Act of 2007 required several organizational modifications within the Department, the implementation of which has brought great change in the daily workings of the NCS. Among these transformations were the establishment of the National Protection and Programs Directorate (NPPD) – formerly the Preparedness Directorate—and the Office of Emergency Communications (OEC). The Department also renamed the Office of Cyber Security and Telecommunications to the Office of Cybersecurity and Communications (CS&C). CS&C aligned the NCS, the National Cyber Security Division, and the OEC under its scope. As a result of this large policy shift, the NCS reevaluated and expanded its partnerships with its CS&C colleagues, collaborating with them to more fully address emergency communications and cyber issues. Additionally, in an effort to increase effectiveness, the NCS conducted an examination of interagency groups, identifying how each operate and interact, and recommending collaboration improvements.

In this past fiscal year, the NCS, aided immeasurably by collaboration with NCS member agencies and industry partners, completed a broad range of advanced technological, operational, and policy activities. These accomplishments demonstrate the unwavering mission of the NCS and its staff to ensure the resilience of the Nation's critical communications systems. I am confident that through the perpetuation of its industry and Government partnerships, the NCS can continue to make truly impressive strides in NS/EP telecommunications preparation, response, recovery, and coordination procedures and capabilities as it approaches its 45th anniversary.

Robert D. Jamison
Manager

NCS Leadership

Mr. Gregory T. Garcia
Deputy Manager

Ms. Sallie McDonald
Deputy Manager and Director

Mr. Allen F. Woodhouse
Chief of Staff

Mr. Robert D. Jamison
Manager

Mr. Gary D. Amato
Chief, Technology and Programs Division

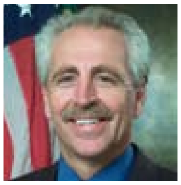
Mr. Jeffrey A. Glick
Chief, Critical Infrastructure Protection Division

Mr. James G. Bittner
Chief, Plans and Resources Division

Ms. Marilyn M. Witcher
Acting 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. John Grimes

Department of Justice (DOJ)
Mr. Kent Holgrewe

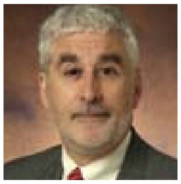
Department of the Interior (DOI)
Mr. Timothy Quinn

Department of Agriculture (USDA)
Ms. Janice Lilja

Department of Commerce (DOC)
Mr. Barry West

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

Department of Transportation (DOT)
Mr. Daniel G. Mintz



Department of Energy (DOE)
Mr. Carl S. Pavetto

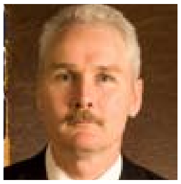
Department of Veterans Affairs (VA)
Mr. Robert T. Howard

Department of Homeland Security (DHS)
Mr. Scott Charbo

Office of the Director on National Intelligence (ODNI)
Mr. Dale W. Meyerrose

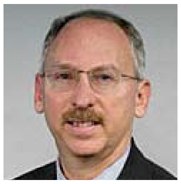
Federal Emergency Management Agency (FEMA)
Mr. Harvey E. Johnson

The Joint Staff (JS)
VADM Nancy Brown, USN



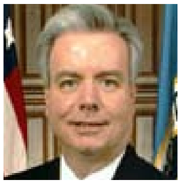
General Services Administration (GSA)
Mr. James Williams

National Aeronautics and Space Administration (NASA)
Ms. Betsy Edwards



Nuclear Regulatory Commission (NRC)
Mr. Roy Zimmerman

National Telecommunications and Information Administration (NTIA)
Mr. John Kneuer



National Security Agency (NSA)
Mr. Russell Flowers

Federal Reserve Board (FRB)
Mr. Kenneth Buckley

Federal Communications Commission (FCC)
Mr. Jeffrey Goldthrop

United States Postal Service (USPS)
Mr. Harold Stark

NCS Council of Representatives

Department of State (DOS)
Ms. Kimberly Godwin

Department of the Treasury (TREAS)
Ms. Vicki Waizenegger

Department of Defense (DOD)
Mr. Bill Gunnels

Department of the Interior (DOI)
Mr. Timothy Quinn

Department of Justice (DOJ)
Mr. Gary Laws

Department of Agriculture (USDA)
Mr. Roy Allums

Department of Commerce (DOC)
Mr. John McManus

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. Donald Sheehan

Department of Homeland Security (DHS)
Mr. Julio Murphy

Office of the Director on National Intelligence (ODNI)
Ms. Sherrill L. Nicely

Federal Emergency Management Agency (FEMA)
Mr. Rex Whiacre

The Joint Staff (JS)
LTC Susan Caromoda, USA

General Services Administration (GSA)
Mr. David Jarrell

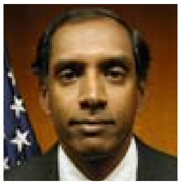
National Aeronautics and Space Administration (NASA)
Ms. Betsy Edwards

Nuclear Regulatory Commission (NRC)
Mr. Thomas Kardaras

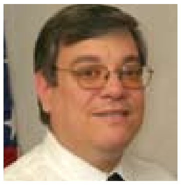
National Telecommunications and Information Administration (NTIA)
Mr. Stephen Veader

National Security Agency (NSA)
Mr. Anthony Cornish

Federal Reserve Board (FRB)
Mr. Wayne Pacine

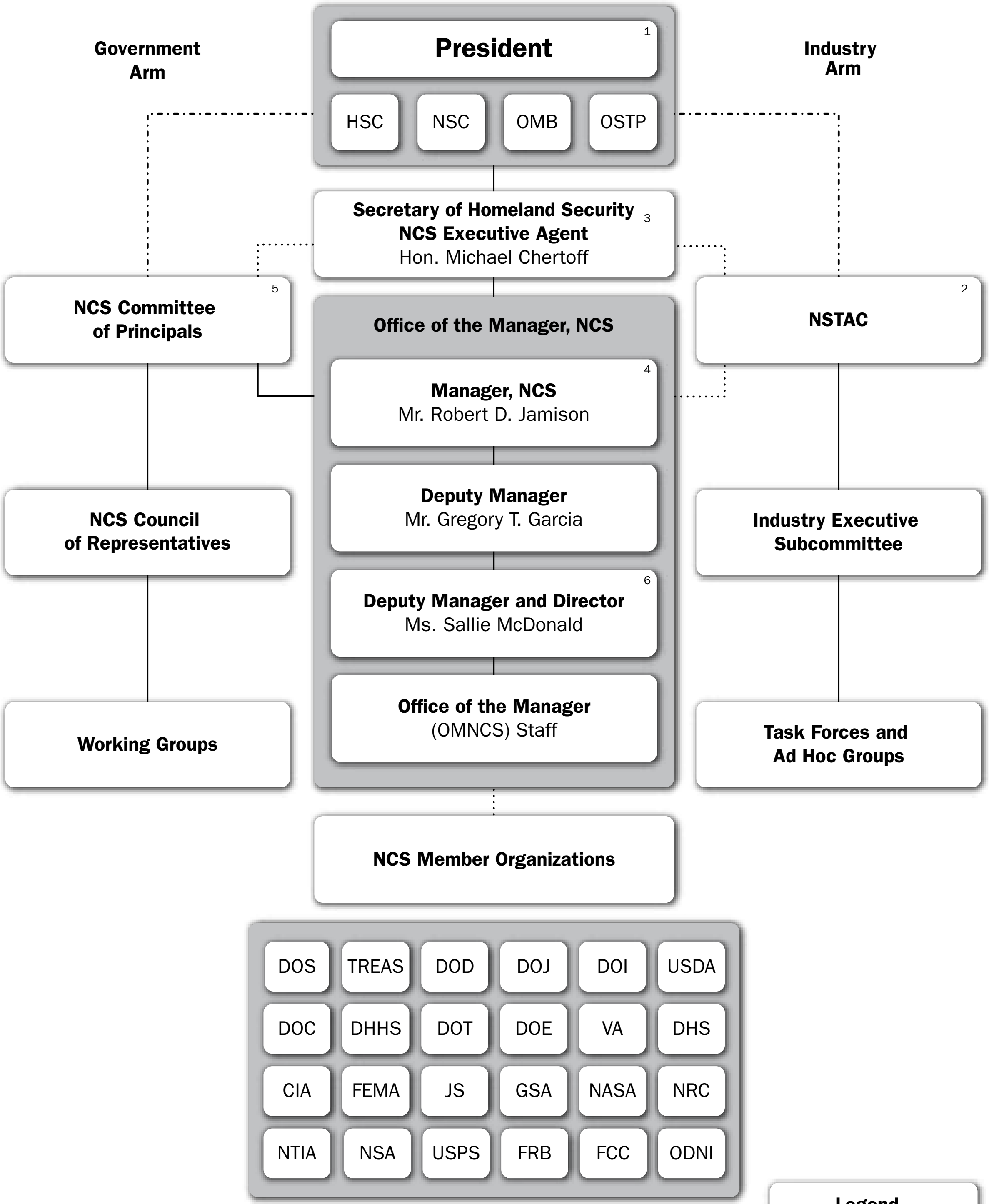


Federal Communications Commission (FCC)
Mr. Allan Manuel



United States Postal Service (USPS)
Mr. Warren Schwartz

The NCS Structure



Government Arm

Industry Arm

President [1]

HSC | NSC | OMB | OSTP

Secretary of Homeland Security [3]
NCS Executive Agent
Hon. Michael Chertoff

NCS Committee of Principals [5]

NSTAC [2]

Office of the Manager, NCS

Manager, NCS [4]
Mr. Robert D. Jamison

Deputy Manager
Mr. Gregory T. Garcia

Deputy Manager and Director [6]
Ms. Sallie McDonald

Office of the Manager (OMNCS) Staff

NCS Council of Representatives

Working Groups

Industry Executive Subcommittee

Task Forces and Ad Hoc Groups

NCS Member Organizations

DOS	TREAS	DOD	DOJ	DOI	USDA
DOC	DHHS	DOT	DOE	VA	DHS
CIA	FEMA	JS	GSA	NASA	NRC
NTIA	NSA	USPS	FRB	FCC	ODNI

Legend

Direction ———
Coordination ·········
Advice -·-·-·-

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

Introduction: The History of the National Communications System

Section I

Introduction: The History of the National Communications System

Background

This report, prepared by the Office of the Manager, National Communications System (OMNCS), describes national security and emergency preparedness (NS/EP) activities and telecommunications events, and highlights the agency's innovations, programs, and achievements during fiscal year (FY) 2007.

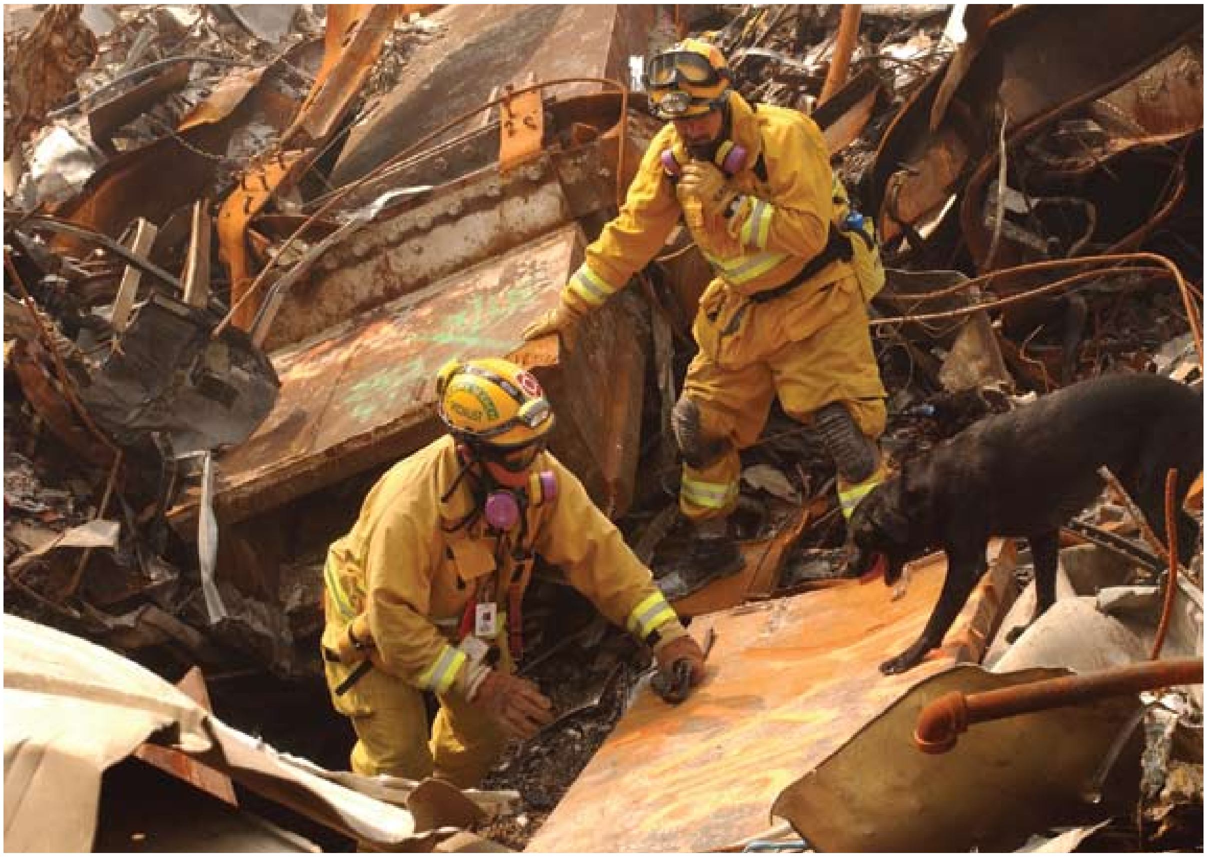
On July 11, 1963, President John F. Kennedy established the National Communications System (NCS) by way of National Security Action Memorandum 252. The mandate sought to remedy communications challenges encountered during the 1962 Cuban Missile Crisis, when key parties experienced difficulties in establishing and maintaining vital communications. The National Security Council (NSC) conducted a study in the wake of the crisis and recommended the creation of a consolidated system to support critical Government communications functions. As a result, the Presidential Memorandum directed that the 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."

Photo portrait of John F. Kennedy, President of the United States. (White House Press Office [WHPO])

Throughout its history, the mission of the NCS has steadily grown, keeping with the expanding role of telecommunications in supporting the Nation's NS/EP functions. Government policy in the late 1970s formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and recovery in the event of a nuclear attack. The expansion of the domestic telecommunications market through the divestiture of AT&T and the emergence of network technology capabilities greatly changed the national security communications landscape in the early 1980s, further complicating the means for satisfying NS/EP requirements.

In response 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 revitalized and 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. Additionally, the E.O. tasked the NCS to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

On September 11, 2001, the Nation experienced the most devastating terrorist attacks in United States history, forever altering the national threat landscape and demonstrating an immediate need for increased awareness and decisive action. In response, President George W. Bush issued E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, on October 8, 2001, establishing the Office of Homeland Security (OHS) and the Homeland Security Council. The E.O. tasked the OHS to coordinate protection efforts for critical public and privately owned information systems within the United States and authorized the OHS to coordinate efforts to ensure the rapid restoration of telecommunications and critical information systems



New York, NY, September 21, 2001—Mike Scott from the California Task Force-8 and his dog, Billy, search through the rubble for victims of the September 11 terrorist attack. (Photo by Andrea Booher/FEMA News Photo)

after disruption by a terrorist threat or attack. On October 16, 2001, President Bush issued E.O. 13231, *Critical Infrastructure Protection*, establishing the President's Critical Infrastructure Protection (CIP) Board and re-established the NCS' COP as a permanent standing committee with additional reporting requirements to the new CIP Board.

Still looking to further shift Government focus to the homeland security arena, President Bush signed into law the *Homeland Security Act of 2002*, on November 25, 2002, signaling the largest Government reorganization in 50 years. The Act established the Department of Homeland Security (DHS) and initiated a major restructuring 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 DHS on March 1, 2003. The NCS was originally aligned under the Information Analysis and Infrastructure Protection Directorate but later transitioned under the Office of Cyber Security and Telecommunications within the Department's Preparedness Directorate in 2005. Subsequently, *the Department of Homeland Security Appropriations Act of 2007* included several provisions requiring DHS organizational change, which included the establishment of the National Protection and Programs Directorate (NPPD) and the renaming of the Office of Cyber Security and Telecommunications as the Office of Cyber Security and Communications (CS&C). In response, the NCS was aligned under CS&C within NPPD.

NCS Environment

The NCS continued to face a dynamically-evolving homeland security policy and technology landscape in FY 2007. Significant developments in continuity communications policy drove the mission and activities of the NCS and its partners. Assured continuity communications are critical for Federal departments and agencies to effectively interoperate and perform their missions under all circumstances. In addition to the release of several important pieces

of policy aimed at continuity communications, the NCS focused its efforts on enhancing emergency response communications, working with industry partners on emerging NS/EP communications issues, and adapting to evolving technologies.

On April 1, 2007, *The Department of Homeland Security Appropriations Act of* 2007 brought together the NCS, National Cyber Security Division, and the newly created Office of Emergency Communications (OEC) under the Office of CS&C. From its inception, the OEC has worked closely with the NCS as the new agency organizes disparate emergency communications programs. For instance, the NCS COP, which provides advice and recommendations on NS/EP telecommunications to the Executive Office of the President, brought its resources to bear in support of the OEC's National Communications Baseline Assessment. Selected COP members, including the Department of Defense, Department of Health and Human Services, DHS, Department of the Interior, Department of Justice, Department of Transportation, Department of the Treasury, and the Federal Emergency Management Agency, played instrumental roles in identifying points of contact to provide data on their respective departments' and agencies' interoperable emergency communications capabilities.

Continuity Communications

On May 9, 2007, President George W. Bush signed National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy* (NSPD-51/HSPD-20), which directs U.S. Government departments and agencies to prepare continuity of operations plans that address man-made and natural threats and to allow them to initiate the plans with little or no notice. NSPD-51/HSPD-20 also directs the executive branch to provide critical communications and to ensure their availability and redundancy with the intention that key leaders remain connected.

Through FY 2007 and looking forward, the NCS remains actively engaged in a range of activities related to continuity communications efforts. In response to NSPD-51/HSPD-20, the NCS is developing a continuity communications architecture that will enable Federal Executive Branch departments and agencies to perform primary mission essential functions and national essential functions under all circumstances. In addition, on July 25, 2007, the EOP released NCS Directive 3-10, *Minimum Requirements for Continuity Capabilities*, which defines the minimum standards needed for execution of each department and agency mission in compliance with NSPD-51/HSPD-20. In a related effort, the NCS is currently drafting NCS Manual 3-10-1, *Guidance for the Implementation of NCSD 3-10: Minimum Requirements for Continuity Communications Capabilities*, to serve as a reference guide and adjunct to NCS Directive 3-10. Specifically, the manual will provide precise details concerning each level of essential communications within the Federal Government. These policy documents support the NCS' mission to establish more reliable and assured communications among agencies and between Governmental senior leadership.

In addition to these policy efforts to ensure continuity communications, the NCS, in conjunction with Department of Homeland Security's Under Secretary for the National Protection and Programs Directorate (NPPD), worked through the National Command and Coordinating Capability (NCCC) Management Coordination Office (MCO) to devise a capability to provide robust Presidential communications and information systems services to critical customers. In July 2007, the NCCC MCO devised an initial operational capability aimed at providing initial connectivity between the President and Federal department and agency principals, State governors, and associated operations centers at the State level.

President George W. Bush. (Photo by Eric Draper, White House)

Emergency Response

While the mission of the NCS continues to grow and evolve, it remains diligent in preparing for catastrophic natural events or man-made disasters. The National Coordinating Center (NCC) is currently revising the Emergency Support Function 2 (ESF-2) portion of the draft National Response Framework (NRF), which replaces the former National Response Plan. The NRF supports the continual development and enhancement of comprehensive, robust all-hazards emergency operations plans.

Continuing its efforts to promote advancement in emergency communications preparedness, planning, and response, the NCS hosted a two-week training session in New Orleans, Louisiana, last June in support of the NRF's ESF-2, Communications Annex. Representatives of Government agencies, local government, and industry are among the diverse array of leadership and response personnel who took part in the comprehensive training event. The training session provided a valuable opportunity for the NCS to reinforce its important partnerships with both its Federal Government and industry members. Representatives of each group participated in an exercise, received communications updates from a variety of briefers, and shared disaster communications experiences from Hurricane Katrina to help enhance continuity of communications and strengthen response efforts during the 2007 hurricane season.

Partnerships

The NCS continues to work closely with industry partners through entities such as the Communications Sector Coordinating Council (CSCC), the NCC, the Communications Information Sharing and Analysis Center, and the President's National Security Telecommunications Advisory Council (NSTAC). In May 2007, the NCS, industry partners, CSCC, and the Government Communications Coordinating Council (GCCC) finalized and published the Communications Sector-Specific Plan (SSP), per a requirement in the June 2006 *National Infrastructure Protection Plan*. The Communications SSP outlines the process for risk management in the communications sector, including infrastructure identification, risk assessments, protective programs, performance measurement, and research and development. The NCS worked with the CSCC and GCCC to implement the Communications SSP. These groups and the SSP Implementation Working Group defined the communications architecture and developed an essential National Sector Risk Assessment methodology.

Biloxi, Miss., September 3 and November 3, 2005—U.S. Highway 90 before (top) and after repair from damage caused by Hurricane Katrina. (Photo by Mark Wolfe/FEMA)

During FY 2007, the NCS fostered another partnership as it worked with the NSTAC to examine ongoing key issues to national security, including the evolution of the NCC; NS/EP implications associated with interdependencies between the telecommunications and electric power sectors; global infrastructure resiliency; and emergency communications and interoperability. Currently, the NCS and the White House are considering the NSTAC's recommendations in regards to these issues.

The NCS COP established the Communications Dependency on Electric Power Working Group in response to the recommendations in the *NSTAC Report to the President on Telecommunications and Electric Power Interdependencies*. In addition, in its final report, the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, expressed support for the NSTAC's recommendation to establish a national standard

for credentialing telecommunications repair workers. The panel also endorsed the NSTAC recommendation to designate telecommunications infrastructure providers as "emergency responders" under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* and the NRF. In a related effort, DHS is working to develop a set of access standards to ensure that private critical infrastructure responders receive priority access to disaster areas.

In addition to its collaboration with industry and Government entities, the NCS has also reached out to the international community through the Network Security Information Exchanges (NSIE). Specifically, the U.S. Government and the NSTAC NSIE recently held a trilateral information exchange with the British and Canadian NSIEs. The collective groups agreed to work more closely together in the future on international network security issues of concern related to next generation networks (NGN). These partnerships serve a valuable role in ensuring communications during response to emergency situations.

Technology

During the past fiscal year, the NCS also was intent on adapting to the ongoing advancement of technology. As a result of the evolution from wireline services to the NGN, the NCS created a priority service model group to perform predictive analysis and planning of the Government Emergency Telecommunications Service and Wireless Priority Service programs. This analysis and planning provides enhanced support to ensure that these critical programs function effectively in the event of a disaster.

In FY 2006, in an effort to mitigate risk to the telecommunications network caused by natural and man-made disasters, the NCS worked with the U.S. Departments of Energy, Health and Human Services, and Homeland Security to validate the route diversity methodology (RDM) through proof-of-concept assessments. In 2007, the NCS presented the assessment findings to the respective departments and agencies and incorporated the feedback into the final version of the RDM. The NCS also assisted in the enhancement of an Incident Management Team tool with real-time capability to better respond to requests generated from incidents of similar magnitudes to Hurricane Katrina.

In August 2007, the NCS and the Homeland Security Council conducted a study on the possible impacts of a pandemic influenza outbreak on communications networks. The study grew out of the May 2006 *National Strategy for Pandemic Influenza Implementation Plan's* identification of telecommuting as a key component of the national response to a pandemic influenza. An earlier study in November and December of 2005 identified potential congestion points for various types of telecommunication access and enterprise networks. The August 2007 study analyzed the current telecommuting strategy during a pandemic and provided recommendations of best practices for the general public and service providers to follow in the event of a pandemic outbreak. The best practices include suggested methods to support anticipated increase in telecommuting traffic and actions to help reduce potential congestion on residential access networks. Further, the NCS developed a model to analyze the relationship between a pandemic spread, network user behavior, and network performance, and concluded that the development of NGN priority services would help mitigate network congestion during a pandemic. However, the analysis concluded that the NCS and stakeholders (for example, representatives from major communications carriers, Internet service providers, and the financial community) may need to continue to research and assess cybersecurity standards to determine the need for additional protective measures.

As it has since its inception, the NCS actively strives to devise and present solutions for evolving policy, technology, and threat challenges that affect the homeland and national security telecommunications environment. The NCS maintains strong leadership in its partnerships with industry and the U.S. Government, providing stakeholders with the tools and preparedness to address the risks that challenge national security. As the homeland security environment experiences constant transformation, the NCS ventures to lead the collaborative mission of strengthened national communications continuity, emergency communications, and response.

Emergency Response Activities

Emergency Response Activities

Hurricane Season 2007

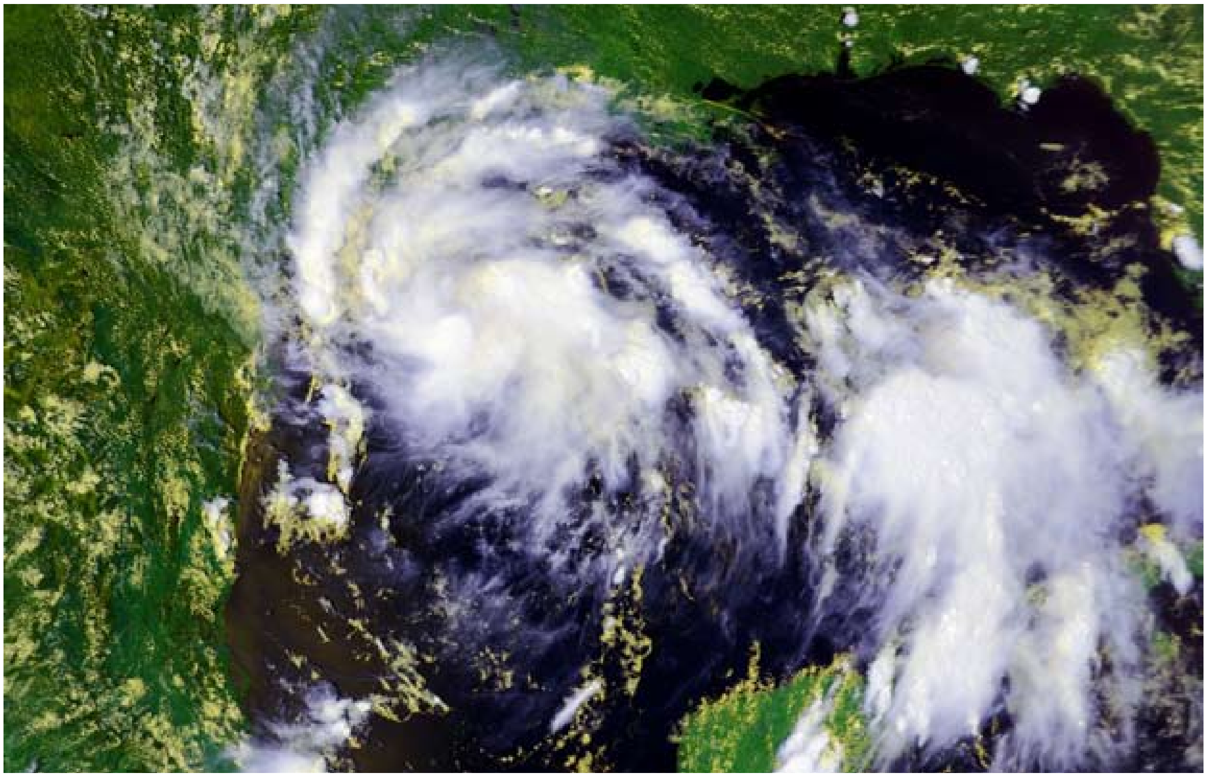
The 2007 Hurricane Season was fairly active with 18 storms in the Pacific and 14 in the Atlantic with two Category 5 hurricanes making landfall in Mexico. However, of the 14 storms in the Atlantic, only two hurricanes, one tropical storm, and one tropical depression threatened and/or made United States landfall. Although the Federal Emergency Management Agency (FEMA) activated Emergency Support Function 2 (ESF-2) only once—in preparation for Hurricane Dean, a Category 5 storm that struck the Yucatan Peninsula—there was no significant impact on communications assets this hurricane season. Despite the moderate level of activity, the National Coordinating Center (NCC) maintained a high alert posture throughout the hurricane season and monitored, analyzed, and assessed all approaching storms.

Hurricane Flossie

Flossie became a tropical storm on August 9 off the coast of Baja, California. As Flossie approached the Big Island of Hawaii, it intensified into a Category 4 storm on August 11. Fortunately, Hurricane Flossie maintained its southwestward track, passing just south of the Big Island, with no communications significantly impacted.

Throughout Flossie's track, the NCC participated in daily FEMA Leadership conference calls as a means of maintaining situational awareness, and held daily conference calls with industry and Government representatives to facilitate information sharing and coordinate pre and post landfall activities.

This FEMA video teleconference held August, 14, 2007 with the FEMA regional directors, state Emergency Operations Centers and Federal partners concerns Hurricane Flossie which is expected to pass just south of the island of Hawaii and Tropical Storm Dean which is building in the Atlantic and moving west toward the Caribbean Sea. FEMA's National Response and Coordination Center (NRCC) is activated at Level 2. (Photo by Bill Koplitz/FEMA)



Tropical Storm Erin on August 15 at approximately 1939 UTC. This image was produced from data from NOAA-18, provided by NOAA.

Tropical Storm Erin and Hurricane Dean

Erin made landfall as a tropical storm on August 16, near Lamar, Texas. At the same time, Hurricane Dean was slowly approaching the Caribbean, with early projections of a more northerly track towards the United States mainland. FEMA Regions II and VI stood up their respective Joint Field Offices and Emergency Response Teams-Advance deployed ESF-2 representatives to Denton and Austin, Texas, Puerto Rico and the U.S. Virgin Islands.

For Dean, the NCS provided two 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 NCC participated in daily FEMA Leadership conference calls as a means to maintain situational awareness, and held conference calls with industry and Government representatives to facilitate information sharing and coordinate response activities.

Hurricane Dean maintained is southwesterly track and struck the Yucatan Peninsula as a Category 5 hurricane on August 13. Tropical Storm Erin impacted the Texas mainland and parts of Oklahoma with heavy rains and flooding; however, there were no impacts on the telecommunications infrastructure.

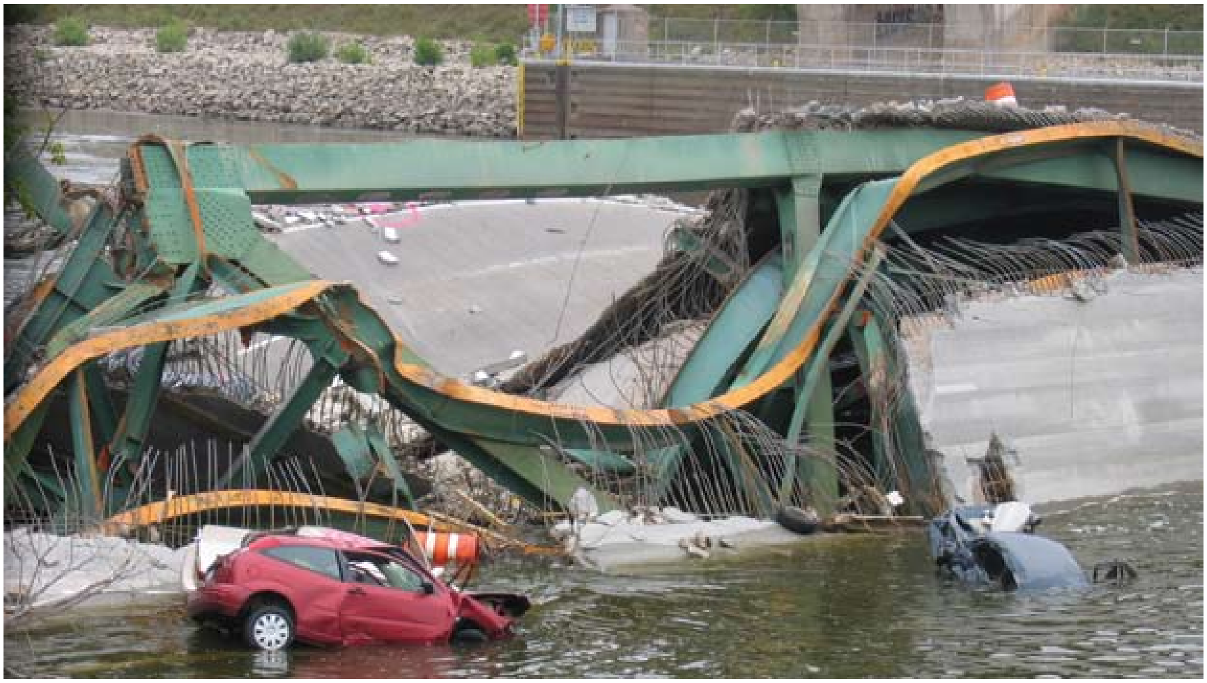
Hurricane Humberto

Humberto made landfall on September 13 as a Category 1 hurricane, just east of High Island, Texas. For several days, Tropical Storm Humberto traveled through the Gulf Coast, intensified into hurricane status, and made landfall on the same day. Downgraded to a tropical depression, it dumped heavy rains onto parts of Louisiana before dissipating over Mississippi.

The telecommunications infrastructure suffered no significant impact. However, heavy rains and wind gusts caused damage in the millions of dollars, and officials reported one fatality.

Tropical Depression Ten

Tropical Depression Ten made landfall on September 21, near Fort Walton Beach, Florida. Winds never exceeded 35 mph and quickly dissipated shortly thereafter over Florida. Again, there were no reported impacts to the telecommunications infrastructure.



Cars and roadway litter the river where the I-35 bridge collapsed in Minneapolis on August, 5, 2007. (Photo by Todd Swain/FEMA)

Other Events

Notwithstanding a relatively active hurricane season, the NCS also supported response efforts for a number of other events. Specifically, the NCC Watch performed infrastructure analyses to determine the impact to telecommunications assets for the following events:

- Ice Storms—Midwest/Northeast United States, January 16
- Tornado—Lady Lake, Florida, February 2
- Super Bowl XLI, February 4
- Chemical Plant Explosion—Kansas City, Missouri, February 7
- Enterprise HS Tornado, damage to Coffee and Wilcox counties, Alabama, March 1
- Subtropical Storm Andrea, May 9
- Flooding in Kansas and Missouri (Region VII ESF-2 Activation) July 4
- Interstate 35W Bridge Collapse in Minneapolis, Minnesota, August 1
- California earthquake, north of Los Angeles, August 8

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 2007. 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.

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) 2007.

National Communications System Organization and Leadership Changes

FY 2007 saw some major changes in the National Communications System (NCS)—in terms of leadership, membership and in its relationships within the Department of Homeland Security (DHS).

On January 8, 2007, the first changes occurred when Sallie McDonald became Deputy Manager and Director of the NCS, replacing Dr. Peter M. Fonash. Ms. McDonald, who had been with the Department when it first was formed in 2003, became the NCS director after returning from a one year fellowship at George Mason University's School of Law, working on a Critical Infrastructure Research Program. Dr. Fonash, who had been the NCS Deputy Manager and Director since July 2004, became the Chief Technology Officer for the Department's Cyber Security and Telecommunications (CS&T) Branch.

That same day, Air Force Colonel Victoria Velez–the NCS Chief of Staff–was named by DHS Assistant Secretary Greg Garcia as the acting chief of the newly designated Office of Emergency Communications (OEC)–an organization that would officially join the Department in April 2007. With the transfer of Colonel Velez to OEC, Thomas J. Falvey, Chief of the NCS Customer Service Division, added the NCS Chief of Staff duties to his responsibilities.

In April 2007, the DHS restructured in compliance with congressional legislation. The reorganization transferred some Preparedness Directorate programs to the Federal Emergency Management Agency. With those changes, the Preparedness Directorate was renamed as the National Protection and Programs Directorate (NPPD), with George W. Foresman, the DHS' Undersecretary for Preparedness and NCS Manager, as its leader. That same legislation changed the title of CS&T to Cyber Security and Communications (CS&C), and formally activated the OEC.

Soon after, Mr. Foresman submitted his resignation to DHS Secretary Michael Chertoff and formally left the Department in May 2007. Robert D. Jamison, assumed duties as the NCS Manager while serving as the Acting Under Secretary for NPPD. During that same period, Robert S. Zitz, the NCS Principal Deputy Manager and Deputy Under Secretary to Mr. Foresman, moved to another organization within the Department.

In July, Mr. Falvey retired from Federal service. Marilyn M. Witcher, Chief of the NCS Industry, Government and External Affairs Branch, assumed duties as the Acting NCS Customer Service Division chief.

Just before the end of the fiscal year, the White House announced that the Office of the Director of National Intelligence would become the 24th member of the National Communications System. Shortly after that announcement, Ms. McDonald announced that Allen F. Woodhouse would become the NCS Chief of Staff, filling the position vacated by Mr. Falvey in July.

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 that recommendations incorporate NS/EP requirements.

The following pages highlight the major projects undertaken by the Technology and Programs Division during FY 2007.

Emergency Telecommunications Services

Government Emergency Telecommunications Service (GETS)

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 ubiquitous, robust, and flexible PSTN, which supports more than 90 percent of the Government's telecommunications needs.

The first objective of GETS planners was to expeditiously field a service that would provide priority call treatment, and incrementally improve the service 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 initial GETS implementation approach focused on the interexchange carrier (IXC) portion of the network. This was accomplished by separate sole-source GETS contracts with AT&T, MCI (now Verizon Business), and Sprint Nextel, the three largest IXCs and, currently, the only IXCs that can authenticate and process GETS calls. As such, access to these carriers must be available at all PSTN end offices as described in the Lockheed Martin planning letter for handling NPA 710 calls.[1] 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 an 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 NS/EP call access by automatically attempting all three GETS IXCs.

The GETS integration contractor (IC) entered into contracts with four primary switch manufacturers (Lucent Technologies, Nortel Networks, AG Communications Systems [AGCS], and Siemens) for the implementation of priority treatment and enhanced routing features. The GETS IC also contracted with LECs to deploy and operate these features. These entities deploy GETS features on additional switches during software release upgrades or as additional LECs come under contract. In addition, as industry upgrades their 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.

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the NCS worked to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks. In 1993, the American National Standards Institute (ANSI) approved the High Probability of Completion Standard ANSI T1.631-1993, which provided a class mark for NS/EP-related signaling messages. ANSI reaffirmed this standard in December 1999 and revised it in 2005 (now ATIS-PP-1000631.2005) to clarify domestic and international gateway exchange requirements. The classmark allows NS/EP call identification in any U.S. network, facilitating the application of available GETS features.

ANSI modified the SS7 standards so that emergency (NS/EP and 911) traffic would have a higher signaling priority level than regular or non-priority telephone traffic. The GETS Program Management Office worked closely with the Alliance for Telecommunication Industry Solutions (ATIS) 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, subsequently 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.

Functional Description

To access GETS, users dial the universal access number (710-NCS-GETS) using common telephone equipment, such as a standard desk set, payphone, secure telephone, 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 GETS personal identification number (PIN). 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 PSTN calls. The utility of this feature was most notable during the September 11, 2001, attacks on America and again during the hurricane seasons of 2004 and 2005.

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 their on-net GETS calls and priority access to the PSTN for off-net GETS calls.

GETS Benefits to the NS/EP Community

For NS/EP users, GETS is a significant emergency communications asset that has proven to be effective during natural and man-made disasters. GETS was one of the first communications services used following the terrorist attacks of September 11, 2001. Despite the heavy telephone congestion, 95 percent of the over 10,000 GETS calls attempted in or out of the New York City and Washington areas were successfully completed. From the date of the attack until September 28, 2001, the NCS issued over 1,000 GETS cards to emergency personnel.

In the hurricane season of 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, over 40,000 GETS calls originated or terminated in the affected areas and the NCS issued over 2,000 new GETS cards to support NS/EP activities.

FY 2007 Accomplishments and Improvements

In the past year, the GETS program continued 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 June 25, 2007, there were 160,015 active GETS cards–an increase of 28,259 cards since July 17, 2006.

GETS NS/EP Category	GETS NS/EP Users
Federal	86,087
State	17,103
Local	27,897
Industry	27,444
Other NS/EP organizations	1,484
Total	160,015

Table 1. GETS User Breakdown

Highlights and Status of Ongoing Activities

NCS continues to expand GETS capabilities in the PSTN and participate in activities that facilitate this:

- The GETS IC has worked with Hawaiian Telcom and Puerto Rico Telephone to provide GETS capabilities in their networks and is in discussions with Level 3 and XO Communications to investigate the possibility of implementing GETS capabilities in their networks, including migrating to next generation networks (NGN);

- To ensure NS/EP needs are met as the PSTN migrates to the NGN, the GETS IC contracted with Sonus Networks to maintain NS/EP call identification for calls between SS7 and IP networks traversing Sonus equipment; and

- The NCS continues to participate in the ATIS NIIF to promote NS/EP needs. The NCS worked with the ATIS NIIF to facilitate nationwide activation of the passing of the SS7 precedence parameter to carry Wireless Priority Service (WPS) information across landline networks.

Partnership Activities

Federal Departments and Agencies—The NCS coordinates with Executive Office of the President (EOP), including Homeland Security

Council, National Security Council, Office of Management and Budget, and Office of Science and Technology Policy to provide NS/EP priority telecommunications to the Federal Government.

In operating GETS, the NCS coordinates with the 24 Federal departments and agencies that comprise the NCS membership (*See http://www.ncs.gov for details*) as well as other departments and agencies as appropriate.

***State and Local Agencies and Organizations*—**
GETS users include State and local government organizations and officials supporting emergency preparedness and response.

***Private Sector*—**The NS/EP community supporting NS/EP mission requirements includes industry and non-government emergency response organizations plus industry owners and operators of critical infrastructures (such as, nuclear facilities, regional and national airports, ports, railroads). Further, GETS is a government/industry partnership dependent on the participation of the PSTN vendors and service providers. Current industry partners include: AT&T, Verizon Business, Sprint Nextel, Verizon, Embarq, Qwest, Cincinnati Bell, Nokia Siemens Networks, Time-Warner Telecom, Nortel, Sonus Networks, and Alcatel-Lucent.

***International*—**GETS serves components of the Departments of Defense and State, to include U.S. embassies, worldwide and supports the Federal Reserve Bank by providing GETS to international banking entities. GETS also serves strategic international allies of the United States, including Canada and the United Kingdom.

Wireless Priority Service (WPS)

Background

WPS is a nationwide wireless telephone service that interoperates with GETS and provides priority NS/EP telecommunications via selected commercial mobile radio service providers. 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.

WPS provides end-to-end nationwide wireless priority communication capabilities to key NS/EP personnel during natural or man-made disasters or emergencies that cause congestion or network outages in the commercial cellular telephony network. WPS is complementary to and most effective when used in conjunction with GETS to ensure a high probability of call completion in both the wireless and wireline portions of the public network.

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 has 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&O) [FCC-00-242, July 13, 2000] on wireless Priority Access Service (PAS). The R&O offers Federal liability relief to wireless carriers if they 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 events of September 11, 2001, 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.[2] Responding to this guidance, the NCS provided an off-the-shelf immediate WPS (I-WPS) solution, with limited capabilities in place for the February 2002 Winter Olympics in Salt Lake City. I-WPS was operational by May 2002 in the District of Columbia and New York City; by December of that year, the NCS achieved nationwide WPS capabilities.

NS/EP users are currently able to subscribe to WPS in nearly all the major wireless markets in the continental U.S. (AT&T, Sprint Nextel, T-Mobile, and Verizon Wireless) and in U.S. territories served by these nationwide carriers. In addition, the NCS is working with regional carriers to expand the coverage areas available to NS/EP users to increase the probability of NS/EP calls receiving full end-to-end priority treatment from geographically remote or sparsely populated areas.

Functional Description

WPS is a subscription-based service that enables a properly authorized and enrolled NS/EP user to invoke WPS on a per-call basis. Unlike GETS (which uses PIN based authentication), WPS uses a *272 feature code prefix plus the destination number to originate a WPS call.

If all radio channels in the user's cell [sector] are busy, the user's call will be queued for access to the next available radio channel in accordance with the users' assigned priority and time of call origination. Furthermore, WPS provides queuing to congested PSTN interfaces for calls originated at a mobile switching center (MSC) and traversing another carrier's network. Regardless of whether a WPS call traverses the PSTN or simply connects within the same MSC, queuing is also applied when terminating a WPS call into a cell where all radio channels are busy. WPS and GETS integration provides an end-to-end priority treatment for NS/EP calls, including calls that originate, transit, and/or terminate in wireless and/or landline networks.

WPS provides priority for radio access, transport, and radio egress to commercial cellular networks. Similar to GETS, WPS is in a constant state of readiness to maximize the use of all available communications resources should outages or congestion occur during an emergency or crisis. WPS serves NS/EP needs while minimizing impact on the general public access to the public wireless infrastructure. WPS priority functionality in the commercial cellular networks includes priority-based radio access queuing, trunk queuing, priority based radio egress queuing, enhanced routing schemes, transmission of the precedence parameter when configured, border cell call delivery, ANSI-41 enhancements (Code Division Multiple Access [CDMA] only), and Transaction Capabilities Application Part messaging priority.

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 CDMA. WPS GSM rollout is complete, with service provided by major GSM carriers AT&T Wireless (formerly Cingular Wireless), T-Mobile, and Sprint Nextel (GSM). Sprint Nextel (GSM) uses GSM switching technology coupled with proprietary Integrated Digital Enhanced Network air interface technology. In addition, two regional GSM carriers, SouthernLINC and Edge Wireless, provide WPS in their service areas. Verizon Wireless and Sprint Nextel (CDMA) use CDMA technology.

Wireless standards and Industry Requirements (IR) documents jointly developed by industry and Government form the basis for WPS. The active

and cooperative participation of all stakeholders, including major wireless equipment vendors and service providers, successfully produced these IR documents in February 2002, only four months after NSC directed. The FOC requirements for both GSM and CDMA are complete. In addition to establishing engineering requirements, these documents formed the 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, a reasonable amount of capacity is always available for public use.

WPS Benefits to the NS/EP Community

WPS is a significant emergency communications asset that has proven to be effective for the NS/EP community. During the hurricane season of 2005, WPS assisted NS/EP emergency response and recovery communications along the Gulf Coast region. Following Hurricane Katrina in August 2005, the NCS activated 2,500 new WPS users. Of the more than 5,000 WPS calls attempted into and out of the affected regions during Hurricanes Katrina, Rita, and Wilma, 95 percent gained access to the radio channel and 63 percent were completed. In addition, following the tornadoes during March 2007, WPS benefited rescue workers and volunteers converging on the town of Enterprise, Alabama, when wireless networks were jammed.

FY 2007 Accomplishments and Improvements

In the past year, the WPS program continued to make significant progress in its outreach efforts to all levels of government and other qualified NS/EP industrial and non-profit organizations. As of June 25, 2007, there were 45,525 authorized WPS users-a 31 percent increase since July 17, 2006.

WPS NS/EP Category	WPS NS/EP Users
Federal	33,227
State	1,574
Local	4,499
Industry	6,213
Other NS/EP organizations	12
Total	45,525

Table 2. WPS User Breakdown

Additional WPS accomplishments during FY 2007 include:

- Adding Sprint Nextel as a WPS CDMA carrier;
- Completing deployment of the next phased WPS CDMA enhancement in the Verizon Wireless network;
- Commencing development of the WPS CDMA Nortel/Motorola Interoperability Specification (IOS);
- Initiating discussions with leading service providers of satellite-cellular telecommunications networks to investigate the need for and the feasibility of WPS over satellite in response to the growing dependence on satellite mobile telephones by NS/EP personnel; and
- Working with industry to ensure completion of all laboratory and live network testing to achieve successful nationwide activation of the precedence parameter by December 31, 2006.

Highlights and Status of Ongoing Activities

There are two phases for WPS CDMA development. Alcatel-Lucent and Nortel completed their first phase of WPS MSC and base station subsystem product enhancements, and Nortel is developing Phase 2 in two sub-releases. Alcatel-Lucent and Nortel completed their Phase 2 and Phase 2A releases by December 2006; Nortel's Phase 2B is currently under development, with completion scheduled by the end of the first quarter of FY 2008. In addition, Alcatel-Lucent completed development of its WPS capability in its super distributed home location register.

The provision of WPS capabilities in the major CDMA carriers, Verizon Wireless and Sprint Nextel (CDMA), is well underway. In September 2006, Verizon Wireless completed deployment of WPS FOC Phase 1, which provides priority access to local radio channels when originating a WPS call. In May 2007, Verizon Wireless fully deployed the next phased WPS CDMA enhancement: trunk queuing and radio channel priority for terminating wireless calls. Sprint Nextel is on schedule to complete nationwide FOC implementation by the end of the first quarter of FY 2008. Budget constraints delayed Nortel/Motorola IOS development and testing for CDMA WPS, programmed for FY 2006, consequently delaying the WPS FOC. This affected WPS availability in approximately 20 percent of the

CDMA carrier markets[3] where Motorola's proprietary IOS software configuration is used. CDMA WPS IOS development began in 2007 and will complete by December 2008. 2009 is the target year for IOS network deployment and WPS FOC.

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.

Partnership Activities

Like GETS, WPS is coordinated with the EOP and serves NS/EP users within the Federal, State, and local governments and other qualified NS/EP organizations. The NS/EP community supporting NS/EP mission requirements includes industry and non-government emergency response organizations plus industry owners and operators of critical infrastructures (such as, nuclear facilities, regional and national airports, ports, railroads). Further, WPS is a government/industry partnership dependent on the participation of the mobile equipment vendors and service providers. Current WPS industry partners include: AT&T Wireless, Sprint Nextel, T-Mobile, Verizon Wireless, Hewlett-Packard, Alcatel-Lucent, Motorola, Ericsson, Nokia, Nortel, Qualcomm, and Siemens Networks.

NS/EP Priority Services in Next Generation Networks

Historically, NS/EP priority services such as GETS and WPS were specified, engineered, and implemented when the PSTN was based exclusively on circuit-switched technology. Today's PSTN is supplementing, and eventually replacing, circuit-switched equipment with the packet-based technologies that have supported IP data networks for some time. This migration to a packet-based technology dictates the evolution of GETS and WPS into the NGN. Using packet technology, NGN GETS will provide priority NS/EP communications not only for voice band service, but also for broadband applications (such as, video and data).

The NCS developed an NS/EP NGN reference architecture and continues to work with service providers and vendors to assure NS/EP requirements as they develop their individual architectures. The NCS is actively participating in standards development organizations and fora, coupling its industry liaisons and IR processes with initiatives to ensure that the appropriate standards include NS/EP NGN needs.

The NCS is partnering with wireline and wireless carriers, equipment vendors, cable providers, and other new NGN industry segments to define industry requirements for NS/EP voice services supported by the NGN core network. The schedule for the first phase of the IP Multimedia Subsystem (IMS) Core NS/EP IR is the end of 2007. Subsequent IR efforts will address requirements for other priority services (including, multimedia, web server access, and e-mail).

The NCS continues to participate in the activities of the MultiService Forum (MSF), including the Global MSF Interoperability testing event (GMI 2006), during which the NCS and industry partners demonstrated proof of concept priority capabilities that address NS/EP NGN needs. Priority features (such as, priority video teleconferencing, priority roaming, and several novel user-authorization methods) were demonstrated on a global scale using commercially-available NGN equipment. The NCS published two GMI2006-related papers: "Ensuring Emergency Calls on the Next Generation Network" in the February 2007 issue of the Armed Forces Communications and Electronics Association (AFCEA) journal, "Signal," and "Global Interoperability of Priority Telecommunications Services," presented at the 3rd International Conference on Security and Privacy in Communication Networks (IEEE SecureComm 2007).

The NCS will continue joint development of NS/EP solutions with industry partners, a highly successful approach proven during the development of the GETS and WPS programs. This ensures the provision of priority services to users with NS/EP mission requirements.

NS/EP Standards Development

Presidential Executive Order (E.O.) 12472 directs NCS consideration of evolving national and international standards with respect to NS/EP telecommunications, and Office of Management and Budget 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.

Emergency Telecommunications Services (ETS) includes ongoing standards development initiatives encompassing prime functionalities of: signaling, access, management, transport, interoperability, mobility, and their associated architectures, comprises.

Traditional NS/EP telecommunications services were designed 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, commercial standards stemming from technologies based on packet-switching, such as Internet Protocol (IP) based networks, will guide priority telecommunications services. Recognizing that IP and third generation 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. State Department by chairing the International Telecommunications Advisory Committee Study Group 'B' along with serving as senior Government advisors and leaders (such as, head of delegations) to a variety of international and national meetings on telecommunications. 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 (TIA);
- International Telecommunication Union, Telecommunications Standardization Sector (ITU-T);
- Internet Engineering Task Force (IETF);
- TeleManagement Forum;
- Third Generation Partnership Project (3GPP);
- Third Generation Partnership Project 2 (3GPP2); and
- Institute of Electrical and Electronic Engineers (IEEE).

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, 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 and associated application notes for IP-based services, to better specify criteria for availability, reliability and quality performance of delivered NS/EP telecommunication services.

Accomplishments in FY 2007 include:

- Alliance for Telecommunications Industry Solutions
  - ATIS-PP-1000010.2006: Standard for Support of ETS in IP Networks; and
  - ATIS-0100006: Service Restoration Priority Levels for IP Networks.
- ITU-T Standards Developments
  - (ITU-T SG 16) 2007 January, completed (1) New H.246 Amendment 1 "Mapping of user priority

level and country/international network of call origination between H.225 and ISUP" (Approved January 2007) (2) Revised ITU-T H.460.4 "Call priority designation and country/international network of call origination identification for H.323 priority calls" (Approved January 2007);

- (ITU-T SG2) 2007 February, completed development of E.107-(ETS) and Interconnection Framework for National Implementations of ETS (Approved February 2007);
- (ITU-T SG 11 & 2) 2007 April, continue development of signaling support for NGN NS/EP requirements. 2007 April, ITU-T Series Q Supplement 53, "Signaling Requirements to Support the International Emergency Preference Scheme (IEPS);"
- (ITU-T SG 11 & 2) 2006 April, "New Q.1950 Annex G for IEPS;"
- (ITU-T SG 13) 2007 April, Continued to develop (*i.e.*, progress for final approval in calendar year 2008) draft Recommendation Y.NGN-ET-TECH on NGN technical mechanisms for NGN emergency communications; and
- (ITU-T SG 9) 2007 June, progressed draft Recommendation J.pref on technical specifications to enable preferential (GETS like) communications in the current suite of Next Generation IP Cablecom networks that industry is now deploying.

▸ Internet Engineering Task Force Request For Comments (RFCs)

- Progressed three draft RFCs, dealing with the following technical topics, to last the stage of the IETF approval process:
  - Framework to Support ETS in a single domain (the final informational RFC of the IEPREP Working Group);
  - Extension to the TRIP Protocol (defines an attribute that identifies ETS capable gateways); and
  - Extension to the RSVP Protocol (defines a new policy element to identify ETS type reservations).

Modeling, Analysis and Technology Assessment

As directed by E.O. 12472, the NCS developed 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 (NDAC)

Due to the NS/EP community's heavy reliance on public networks, the Network Design and Analysis Capability (NDAC) was developed to analyze current U.S. networks and technologies, and to evaluate the need for additional capabilities. The NCS has invested over 20 years in establishing strong working relationships with commercial carriers and Government departments and agencies, and in developing modeling tool sets, methodologies, and unique databases that include proprietary data from the major carriers. The NDAC provides a comprehensive modeling and analysis capability and the ability to answer a wide variety of questions, such as: What impact would a pandemic flu have on the telecommunications infrastructure? What impact will the convergence of traditional circuit-switched networks with packet-switched/IP-based networks have on NS/EP requirements?

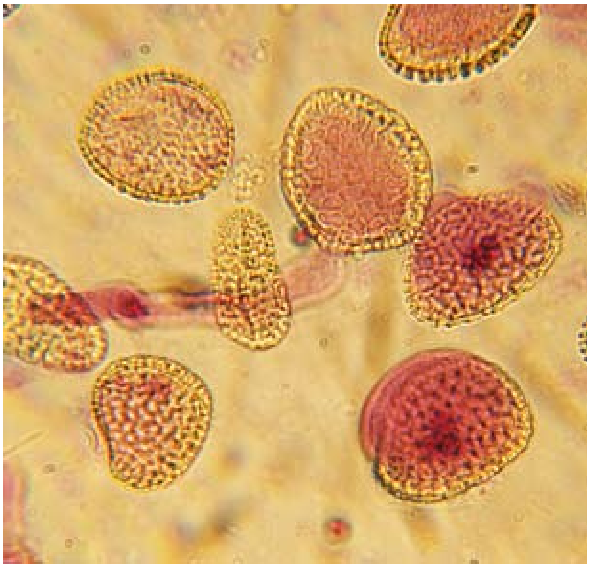
Pandemic Influenza Study

A pandemic influenza in the U.S. will likely have widespread impact on the economy including potentially up to a five percent drop in Gross Domestic Product. Several national pandemic plans, including those from Homeland Security Council, DHS, and Department of Health and Human Services, identify telecommuting as a key component of the national response to a pandemic. Telecommuting is a social distancing measure that can limit disease spread, while allowing businesses to continue to function.

Given the telecommuting strategy advocated in several national pandemic plans, the following questions remain:

▸ Will the telecommuting strategy work during a pandemic given the existing communications infrastructure?

- What preparations would better prepare for telecommuting during a pandemic?



The NCS conducted an initial assessment during November and December of 2005, identifying potential congestion points for various types of communications access and enterprise networks. After presenting the results of the initial study to the Financial and Banking Information Infrastructure Committee and Financial Services Sector Coordinating Council in July 2006, the NCS agreed to the financial community's request for a more detailed congestion analysis. In support of this effort, the NCS is working to:

- Provide analysis and recommendations on national telecommuting policy and business continuity planning for the pandemic influenza threat;
- Provide analysis and recommendations on potential enterprise level communications issues that may arise during a pandemic; and
- Identify ways to enable the telecommuting policy to succeed during a pandemic (best practices, policy mechanisms).

Risk Assessment Methodology

The NCS is partnering with industry to lead the National Sector Risk Assessment (NSRA) for communications in support of the Communications Sector Specific Plan (CSSP). Completed actions include:

- Co-led the development of the CSSP Implementation Working Group with industry; formed to address the risk milestones outlined in the CSSP;
- Coordinated several working group meetings to discuss the architectural framework and methodology for the NSRA;
- Outlined examples and working group starting points for threats, vulnerabilities, and consequences;
- Developed concepts for qualitative risk assessment methodologies that address threat, vulnerability, and consequence; and
- Cooperated with industry to develop and obtain working group agreement on a risk methodology framework.

In addition to NSRA-related efforts, the NCS has initiated work supporting future milestones for detailed risk assessments and cross-sector dependency analyses as outlined by the CSSP. A qualitative detailed risk assessment framework, including an example implementation of the framework, starts the development of a capability to identify:

- Consequences, vulnerabilities, and threats to the communications architecture;
- Architecture elements and functions that could be nationally critical based on HSPD-7 defined consequences;
- Specific assets related to an architecture element or function deemed to be at high risk; and
- Protective measures to mitigate risk.

The NCS has developed a process for responding to requests for support in identifying the communications dependencies of other organizations that includes leveraging existing NCS Technology and Programs Division tools and capabilities, like those on the Route Diversity Project. In support of cross-sector dependency analyses, the NCS conducted a high-level communications dependency analysis of the rail infrastructure to identify general dependencies that the rail industry has on the communications sector. A high-level dependency analyses apply to any sector.

Priority Services Modeling (PSM)

The convergence of the circuit-switched architecture of the PSTN with the packet-switched technologies of the Internet is changing the communications infrastructure which formed the basis for NCS programs and analyses. As the infrastructure changes, NDAC tools and methodologies must evolve to effectively analyze the implications of NS/EP services transitioning to these next generation network architectures. The NDAC PSM team must address multiple new questions introduced by the evolution of traditional GETS/WPS services to NGN architectures, including—

- Will these new architectures be able to support viable communications at 10x overload and with up to 70 percent infrastructure damage?
- How will industry's move toward IMS-based solutions affect the performance and reliability of current NS/EP services?
- How will the NGN provide priority e-mail, video teleconferencing, and other multimedia services?

The NDAC has responded to these new challenges by modeling the effectiveness of various priority service features—with respect to network and application performance—under various damage and congestion scenarios. The results of these modeling efforts have been—

- Incorporated into the GETS/WPS programs' IR process;
- Briefed at various CS&C conferences, such as the GETS Team Forum and the GFIRST Conference; and
- Submitted as a draft document to the IETF.

Given that service providers' technologies, architectures, and protocols are in a constant state of flux, the NDAC plans to continue its priority services modeling work throughout the upcoming year and produce modeling studies to aid the decision making process of the GETS and WPS programs. The results of these modeling studies will quantify the effectiveness of proposed priority service mechanisms and feed policy and budgetary decisions related to both the GETS and WPS programs.

Internet Analyses

Although the PSTN has long supported NS/EP communications, an increasing number of Government users are using services offered through the Internet; consequently, models of the logical and physical infrastructures of the Internet are now required to support NS/EP analyses. With the on-going NDAC expansion to include packet-switched networks, the NCS has developed an Internet modeling capability that captures physical and logical interdependencies between Internet Service Providers from both architectural and traffic perspectives. This capability determines the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure, and provides situational awareness information.

Committee for Foreign Investment in the U.S. (CFIUS)

The NCS is an active CFIUS participant, with specific objectives to manage the critical infrastructure risk caused by globalization of the telecommunications sector and respond to the unique policy challenges created as the United States continues to encourage foreign investment while balancing security priorities. This work involves conducting critical infrastructure analysis to identify key telecommunications assets and associated vulnerabilities, and providing technical and policy analyses to increase the level of transparency in commercial mergers and acquisitions.

Traffic Analysis of Critical Federal Telecommunications Infrastructures

The NCS has also developed an analysis tool that uses FTS2001 data to interactively view an agency's traffic inventory and perform critical infrastructure/sensitivity analysis on the impact to the traffic if a telecommunications facility is disabled. Critical

infrastructure analyses have been conducted for 11 NCS member agencies, including the General Services Administration, National Aeronautical and Space Administration, Department of Transportation, National Telecommunications and Information Administration, Department of Agriculture, Department of Health and Human Services, Nuclear Regulatory Commission, Department of State, Department of Energy, Department of the Interior, 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 has opted to use the NCS' demonstrated network modeling proficiency, tools, and data to support this effort.

Technology Assessment and Data Analysis Cell (TADAC)

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

- **Evaluate Contract Deliverables**—The TADAC provides a facility to evaluate the hardware and/or software deliverables of some contracts 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 & 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. Internet community projects provide an excellent opportunity to enhance our engineers' and computer scientists' expertise in critical areas and 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 eXperimental Testbed Environment (XTE), the Technology Assessment Network (TAN), and the classified Data Analysis Network (DAN).

eXperimental Testbed Environment (XTE)

The XTE provides the ability to emulate a scaled-down version of the Internet, converged network service provider networks, and enterprise networks. Operators simulate severe congestion on both the network and NGN end systems, and test and validate that emergency telecommunications services work properly from end-to-end using call load generators, traffic generators, and associated customized call processing systems. The XTE is a distributed test environment consisting of:

- Network devices (routers and switches) simulating an Internet Service Provider's backbone/core and access network;
- Security devices (authentication systems, firewalls, session border controllers, and intrusion detection capabilities) to protect network assets by enabling access control and by detecting and responding to simulated threats;
- Hosts and servers enabling the invocation and termination of NGN services and priority services;
- Test and analysis equipment to generate voice, video, and data traffic and to gather results of the effects of congestion on NGN services and service elements;
- VoIP telephones and systems to represent a VoIP service provider's service infrastructure; and

- Video endpoints and systems to access scaled-down IMS core NGN network service platforms with NS/EP functionality.

Technology Assessment Network (TAN)

The 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)

The DAN is a closed, classified network (for example, 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 (ATG)

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 NS/EP related communications concerns. The ATG supports multi-agency efforts to improve the national emergency communications infrastructure; the following paragraphs address support efforts in detail.

Telecommunication Electromagnetic Disruptive Effects (TEDE)

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 EMP technical data and studies concerning telecommunications. The NCS, specifically the ATG, coordinates and approves these tests and studies. The NCS looks across the electromagnetic spectrum to consider not only EMP, but all telecommunications disruptive effects. The NCS defines TEDE as encompassing 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 studies in the following topical areas:

- Susceptibility of the telecommunications infrastructure to EMP;
- Approaches to telecommunications systems protection from TEDE;
- Hardening essential communications systems, continued surveillance, and maintenance;
- Protection for new communications technologies and systems; and
- Affordability of EMP protection.

TEDE susceptibility tests of the telecommunications infrastructure include:

- PSTN switching systems and infrastructure;
- Terrestrial/satellite transmission and power systems;
- Equipment level tests and network level modeling;
- Partnered with Congressional "Live Fire" high power microwave vulnerability tests of SCADA systems, PSTN switching systems, local area networks and computer systems;
- Disruption of fiber-optic telecommunication links due to secondary effects associated with high energy illumination;
- Internet systems vulnerability tests; and
- Aviation Transportation communications systems vulnerability tests.

During DHS/NCS participation in the work of the Congressional EMP Commission, the ATG made legacy TEDE studies available and provided several briefings of current efforts, focusing on vulnerabilities to the telecommunications infrastructure.

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.

Emergency Communications

DHS/NCS evaluated the ability of satellite communications systems to supplement NS/EP related terrestrial systems and provided reports of the findings to the President's National Security Advisory Committee (NSTAC).

DHS/NCS participated in the NSTAC's Telecommunications and Electric Power Interdependency study, providing technical expertise on the effects of MHD, EMP-E1, E2 and E3 electromagnetic insults on the power grid and its control systems.

Evolving Technologies Studies

The ATG prepared and launched an extended area communications proof of concept to demonstrate the ability to provide a rapidly deployable extended communications capability. This capability is targeted towards emergency responders supporting disasters such as hurricanes, forest fires in areas where infrastructure does not exist to support communications or where the telecommunications infrastructure (both private service provider and public wired and wireless networks) have been rendered inoperable. The focus of this first phase was to evaluate existing communications technologies matched to aerostats architectures in an effort of providing deployable, rapid recovery, emergency response communications to first responders. This included assessing devices such as the police and fireman handheld radios, cellular instruments, citizens band radios, civilian ham radios and technologies which could improve coverage, service availability and interoperability between communications systems.

ATG continues to support management as the subject matter experts in sudden advanced technologies issues related to communications including but not limited to satellite, wireless and landline networks.

Warning Alert Response Network (WARN) Act

Section 603 of the Warning, Alert and Response Network Act (WARN Act), enacted on October 13, 2006, requires that the FCC develop recommendations on technical standards and protocols to facilitate the ability of commercial mobile service (CMS) providers to voluntarily transmit emergency alerts to their subscribers. In support of this effort the FCC Formed the Commercial Mobile Services Alert Advisory Committee (CMSAAC) to oversee the development of the recommendations. Pursuant to Section 603(c) of the WARN Act, the Committee is developing recommendations for the FCC in the following areas: protocols and technical capabilities and procedures; technical standards for priority alert transmission, technical standards for priority alert transmissions, technical standards for device equipment; and technologies and alert to non-English speakers.

The ATG is participating in the work of the CMSAAC and is a serving as a voting member of the Alert Gateway Group (AGG), an Informal working group of the CMSAAC. The primary mission of the AGG is to develop and submit recommendations for protocols, technical capabilities, and technical procedures through which CMS providers:

- Receive, verify, and transmit alerts to subscribers;
- Develop technical standards for priority transmission of alerts by CMS providers to subscribers; and
- Support the development of recommendations under which CMS providers may offer subscribers the capability of preventing the subscriber's device from receiving emergency alerts other than an alert issued by the President.

The ATG is assisting in the development of the Alert Gateway requirements through attending monthly meetings of the AGG and by participating in bi-weekly AGG requirement development meetings of the AGG technical subgroup, who is responsible for drafting Alert Gateway requirements for incorporating into the CMSAAC WARN Act requirements recommendations document for submission to the FCC in October 2007.

Transformational Communications Architecture (TCA)

The ATG is supporting the development of the DHS contribution to the As-Is, To-Be, and Should-Be Transformational Communications Architecture (TCA). The "As Is" architecture for TCA v3.0 is 2007-2008; the "To Be" Architecture is from 2008 to 2020; and the "Should Be" Architecture is 2020+.

The TCA is a space transport-level architecture that works in concert with the Global Information Grid (GIG) to help synchronize multiple acquisitions; to promote standards and interoperability; to deliver time-phased capability in an evolutionary approach; and to support information architecture concepts that enable critical information sharing needs. The TCA involves SATCOM satellites of the Department of Defense (DOD), Intelligence Community (IC), and National Aeronautics and Space Administration (NASA), DHS, and leased commercial MSS and FSS services; SATCOM Terminals; Terrestrial Infrastructure (Teleports and Gateways); and Network Management and Information Assurance to control the space assets and entry into the ground infrastructure.

The TCA attempts to break the stovepipe mentality by jointly focusing on DOD, IC, DHS, Commercial and Civil satellite and terrestrial communications development in a synchronized fashion, so that fielded systems and equipment materialize when a needed capability is intended to be fielded. NCS-N2 ATG represents the DHS in providing input to the Transformational Communications architecture, v3.0. The National Security Space Office Communications spearheads the TCA effort.

NSTAC Telecommunications and Electric Power Interdependencies Task Force (TEPITF)

The ATG participated in the NSTAC effort to address issues created by the increasing interdependencies between the North American telecommunications and electric power sectors from a long-term perspective. The ATG participated in the work of the TEPITF whose primary focus was on the technological and engineering challenges and issues related to long-term outage interdependencies.

In December 2006, NSTAC published its report to the President on "Telecommunications and Electric Power Interdependencies, The Implication of Long-Term Outages."

Looking Ahead

The ATG plans to continue TEDE vulnerability assessments of next generation networks and track, evaluate, and advise management of ongoing changes to satellite communications with the advent of but not limited to Ancillary Terrestrial Component technologies and industry implementation plans that would effect NS/EP communications. ATG will continue to participate or lead in Federal Government efforts to improve NS/EP communications.

Continuity Communications Working Group (CCWG)

Background

In 2004, the Enduring Constitutional Government Coordinating Council identified a need for a Continuity Communications Architecture (CCA) and the Office of Science and Technology Policy (OSTP) tasked the NCS with its development, based on assigned responsibilities under E.O. 12472. Constituted under the NCS Committee of Principals (COP), the CCWG addresses stove-piped systems and the lack of interoperability between Federal Executive Branch (FEB) departments and agencies in their continuity communications infrastructure.[4] 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."[5] 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 (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 FEMA serving as co-chairs. The Office of the Manager, NCS, 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 CCA PO 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 Department of State and DHS, initiated.

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

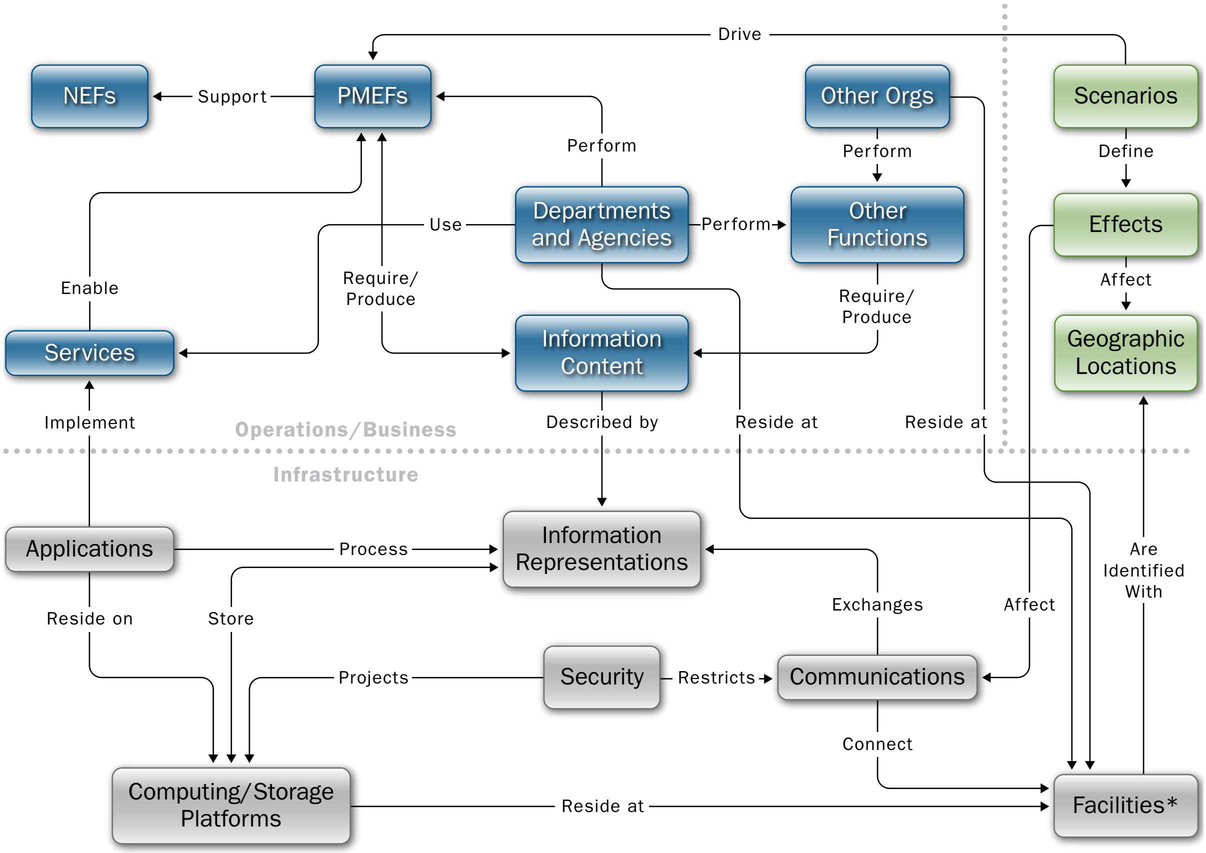


Figure 1. Continuity Communications Architecture Metamodel

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 CCA PO used the five FEA reference models as defined by the Office of Management and Budget OMB).[6] The performance reference model (PRM) can be tied to the PMEFs and NEFs to identify required performance measures enabling continuity. The business reference model (BRM) 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 (DRM) is used to map the departments and agencies' information requirements with specific formats. The service component (SRM) and technical (TRM) reference models provide examples of operational services, applications, information representations, and communications capabilities that they use in performing their PMEFs.

Another accomplishment of the CCA PO 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.

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

The CIP Division is organized around its operational role in preparing for and responding to incidents that impact NS/EP communications. After the devastating 2005 hurricane season, the Division was re-organized to include the following branches:

- **Operations Branch**—Coordinates and manages emergency response, operations and information sharing activities among the communications industry, government and international partners
- **Contingency Planning (CP) Branch**—Develops and implements emergency response doctrines and operational plans
- **Operational Analysis (OA) Branch**—Provides near real-time analytical assessments of the communications infrastructure
- **Training and Exercise (TE) Branch**—Develops a cadre of fully knowledgeable and skilled emergency response personnel

New Initiatives

The CIP Division has expanded the scope of its training program, holding its largest ever spring training conference in New Orleans, June 2007 for its nationwide, interagency team of communications responders. This conference included a 9-day, full scale exercise combined with extensive classroom training, field trips to emergency operations centers and facilities, and vendor demonstrations of communications equipment. The conference prepared over 150 team members with the knowledge, skills, and abilities necessary to ensure effective communications-related coordination, assessments, provision, and restoration during an incident.

Post-Katrina lessons learned revealed the necessity for a forward-deployed, permanent, regional presence for the NCS. As such the NCS proposed establishing a cadre of personnel to assist with regional communications coordination. The intent was to place two individuals at each Federal region. These positions, Regional Communications Coordinator (RCC) and Deputy Regional Communications Coordinator, would report to the CP Branch Chief but reside at the FEMA Regional Offices. As a proof of concept, contractor positions were established to fulfill the RCC roles in the three locations where significant activity was anticipated: Region IV,

US Coast Guard (USCG) Petty Officer Second Class (PO2) Shawn Beaty scans the horizon looking for survivors form the crew door his HH-60 Jayhawk helicopter during a search and rescue mission over the city in New Orleans, Louisiana (LA), during Hurricane Katrina relief operations. (DoD photo by PO2 NYXOLYNO CANGEMI)

Region VI and Region VIII/U.S. Northern Command (NORTHCOM). Additionally, NCS continued to refine the makeup of the Emergency Communications Teams (ECT) and began incorporating the new roles and responsibilities regarding "tactical communications."

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 National Coordinating Center for Telecommunications, the Communications Information Sharing and Analysis Center (ISAC), and several operational programs.

National Coordinating Center for Telecommunications (NCC)

The NCC, an industry-government collaborative body, is the primary mechanism within the NCS for fulfilling its emergency response role. The NCC's mission is "to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications service or facilities under all conditions, crises or emergencies." NCC membership includes over 40 industry participants and 24 Federal government agencies. This allows both public and private industry to work in close proximity to one another and ensures the success of the NCC's mission.

The operational arm of the NCC is its 24X7 watch and analysis center. Senior level information assurance analysts are located on site at the NCC Watch, which is the focal point for NCS emergency response and restoration 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 with situational awareness of their communication systems status in the disaster area.

Major NCC Activities in 2007:

- Throughout the 2007 hurricane season, the NCC actively tracked, analyzed, and assessed approaching storms to include Hurricanes Dean, Felix, Flossie, Humberto, Ingrid, and Tropical Storm Erin and Tropical Depression Ten. Hurricane Humberto was the only hurricane that made U.S. landfall in 2007 as a Category 1 storm, with little to no impact on the telecommunications infrastructure.

- Conducted conference calls with NCS Industry and Government partners, and communicated pre and post landfall staging/response activities in coordination with ESF-2 partners, field office components, and Industry liaisons.

- Maintained situational awareness by identifying assets and communication status for areas impacted by Hurricanes Flossie and Humberto, Tropical Storm Erin, Tropical Depression Ten, and the I-35W Bridge Collapse in Minneapolis, MN.

- Participated in two National Level Exercises to include Ardent Sentry 2007, and PINNACLE 2007.

- Participated in the *National Symposium on Emergency Telecommunications* in Montreal, Canada. The NCS provided briefings on the history and operational capabilities of the NCS and NCC.

- Participated in the semi-annual U.S./Canada Civil Emergency Planning Telecommunications Advisory Group (CEPTAG) meeting held in Montreal, Canada. The CEPTAG is composed of members from the NCS and Industry Canada (NCC equivalent) to address communications concerns, cross border cooperation, and to foster mutual assistance in the event of an emergency.

- Participated in the NCS' ESF-2 Spring Training Conference in New Orleans. The ESF-2 conference featured briefings highlighting support team operations, new technologies, and training modules covering a variety of organizational and operational topics (including, ESF-2 Roles and Responsibilities, Alternative Communications Solutions). ESF-2 personnel also took part in "Hurricane Exercise Carl," a Functional exercise of a Category 3 hurricane making landfall on New Orleans.

- Expanded NCC industry membership to include satellite and cable providers, broadcasters, and industry associations.

- Worked with the Federal Communications Commission to improve situational awareness, information gathering, and the reporting of communication statuses during a major disaster. Implemented the Disaster Information Reporting System, an on-line system that allows the various communications providers (public safety, television, radio, cable, cellular and telephone) to report the status of their service and infrastructure within the disaster area. The information collected provides information critical to restoration activities and supports prioritization of NS/EP restoration requirements.

- Developed an Emergency Wireless Protocol (EWP) to provide detailed procedures for the NCC to coordinate requests for the disruption of cellular service. Began outreach endeavors with State and local emergency officials and the U.S. Secret Service to increase awareness of the EWP. Additionally, an EWP training presentation was developed in collaboration with industry. In FY 08, the EWP outreach efforts will be tied in with the GETS/WPS program to provide comprehensive outreach and marketing.

- Conducted ongoing activities related to NCC's move from the South Courthouse DISA facility to the DHS Glebe Road facility. This move will co-locate the NCC Watch with the National Cyber Security Division's U.S. Computer Emergency Readiness Team, allowing the two operations to leverage the synergies and converging aspects of the telecommunications and information technology sectors.

Communications Information Sharing and Analysis Center (ISAC)

In 2000, the NCC was designated the ISAC for the communications sector per the guidance of the 1998 Presidential Decision Directive (PDD-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 2007:

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

- Participated with NCS in exercises designed to test the ability of Federal government and private industry to respond to incidents. These exercises included:
  - DHS Ardent Sentry 2007;
  - Pinnacle 2007; and
  - ESF-2 Spring Training Conference 2007.
- Participated in the *National Symposium on Emergency Telecommunications* and CEPTAG meetings in Montreal, Canada.

Columbia, SC, August 31, 2006—Coast Guard Admiral John Currier (center) speaks with FEMA staff in the Mobile Emergency Response Vehicle (MEOV). The MEOV has been deployed to prepare for the landfall of Tropical Storm Ernesto. (Mark Wolfe/FEMA)

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 when normal communications are destroyed or unavailable. It brings together existing high frequency radio resources of Federal and federally affiliated organizations to include telecommunications industry and critical infrastructure providers. SHARES membership currently totals over 1300 individual stations supporting NS/EP events.

The SHARES HF Interagency Working Group, consisting of 110 members representing 107 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.

Additionally, the NCS HF Radio Program coordinated a two-day conference, “Non-Governmental Organizations (NGO) Radio Roundtable,” with representatives from eight NGO Radio community organizations. The conference was held to facilitate increased partnership between the Federal government and NGO emergency communications support entities.

During FY 2007, the SHARES HF network organized and/or participated in the following training exercises and program outreach activities:

- SHARES Exercise Operation Messenger (October 4, 2006);
- T-G Exercise (October 17, 2006);
- FEMA-National Emergency Communications Network test (December 7, 2006);
- SHARES Network Exercise (December 13, 2006);
- DOD-DICE Exercise (March 13-16, 2007);
- DHS-Ardent Sentry Exercise (May 7, 2007);
- Dayton/Nationwide Amateur Hamfest (May 18, 2007);
- Florida Governor’s Hurricane Conference (May 21, 2007);
- Verizon Disaster Recovery Exercise (May 23, 2007);
- FEMA-National Emergency Communications Network test (June 1, 2007);
- Verizon Communications Recovery Team Exercise (June 22, 2007);
- T-G Exercise (July 19, 2007); and
- SHARES Exercise (September 2007).

In addition to these events, the SHARES team conducts weekly daytime network checks and quarterly night-time network checks to maintain a state of equipment and procedural readiness for the NS/EP radio community.

Telecommunications Service Priority Program

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

Currently there are over 141,000 total active TSP assignments in support of NS/EP communications. During FY 2007, over 44,000 TSP codes were added, changed or revoked. Additionally, the TSP user base increased by approximately 115 new organizations bringing the total number of organizations with active TSP codes to over 860.

Network Security Information Exchanges (NSIE) Activities

In 1991 the NSC and the President's NSTAC recommended the establishment of a government-industry partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. A government NSIE and an NSTAC NSIE were formed to exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. In FY 2007, the NSIEs held bimonthly joint information sharing meetings and several ad hoc sessions to discuss security technologies and their implementation, including software and hardware encryption, personally identifiable information, and device theft. During FY 2007, the NSIEs participated in several conference calls to provide immediate assistance to NSIE member organizations when urgent security concerns arose. The NSIEs also produced the 2007 *Assessment of the Risk to the Security of the Public Network.*

The NSIEs also engage in international outreach activities. In FY 2007, the NSIE representatives participated in a trilateral NSIE meeting with the United Kingdom and Canadian NSIEs in Abingdon, United Kingdom. Included in the trilateral NSIE meeting were briefings and endorsements by leading figures in the United Kingdom information assurance and security community and telecommunications industry. The event included tri-lateral information sharing between all the participants representing the organizations within each country's NSIE. Following the sharing session were workshops based on the security issues of NGN convergence and how all three countries can work together. Each country's NSIEs agreed to champion at least one of the issues derived from the workshops and all three countries agreed to work collaboratively with one another on these issues. Canada will host the 2008 trilateral NSIE meeting and the U.S. will host the meeting in 2009.

Contingency Planning Branch

The Contingency Planning Branch focuses on developing doctrine and operational plans within the CIP division. The branch also translates these plans into tools and learning aids to effectively assimilate key concepts, roles and responsibilities to Emergency Communications Team members.

Contingency Planning

CP Branch focuses on contingency communications planning and has primary responsibility for development and publication of the Emergency Support Function 2–Communications (ESF-2) Annex to the National Response Framework, the ESF-2 Operations Plan (OPLAN), the NCS Continuity of Operations (COOP) Plan, the COOP Multi-Year Strategy and Program Management Plan, and numerous communications support documents.

The OPLAN augments the ESF-2 Communications Annex to the draft National Response Framework (NRF) which replaces the former National Response Plan. The OPLAN defines the organizational structures that form when ESF-2 is activated in response to an incident and outlines the roles and responsibilities of all ESF-2 supporting agencies under the NRF and the National Plan for Telecommunications Support in Non-Wartime Emergencies.

The NCS COOP plan identifies the NCS essential functions 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 Multi-Year Strategy and Program Management Plan (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 Branch is responsible for the development of job aids to translate national plans (National Response Plan) into specific tasks for Emergency Communications Team members. These tools are designed to increase efficiency by providing information on specific positions so that any official could perform the tasks associated with that position.

In addition to these job aids, the CP Branch produces standard operating procedures to provide direction, improve communication, reduce training time and enhance work consistency. Standard operating procedures are general guidelines promulgated by the CP Branch to promote a cohesive approach to responding to an incident.

A National Guard High-Mobility Multipurpose Wheeled Vehicle (HMMWV) departs the New Orleans Superdome in Louisiana to patrol the streets after Hurricane Katrina devastated the city. Department of Defense (DoD) units mobilized in support of humanitarian relief operations in the Gulf Coast region. (DoD photo by PH1(AW) BRIEN AHO, USN)

Regional Infrastructure

After Hurricane Katrina the CIP Division identified the requirement for a more robust regional presence. 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 RCC and a GS-13 Deputy RCC, will report to the CP Branch Chief.

During FY 2006, contractor personnel were assigned to Federal regions IV (Atlanta, GA), VI (Denton, TX), and VIII (Denver, CO) to serve as RCCs. Throughout FY 2007 those individuals remained in place and NCS submitted plans to replace these contractor staff with permanent Federal employees as well as staff the remaining RCCs and all Deputy RCCs throughout the country. RCCs attend emergency response planning conferences; participate in national, regional and local exercises; aid national, regional and local officials in their planning efforts; and establish and strengthen relationships with Federal agencies, State and local officials and private industry.

In FY 2007 the Region VI and IV RCCs participated in drafting Emergency Communications plans for states along the Gulf Coast which were seen as vulnerable to hurricanes. The focus was on identifying and pursuing mitigation strategies for communications vulnerabilities. The Region IV RCC continued working extensively in the Baton Rouge JFO as they implemented these mitigation strategies for Louisiana.

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 2007, the OA Branch focused on improving the quality, comprehensiveness and timeliness of telecommunication analytic products. Initiatives conducted during FY 2007 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. To address 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, other support elements, 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 refined a set of standard operating procedures and exercised them through a tabletop and live-scale exercise.

Exercise Activities

The United States faces the continuing threat of natural disasters and terrorist activity within its borders. The need for immediate response to these events increases the demand for real-time analytic capabilities during emergency response operations. The government and its sector specific agencies must be fully prepared to produce quality analytic products in a real-time environment in an effort to help protect and restore the nation's critical infrastructure during and the preparation, response and recovery phases of NS/EP emergencies. In order to ensure proper response to such events, government and industry exercises are developed around specific scenarios to test and improve response and recovery capabilities. During FY 2007, the OA Branch participated in the planning, conduct, and evaluation of multiple exercises to test and evaluate its analytic capabilities in response to various scenarios. The OA Branch supported both pre- and post-impact scenario exercise analyses, utilized models to identify potential impacts to the communications infrastructure, represented actual impacts to the communications infrastructure, and tracked restoration activities to inform key government officials as to the progress of overall restoration efforts. During this reporting period, the OA Branch provided support for NORTHCOM's Vigilant Shield '07 and Ardent Sentry exercises, the Department of Homeland Security's Pinnacle '07, TOPOFF4, and ESF-2 exercises, and the NCS's Live-Scale Analytic exercise series.

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, and its interaction with various other infrastructures and sectors. 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. Additionally, each regional characterization identifies and provides in depth analysis of specific agency and communications sites of particular significance in the region. The results of these studies are incorporated into the NCS analytical tools and models used to support telecommunication assessments. During FY 2007, the OA Branch completed characterization studies in the metropolitan areas of Boston, Chicago, Dallas, Seattle and Atlanta. In addition, the OA Branch has updated FY 2006 characterizations of San Francisco, Miami, and Philadelphia to incorporate updated findings, data, and design, to provide the most accurate and relevant understanding of high-risk areas.

Concentration Analysis

In FY 2007, the DHS Risk Management Division requested the NCS identify bridges and tunnels where there is a potential for a concentration of telecommunications fiber crossings. The OA Branch expanded the request to analyze concentration of the physical telecommunications infrastructure within metropolitan areas and across the United States. The purpose of the analysis is to identify potential points of concentration within the telecommunications infrastructure. Risks to the telecommunications infrastructure may increase at points of concentration because damage at a concentration point has the potential to affect a large segment of the telecommunications infrastructure. During FY 2007, the OA Branch initiated regional concentration studies for the major metropolitan regions within the United States, as well as a core network analysis to identify infrastructure routes that support large volumes of telecommunications traffic and locations in the long distance network where infrastructure is concentrated. The finished analysis document is intended as an "on the shelf" document for the NCS to be used to enhance operational understanding of the telecommunications network and augment the current understanding of the overall risks to the telecommunications sector.

Training and Exercise Branch

The T&E 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 2007, the T&E Branch successfully planned, coordinated and performed the following activities:

Emergency Support Function (ESF) 2 Training Conferences

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. This resulted in the modification of the training and exercise program to improve ESF-2 staff members' 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. Additionally, ESF-2 Training Conferences were implemented to prepare the Emergency Communication Teams (National and Field) (ECT-N and ECT-F) to respond to any communications infrastructure crisis or emergency condition. These ESF-2 Training conferences occur biannually and consist of a myriad of various training topics and exercises which are used to educate, exercise, and provide hands on experience for ESF-2 team members. These training conferences ensure that the ECT-N and ECT-F are developed as response teams with diverse functional telecommunication skill sets enabling them to perform the ESF-2 missions.

FY 2007 Winter Training Conference:

From December 5-6, 2006, the NCS conducted an ESF-2 training conference for over 120 attendees in Oakton, VA. This conference focused on reviewing the lessons learned from the 2006 Hurricane Season and any catastrophic events that required deployment of ESF-2 resources and support. Additionally, the conference focused on the role of the NCS within DHS; highlighted the national telecommunications programs that support emergency management and response operations; and facilitated an inter-agency discussion of communications support for emergency response operations. The conference featured presentations of updated organizational policies, procedures, and program resources that support the operation of the ECT-N and ECT-F. The conference culminated with an Emergency Preparedness and Response Panel Group Discussion consisting of 8 panel members and a facilitator. The panelists represented different roles of authority within Federal, regional, State, and local government and private sector emergency management. Members of the panel responded to different scenario events that dealt with regional situations caused by an earthquake and after shocks in the New Madrid Seismic Zone. The panelists' comments were supplemented by audience participation throughout the session.

FY 2007 Spring Training Conference

From June 19-28, 2007, the NCS conducted an ESF-2 training conference for over 150 ESF-2 team members in New Orleans, Louisiana. The training conference was focused as a capstone training event in preparation for the upcoming 2007 Hurricane Season. Specifically, it focused on preparation and response to a major hurricane making landfall along the U.S. coastal areas of the Gulf of Mexico. Replicating the activation, deployment, response and deactivation activities for ESF-2 operations, the exercise began with participants being alerted to the approach of a significant tropical storm projected to cross the Caribbean Sea into the Gulf of Mexico. This alert phase was followed by the activation and deployment phases with instructions for the participants to deploy to join an ECT-F at a notional Joint Field Office (JFO), or the ECT-N. The participants were then formed into three teams (Red, White, Blue) simulating "JFOs" as well as a "National" team to replicate the NCC, and subject matter experts participating as observers, controllers, and response cell personnel. The exercise play continued throughout the nine-day training period using scenario specific exercise injects. Additionally, ESF-2 conference agenda included classroom instruction and site specific tours

Debbie Warden, communications manager for the Louisiana Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) in Baton Rouge, La., directs a tour of the emergency communications center for Federal communications personnel. Federal workers toured a variety of emergency communications facilities during parts of their nine-day Emergency Support Function 2 training held June 19-28 in New Orleans. (Photo by Steve Barrett, National Communications System)

Captain Stephen Gordon of the New Orleans Police Department addressed Federal emergency communications officials on New Orleans public safety and emergency 9-1-1 operations before and after Hurricane Katrina as part of a nine-day Emergency Support Function 2 training seminar held in New Orleans June 19-28. (Photo by Steve Barrett, National Communications System)

in the New Orleans region. Topics for the classroom instruction incorporated audience feedback from the 2006 Spring Training Conference (Homestead, FL) and the 2006 Winter Conference (Oakton, VA) as well as newly updated information and guidance impacting the ESF-2 community.

Classroom Instruction

- National Response Plan/FEMA Communications;
- ESF-2 Roles and Responsibilities;
- Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act);
- Mission Assignments;
- Spectrum Management;
- Land Mobile Radio Systems;
- Network Operations;
- Communications Assessments;
- Public Safety and Public Safety Access Point (PSAP) Operations;
- Alternative Communications Solutions;
- RoIP and VoIP;
- Stress Management and Conflict Resolution Tours;
- Parish Locations affected by Hurricane Katrina;
- New Orleans 911 PSAP;
- New Orleans AT&T Central Office;
- New Orleans Emergency Operations Center (EOC);
- State of Louisiana EOC; and
- Telecommunications Vendor Demonstration Site.

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 2007, the NCS IMAs continued to support the post-Katrina long-term recovery operation by representing ESF-2 at the Federal Joint Field Office in Baton Rouge until deactivation in December 2006. Additionally, officers from the IMA Unit joined the NCS Regional Managers to represent ESF-2 in the following regional exercises: GOLDEN GUARDIAN (Sacramento, CA) and BLUE CASCADES (Tacoma, WA). The ESF-2 Training Conferences are important training events for the IMA Unit. These events provide opportunities for the military officers to train with their civilian team members, whom they will work with during emergency operations. In response to the increased frequency and duration of duty deployments, the NCS IMA Unit increased its personnel strength to the current roster of 21 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 *National Response Plan*. The IMA's received briefings about the NCS programs that provide priority communications services to assist the emergency responder; the IMA training program; and relationships and coordination between industry and

government on telecommunications matters. The Augmentees also received a tour of the NCC, the FEMA-NRCC and the FCC operations center.

ESF-2 Exercises

In preparation for the 2007 Hurricane Season and the potential development of Incidents of National Significance, the Department of Homeland Security sponsored multiple exercises to assess the capabilities of Federal, state and local governments and private industry to respond to catastrophic events. The NCS partnered with various agencies, including the General Services Administration, the Federal Communications Commission, the National Telecommunications and Information Administration, the Federal Emergency Management Agency, and the Department of Agriculture, to plan and execute ESF-2 responsibilities as a major participant in the following exercises:

- Exercise PINNACLE 07 (sponsored by EOP); and
- Exercise ARDENT SENTRY NORTHERN EDGE (ASNE) 07 (co-sponsored by DOD/NORTHCOM and DHS).

The NCS demonstrated dedicated involvement with each one of these exercises by providing realistic and coordinated communications impact analyses and scenario-based injects to support the exercise play.

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

- Exercise GOLDEN GUARDIAN (sponsored by FEMA Region 9)
  - Scenario featured
    - Terrorism with Improvised Explosive Device;
    - Bio-toxin release;
    - Earthquake; and
    - Mass Care and Sheltering.
- Exercise BLUE CASCADES (sponsored by Pacific Northwest Economic Region)
  - Scenario featured: Impact of a pandemic flu on Critical Infrastructures and Key Resources

NCS International–FY 2007

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 CIP and Civil Emergency Planning (CEP).

Brian Carney (right), Manager of the National Communications System's National Coordinating Center, discusses emergency communications with retired Marine Corps Lt. Col. Jerry Sneed, Director of the Office of Emergency Preparedness for the City of New Orleans. The visit was part of a tour of emergency response facilities attended by Federal communications officials during Emergency Support Function 2 (Communications) training held in New Orleans June 19-28. (Photo by Steve Barrett, National Communications System)

Summary

Over the course of the year, the NCS maintained its robust relationship with Canada, 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 second year with the NCS continuing to lead four initiatives. 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 was significant with increasing focus on NGN and its implications for U.S. NS/EP communications. Finally, the NCS continued its role as a reviewing organization to the CFIUS.

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

I. Multilateral Engagements

a) The Security & Prosperity Partnership

The leaders of the United States, Canada, and Mexico celebrated the two-year anniversary of the SPP in August 2007. The NCS worked with its counterparts on several initiatives of the Security pillar's Goal 9, which addresses Protection, Prevention & Response. The NCS' work with Canada resulted in continued progress on information sharing initiatives, as well as robust discussions on vulnerability assessments. Progress with Mexico moved at a slower pace, but the NCS hopes to reengage with the Government of Mexico in late-2007.

b) The North Atlantic Treaty Organization's Civil Communications Planning Committee (CCPC)

The NCS Department of State detailee heads the U.S. delegation to the CCPC with a U.S. telecommunications industry representative as well as representatives of the U.S. Postal Service. During FY 2007, the CCPC met twice in plenary session, as well as four times in working group format to complete tasks from the 2005/2006 CCPC Work Program (WP), as well as begin work on the 2007/2008 WP. Major FY 2007 activities and accomplishments included:

- The U.S. completed Task 2.1 of the 2005/2006 CCPC WP, which analyzed the relevance of NATO's policy on censorship with regard to NATO & national responses to terrorism.

- The U.S. worked closely with partner nations to develop the CCPC's WP for 2007/2008. This WP will guide the work of the committee for the next two years and the U.S. worked to ensure the resulting tasks were relevant, achievable, and contributed to the U.S.' larger goals at NATO.

- Members of the U.S. CCPC and NATO Joint Medical Committee discussed the potential effects of Pandemic & Avian flu on NATO CEP, as well as utilizing postal resources to distribute key medicines.

- Among many other contributions to the CCPC, the U.S. participated in efforts to complete the initial version of the NATO Rapid Reaction Team Handbook, volunteered to lead and participate in multiple tasks for in the 2007/2008 WP, and continued to build relationships with key members of the committee and in NATO's CEP community.

II. Bilateral Engagements

a) Canada

The NCS maintained its very strong working relationship with Canada throughout FY 2007, embodied primarily in the U.S./Canada CEPTAG. In addition to virtually continuous informal correspondence with Canadian colleagues, engagement included the following activities during FY 2007;

- Information sharing between the NCS' NSIE and Canada's NSIE continued, including the first trilateral NSIE between the United States, Canada, and the United Kingdom (U.K.).

- As prescribed in bilateral agreements, two official CEPTAG meetings were held, with agendas including such topics as; the SPP, the effects of Avian Flu, the NCS GETS and WPS, and NATO.

- Officials from the United States and Canada agreed to establish a bilateral working group to analyze the feasibility, utility, and issues associated with cross-border vulnerability assessments in the telecommunications sector.

- To promote Watch and Warning coordination, the NCS' NCC continued to conduct weekly Video TeleConferences with Industry Canada.

b) United Kingdom

This critical relationship also continued to flourish in FY 2007. Meetings and discussions were pursued under the auspices of the Joint Contact Group (JCG) and NATO. As with Canada, the NCS enjoys a substantial relationship with its U.K. counterparts and notable activities for FY 2007 included:

- Officials from the NCS and U.K. met on several occasions to develop an initiative for resilient communications between the United States and U.K. governments during a crisis.

- Information sharing between the NCS' NSIE and the U.K.'s NSIE continued, including the first trilateral NSIE between the U.S., Canada, and the U.K.

- The NCS conducted discussions with the U.K. about ongoing NATO CCPC developments, as well as their inclusion in the ongoing dialogue between the U.S. and Canada on international CIP issues.

c) Mexico

The NCS began to engage Mexican telecommunications officials in October of 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 2007, the NCS remained engaged in conjunction with parallel efforts of the DoS.

d) Other Bilateral Engagements and International activity

The NCS continued to work closely with the DoS' Bureau of Political-Military Affairs and the Bureau of Economic & Business Affairs among others, 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 USG 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:

- European Union (EU)–The NCS participated in a briefing of an EU official on the activities and priorities of DHS CS&C.

- South Korea–The NCS hosted a delegation from South Korea's Ministry of Communications in March of 2007.

IV. Plans for FY 2008 and beyond

The NCS will continue to review and update its international strategy with key DHS and other agency stakeholders. Particular emphasis will be placed on ensuring the goals outlined in the NIPP and that coordination with CS&C and the National Cyber Security Division (NCSD) on international priorities are addressed. Specific areas of focus will be as follows:

a) Security & Prosperity Partnership

The NCS will continue to work with counterparts in the United States, Canada, and Mexico to achieve the goals established in the SPP.

b) North Atlantic Treaty Organization's Civil Communications Planning Committee

The United States will maintain representation in the CCPC to ensure that U.S. interests and goals are addressed in the body. The CCPC has finalized its 2007/2008 WP and the United States is working with partner nations to ensure the committee's completes its deliverables according to the established timelines.

c) Bilateral Relationship with Canada

The United States expects to continue its strong working relationship with Canada in FY 2008. The NCS expects to attend several face-to-face meetings with Canadian colleagues, as well as maintain regular communications with working-level officials.

d) Bilateral Relationship with the U.K.

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

e) Bilateral Relationship with Mexico

With the inauguration of the new President in Mexico in late-2006, the NCS hopes this event will present an opportunity to improve engagement with the government of Mexico. The NCS hopes to finalize key U.S./Mexican documents and establish sound working-level relationships with appropriate officials.

Plans and Resources Division

The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, manpower allocations, and other 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 established the NCS COP in 1984 through E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. The order outlined a broad new scope for the NCS, defining an organizational structure for the creation of a concentrated NS/EP telecommunications function, and tasking the COP with providing advice and recommendations on NS/EP telecommunications to the EOP.

The President appoints members to the COP, which consists of senior-level officials representing 24 Federal departments and agencies with telecommunications facilities or services significant to NS/EP activities. The committee is a nexus for member departments and agencies to exchange ideas, coordinate interagency activity, and form recommendations on current and emerging telecommunications issues. The committee meets at least twice per year, as mandated 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 regarding policy development and collaborative activities in support of NS/EP telecommunications.

COP Principals represent their respective departments and agencies to work in partnership on NS/EP issues, providing comments and recommendations on current and prospective NCS programs to the NCS, the Homeland Security Council (HSC), the NSC, the OMB, the OSTP, and the Executive Agent. The COP submits its recommendations directly to the OMNCS; the Secretary of Homeland Security; and the President. The COP also performs any other duties or tasks the President or his authorized designee requests. Because of the increasing visibility and significance of its responsibilities, Secretary of Homeland Security Michael Chertoff elevated membership of the COP to the Assistant Secretary level in FY 2007. This change will enable COP members to more effectively support the ability of member departments and agencies to contribute to and benefit from the COP process and ensures that COP members will be able to act on behalf of their departments and agencies with the appropriate understanding of technology, policy, and budget processes.

FY 2007 brought a reinvigoration of the COP on many fronts, including an accelerated meeting schedule, increased sponsorship of working groups, engagement in key issues, and interaction with other entities across the NS/EP spectrum. Within the DHS organizational framework, the NCS and the COP join the NCSD, and the newly-established OEC under the CS&C Directorate to foster an ongoing partnership to build public, private, and international alliances to enhance the security of communications infrastructures.

In response to an OEC request for the National Communications Baseline Assessment, selected COP members played an instrumental role in identifying points of contact to provide data on their respective departments' and agencies' interoperable emergency communications capabilities. Furthermore, the COP provided critical guidance to the Federal Communications Commission in developing the 9/11 Implementation Act's (P.L. 110-53, *Implementing Recommendations of the 9/11 Commission Act* of 2007-H.R. 1/S.4) requirement for a Critical Infrastructure Protection Vulnerability Assessment and Report. Furthermore, the COP has initiated activity toward meeting the requirements of National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, released in May 2007.

Homeland Security Secretary Michael Chertoff briefs members of the President's National Security Telecommunications Advisory Committee during the closed session of the committee's annual meeting in Washington on April 26. (Photo by Donna Burton, Defense Information Systems Agency)

The COP finalized the NCS COP *Report on Telecommunications Service Priority* and voted to establish the Communications Dependency on Electric Power Working Group (CDEP WG) to study the communications sector's dependence on electric power and to address recommendations from the NSTAC *Report to the President on Telecommunications and Electric Power Interdependencies*. The COP spearheaded a meeting dedicated to briefings from department and agency representatives on their organizations' preparedness plans for the 2007 hurricane season. Throughout the year, the COP has requested and received briefings regarding the activities of ESF-2 training, Cyber Storm II and other exercises, and is examining methods of injecting seriously degraded or denied communications scenarios into national exercises. The COP continues to explore the establishment of a Technical Assistance Team to build communications into NCS and COP member entities' exercise programs.

The COP also remained engaged in the progress of the NSTAC *Report to the President on Global Infrastructure Resiliency* and provided comments on the National Command and Coordination Capability (NCCC) Implementation Plan. Member organizations began developing updated memoranda of agreement (MOA) with the NCS, using a new MOA template and designating official detailees.

COP members provided comments on NCS Directive (NCSD) 3-10, *Minimum Requirements for Continuity Communications Capabilities*, and helped to develop the capabilities for the requirements section. Additionally, the COP provided comments on the accompanying NCS Manual 3-10-1, *Minimum Requirements for Continuity Communications Capabilities Users Manual*. The COP continues to support the OMNCS in scoping the potential for a consolidated purchase of communications equipment to meet the NCSD 3-10 requirements.

Council of Representatives

The Council of Representatives (COR) is a permanent subordinate group of the COP established by the COP Bylaws to assist the COP in the execution of its assigned responsibilities. The COR membership consists of the 24 departments and agencies that make up the COP. COR members participate in dedicated working groups to conduct special studies and make recommendations to the COP on matters concerning NS/EP telecommunications.

Priority Services Working Group

The COP established the Priority Services Working Group (PSWG) in 2003, tasking the group with four activities: (1) an evaluation of the NCS GETS, TSP, and the 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.

In FY 2007, the PSWG finalized its report evaluating the TSP program, which was well-received by the HSC and the wider NS/EP community. The PSWG also developed a white paper on the need for expanded use of DHS grants for TSP coverage for State and local responders. The white paper was developed in light of the NCS' successful GETS/WPS outreach efforts among Government, industry, and first responder communities, and the development of a capability for converging GETS into the next generation Internet Protocol environment. The working group also updated its charter, examined next steps for studies of GETS and WPS, and made strategy recommendations aimed at improving the visibility and participation levels of priority service programs.

Continuity Communications Working Group

In May 2006, the COP reconstituted the CCWG to oversee the activities of the CCA PO. The PO was later renamed the NCCC Coordination and Management Office (CMO) to address the overlap between the CCWG and NCCC efforts. The Program Office is charged with developing a Continuity Communications (CC) FEA and Framework to enable FEB departments and agencies to perform PMEF and national essential functions under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

In FY 2007, the CCWG, through the CMO, continued their efforts to develop a draft NCCC Governance Framework and draft NCCC Implementation Plan. The group also continued to direct the CCEA PMEF normalization and data collection efforts. In addition, the CMO was instrumental in the development of NCS Manual 3-10-1, which serves as a guide to achieving full compliance with NCS Directive 3-10 by outlining the requirements to meet each type of essential communication.

Communications Dependency on Electric Power Working Group

As the governmental response to recommendations in the President's NSTAC *Report on Telecommunications and Electric Power Interdependencies* (TEPI), the COP began development of the CDEP WG in July 2007. The working group will seek to examine issues raised in the NSTAC TEPI Report, and will work in concert with the private sector to address the full set of recommendations made by the NSTAC. Additionally, the CDEP WG will assess a broad range of concerns inherent in the communications sector's dependence on the reliable operation of the electric power sector.

The CDEP WG has begun drafting its charter and milestones for accomplishing its objectives, and has also begun the process of examining existing studies on long-term outages of electric power. Upon completion of the draft charter, the CDEP WG will present a preliminary report and the COP will vote to approve the group's charter.

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.

As Robert D. Jamison (left) listens, George W. Foresman, the Department of Homeland Security's departing Under Secretary for National Protection and Programs Directorate (NPPD) and Manager of the National Communications System, emphasizes the importance of government-industry partnership during the 30th meeting of the President's National Security Telecommunications Advisory Committee held April 26. (Photo by Donna Burton, Defense Information Systems Agency)

The NSTAC held its annual meeting on April 26, 2007, 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 2007-2008 Cycle. The NSTAC also met quarterly via conference call. Topics discussed included global infrastructure resiliency, international communications, and emergency communications and interoperability.

Industry Executive Subcommittee

During FY 2007, the NSTAC's Industry Executive Subcommittee (IES) continued to identify communications issues critical to NS/EP activities for consideration by its subgroups. The NSTAC addressed a variety of issues, including: international implications of the NGN; emergency communications and interoperability; telecommunications and electric power interdependency; global infrastructure resiliency; dependence on global positioning system satellites; the evolving role of the NCC; NSTAC outreach efforts; research and development issues; 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, including:

- a overview of the National Infrastructure Protection Plan;
- a briefing on Industry Canada;
- an overview of priority services in the NGN; and
- a briefing on class of service.

National Coordinating Center

The NSTAC reconvened the NCC Task Force (NCCTF) to scope potential issues for additional study and to evaluate progress that Government has made regarding its recommendations in the NCC 2006 report. The report contained a five-year roadmap of recommended actions to improve the operations of the NCC and evolve its mission and organization.

In spring 2007, the committee evaluated a range of potential issues for further examination, including the operational consolidation of the information technology and communications sectors; the rewrite of the *National Response Plan* and the *ESF-2 Annex*; and education and outreach on the NCC. The committee concluded that no issues warranted additional study at the current time.

The NCCTF developed a status report for the NSTAC Principals to review, addressing recommendations and roadmap actions identified in the *NSTAC Report on the National Coordinating Center.* The status report provided updates on the progress made against NSTAC recommendations and feedback to DHS on next steps. Based on the analysis of the progress made to date, the report made the following observations to DHS on next steps:

- Continued success of the NCS process can be ensured by updating the memoranda of agreement between the NCS Member Departments and Agencies and providing expert detailees to the NCS and NCC.

- The NCS should formalize its relationships with the DOD, including watch functions, by entering into memoranda of understanding and/or developing joint standard operating procedures for enhanced coordination in the future, including routine testing and the exercising of capabilities.

- The NCS Manager should provide annual updates on the status of the NCC roadmap to the NSTAC to ensure the NSTAC Principals remain engaged in the important partnership.

- The NCC Manager should implement a new structure that reflects the diversity of expanding NCC membership and enhances the level of trust amongst the membership.

- As the NCC Manager carefully monitors the level of information sharing in the NCC, this will ensure the organization remains a trusted environment.

- As the NCC evolves, industry and Government members should recurrently assess the NCC and its mission to ensure a focus on the primary NCC NS/EP mission while continuing to provide value to all the partners.

Telecommunications and Electric Power Interdependencies

Throughout FY 2007, the NSTAC's TEPITF continued to examine the NS/EP implications associated with interdependencies between the telecommunications and electric power sectors. Task force participation included a significant number of companies from both the United States 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, North American Electric Reliability Council, the NCS, and National laboratories.

The NSTAC tasked the TEPITF to evaluate how sector interdependencies will affect the future of the telecommunications network. The task force divided the effort into two work streams. The first, completed in January 2006 and culminating in the *NSTAC Report to the President on People and Processes: Current State of Telecommunications and Electric Power Interdependencies*, examined the people and processes involved in national emergency communication and restoration. Its recommendations centered on the concept of an "Emergency Responder," a new designation

similar to First Responder, which would apply to key response personnel from telecommunications and electric power service providers. This classification would allow telecommunications and electric power service providers to be involved in Federal, State, regional, and local emergency planning processes and to actively participate in response at operations centers during emergencies. This classification also would allow providers, through the effective use of credentialing, to gain timely and secure access to restricted areas to restore their critical assets.

The second work stream, completed in December 2006 and culminating in the *NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: The Impact of a Long-Term Outage*, examined the technological interdependencies that will affect telecommunications networks in the future. Specifically, this work defined and explored the NS/EP implications of a "long-term outage" (LTO)—an interruption of communications and/or electricity for a period long enough, and within a large enough geographic region, to hamper the provision of telecommunications and electric power even by alternative means. Such an outage has not occurred in North America to date, but could occur in any critical infrastructure and, in the worst case, could have a cascading effect on other sectors.

In its report on LTOs, the committee recommended that the President direct his departments and agencies to:

- Commission a Government-funded, cross-sector, and cross-border engineering analysis of the North American telecommunications and electric power infrastructures with attention given to further international considerations to determine the interdependencies in LTO situations for both the current and the NGN environment, and to estimate the attendant costs of mitigation strategies, including the following:
  - Investigating how dependencies and interdependencies will be affected by technology and structural changes in both sectors; and
  - Supporting exercises at the local, State, regional, national, and international level that investigate the dependencies and interdependencies between the two sectors during an LTO.
- Analyze and evaluate current governance procedures applicable to an LTO to determine the appropriate transition from local to national management authority during an LTO. Internet recovery issues (as they relate to the convergence of the telecommunications network) should also be reviewed, but such a review should not be limited to an LTO event.
- Reduce dependencies between the sectors, maintain a minimum level of internal service availability during an LTO, and vigorously support selected science and technology applications, including the following:
  - Transformer Prototype Technology;
  - Power Conservation Technology for Telecommunications; and
  - Fuel-Cell Technology.
- In concert with industry, support the advent and development of cross-sector situational-analysis tools to facilitate information sharing between industry and Government in advance of, during, and after an LTO.
- As stated in the *NSTAC Report to the President on People and Processes: Current State of Telecommunications and Electric Power Interdependencies*, continue to promote increased collaboration between both the telecommunications and electric power sectors and emergency management authorities at the local, regional, State, national, and international levels to facilitate recovery from an LTO.

The committee officially closed TEPI work on January 18, 2007.

Emergency Communications and Interoperability

Throughout FY 2007, the NSTAC, through its Emergency Communications and Interoperability Task Force (ECITF), continued to examine recommendations to improve emergency communications and interoperability. In January 2007, the NSTAC Principals approved its *Report to the President on Emergency Communications and Interoperability*, which expanded upon previous recommendations and, per White House request, provided input to the planned National Emergency Communications Strategy (NECS) and National Emergency Communications Plan (NECP).

In its report, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by E.O. 12472:

- Direct DHS to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure. The President should also direct the DHS to expand and enhance use of the WPS program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi-carrier WPS end-to-end solutions that facilitate the rapid restoration of essential wireless network elements.

- Direct DHS and other responsible Federal agencies to explore enhancements to the TSP program to accommodate expanded requests from NS/EP users of wireless telecommunications services at critical sites. The President should also direct Federal agencies, and encourage State and local agencies, to fully utilize the existing provisions of TSP and to apply for the enhanced wireless TSP coverage provisions as they are developed for use at their critical sites.

- Modernize existing NS/EP policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities.

- Incorporate the following critical elements in the development, maintenance, and execution of the NECS and associated implementation guidance, and direct the DHS and other responsible Federal agencies to incorporate the elements into the NECP:

    - Large-scale State and regional shared public safety networks and Federal grants;

    - Yearly benchmarks for achieving defined interoperability objectives;

    - Nationwide outreach to support emergency response communications;

    - Consolidation of operations centers to increase coordination and situational awareness; and

    - Identification of specific private-sector emergency communications and interoperability support roles.

- Encourage responsive emergency communications capabilities in the converged environment, establish and incorporate the following capability objectives into the NECS and associated implementation guidance, and also direct the DHS to incorporate the capability objectives into the NECP:

    - Support for a significantly expanded user base;

    - Full leveraging of network assets;

    - Internet Protocol (IP) -based interoperability;

    - Assured access for key users through priority schemes or dedicated spectrum;

    - National scope with common procedures and interoperable technologies;

    - Deployable elements to supplement and bolster operability and interoperability;

    - Resilient and disruption-tolerant communications networks;

    - Network-centric principles benefiting emergency communications; and

    - Enhanced communications features.

The NSTAC continues to evaluate and refine strategies and recommendations to enhance emergency communications operability and interoperability and expects to finalize its analysis by the end of 2007.

International Communications

During FY 2007, the NSTAC, through the International Task Force, continued to examine international concerns raised during the NSTAC's previous examination of the NGN.

The NSTAC received briefings and information from industry and Government subject matter experts in policy development, international relations, operational control (such as cyber incident response), standards and protocol development, intelligence, and internationally significant infrastructure. Briefings covered wide-ranging topics, including the international activities of the NCS and NCSD; the Department of State's international communications coordination activities; the private sector role within

military-to-military relationships; current interagency, DHS, and DOD NS/EP engagements and other direct NS/EP engagements with foreign governments; and the U.S.-Canadian telecommunications and electric power bilateral relationship.

The NSTAC also reviewed international network infrastructure incident response policies and legal frameworks that define or influence how U.S. infrastructure operators currently interact with foreign governments or foreign operators. U.S. Government staff, as well as network security experts from agencies of the U.K. and Canadian governments, participated significantly in this research.

The NSTAC agreed on the following findings:

- The rapidly evolving global communications infrastructure is increasingly interconnected through a system of systems that provides global services and connectivity. A global workforce, including those in non-allied nations, operates and maintains the infrastructure.

- As a result of globalization, the U.S. NS/EP communities, government operations, allies, many key businesses, and their global business partners are increasingly dependent on the availability of global communications and related services.

- Cross-sector dependencies and interdependencies (such as between telecommunications and electric power) create additional complexities, amplifying the difficulties of mitigation and effective repair when broad-scale disruptions occur.

- Cyber threats to global infrastructures may originate from international sources beyond the jurisdiction of United States and allied authorities.

    - Attacks originating outside the territorial United States raise increasing concerns about the security and availability of domestic NS/EP communications and the global communications on which many key U.S. functions and economic interests rely.

    - The sophistication and reach of the global communications infrastructure increase the complexity of the threat, whereas the adversary's barrier to entry is low as a result of anonymity, connectivity, and widespread availability of tools for creating disruptions.

- The U.S. Government's international NS/EP strategies, policies, and operational response frameworks are not sufficient to keep pace with globalization and technological convergence of public networks and private sector networks, nor do they adequately include private sector participation in these processes.

At the close of its investigation in August 2007, the NSTAC recommended that the President direct the following:

- Task DHS to coordinate international planning and development with the appropriate Federal Agencies for adoption of a global framework incorporating operational protocols and response strategies. The framework must accomplish the following:

    - Address physical and cyber events that would disrupt the availability of critical global infrastructure services;

    - Ensure private sector participation in developing the framework to leverage extensive expertise and existing relationships;

    - Support the use of identity management solutions that address NS/EP requirements for normal operations and all-hazards crisis response; and

    - Examine, with the help of private sector partners, existing U.S. laws and policies that could prevent service providers and other stakeholders from taking the necessary proactive measures to restore service and prevent harm to NS/EP users for government essential operations during a crisis.

- In the interim, task Federal Agencies to expand relationships and response coordination using

formal and reciprocal agreements with Allied governments to include participation from selected international service providers and other stakeholders into existing joint U.S. Government and private-sector response and coordination processes and entities, such as the U.S. Computer Emergency Readiness Team and the NCC.

Legislative and Regulatory Issues

During FY 2007, the NSTAC's Legislative and Regulatory Task Force (LRTF), continued to closely follow several laws passed by Congress that altered the face of DHS and its communications component agencies; substantive structural changes of regulatory bodies; and the release of new directives on important homeland security matters.

The Committee evaluated the NS/EP impact of the *21st Century Emergency Communications Act of 2006* as part of the *DHS Appropriations Act*, 2007, and examined the changes in light of communications work performed at other DHS agencies, including the Federal Emergency Management Agency and the Directorate of Science and Technology's Office for Interoperability and Compatibility.

In January 2006, the NSTAC recommended the President ensure telecommunications infrastructure providers have access to restricted areas during a disaster by directing DHS to work with Congress to amend the *Stafford Act*. Amending the Stafford Act included designating telecommunications infrastructure providers as "Emergency Responders (Private Sector)" to ensure they received the Federal resources necessary to recover NS/EP networks. Recognizing the need to modernize the Nation's Emergency Alert System, Congress passed the *Warning, Alert, and Response Network (WARN) Act*, which the President signed on October 13, 2006. The bill addressed telecommunications service provider access to disaster sites during an emergency; the NSTAC had identified a lack of access as a major impediment to recovering telecommunications infrastructure following the 2005 hurricane season. The WARN Act amended the Stafford Act by designating telecommunications providers as "essential service providers" and by stating that Federal agencies may not prevent these providers from accessing disaster sites unless extreme circumstances apply.

The Committee reviewed this legislative change and determined that additional policy changes would help ensure that DHS and other emergency response officials did not misinterpret the statutory basis for non-monetary Federal assistance to telecommunications infrastructure providers during disaster situations. The Committee considered the importance of aligning the "essential service provider" language in the WARN Act with the *Homeland Security Act of 2002* and with the revised NRP.

In September 2006, the FCC established the Bureau of Public Safety and Homeland Security as a clearinghouse for public safety communications information. The LRTF received a briefing from Mr. Jeffery Goldthorp, FCC, on the scope and organization of the Bureau and its role in coordinating with the private sector on emergency response issues. Mr. Derek Poarch, Chief, Bureau of Public Safety and Homeland Security Chief, FCC, addressed NSTAC Principals at the April 27, 2007, NSTAC Meeting and reiterated that industry and Government must work together to restore networks following an disaster.

Participants at the NSTAC Meeting discussed the vulnerability of the Internet to abuse by terrorists and other criminals, prompting the committee to begin studying legal issues associated with disabling the Internet in response to international cyber incidents. The LRTF received a briefing from Mr. James Lewis, Center for Strategic and International Studies, on the April 2007 cyber attack on Estonia and subsequently reached out to U.S. law enforcement agencies for information on cybersecurity tools and their legal precedents.

On May 9, 2007, President Bush issued NSPD 51/HSPD 20, and the NSTAC worked through the LRTF to determine its implications for NS/EP communications. The LRTF examined the Directive in the context of previous continuity of Government Presidential directives. The LRTF determined that due to the Government's reliance on private sector infrastructures, Federal officials drafting the National Continuity Implementation Plan, which is called for in NSPD 51/HSPD 20, should consult with industry.

Finally, the committee continued to examine legislation it estimated would have a significant impact on NS/EP telecommunications, including the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which became law on August 3, 2007, and *DHS Appropriations Act*, 2008.

Research and Development

During FY 2007, the Research and Development Task Force (RDTF) continued to pursue issues identified at the first international Research and Development Exchange (RDX) Workshop in September 2006. The 2006 RDX Workshop Proceedings highlighted six overarching issue areas and corresponding agendas for action regarding international collaboration for cybersecurity research and development (R&D). Conclusions included:

- There is a need for technologies and mechanisms to enable trust and build communities of interest;
- International collaboration is essential for successful cybersecurity R&D initiatives;
- To advance cybersecurity 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 cybersecurity R&D; and
- Strengthened education, awareness, and training programs increase the effectiveness of R&D partnerships and programs.

Based on these conclusions, the task force focused its attention in FY 2007 on examining identity management, a topic that fit into several of the overarching issue areas from the 2006 RDX Workshop. In November 2006, the RDTF conducted a scoping session on identity management as a follow-up to the work of the Next Generation Networks Task Force. The task force invited a limited number of subject matter experts to define the scope of the identity management effort in the context of NS/EP considerations. The scoping session resulted in a list of candidate issues for NSTAC consideration on the identity management topic.

As a follow-on to the identity management scoping session, the RDTF received several briefings on identity management.

- In March 2007, the RDTF received a briefing on the International Telecommunication Union Telecommunication Standardization Sector's focus group on identity management. Following the briefing, task force members discussed potential opportunities for collaboration on identity management issues.
- In April 2007, the RDTF received a briefing on the NCS Technology and Programs Division identity management activities. During the briefing, the NCS highlighted three technical identity management challenges that need to be addressed: (1) integration of all identity management databases; (2) privacy for users; and (3) accounting mechanisms.
- In June 2007, the RDTF received a briefing on the outcomes of the Defense Science Board's task force on biometrics. The biometrics task force identified the following recommendations: (1) establish formal "functional advocacy" for biometrics; (2) move support toward a singular biometrics data architecture within and across the national security sector of Government; (3) consider privacy in system design and architecture planning; (4) support migration of scope from "biometrics" to "identity management;" and (5) develop threat models and security policies with the use of biometrics to enhance rigor of security investigations.

The RDTF also developed an identity management definition discussion document for NSTAC and RDTF purposes. Within this document, the RDTF describes identity management, in the context of a networked system of computers and electronic communications devices, as the "process of managing credentials through their life cycle." Additionally, the RDTF describes an identity management system as a "system comprised of organization(s), people, policies and applicable laws, operational procedures and practices, as well as the tools and infrastructure employed in the identity management process."

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 2007 by:

- Drafting a high-level NSTAC messaging document tying together the various NSTAC initiatives and successes for the purpose of stakeholder outreach;
- Preparing for the 2007 Fall IES Offsite;
- Updating the NSTAC Video;
- Drafting an NSTAC key terms glossary for use as a quick reference guide for NSTAC related terms;
- Providing briefings on NSTAC reports and recommendations to key stakeholders, including meetings with several agencies in the EOP; and
- Participating in several conferences to raise the awareness of the NSTAC, including:
    - The 2006 Military Communications Conference;
    - The 2007 Committee on National Security Systems Conference;
    - AFCEA Canada Conference; and
    - The AFCEA Executive Breakfast Series.

NCS Issuances

Issuances or Revisions Pending during FY 2007

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:

- NCS Manual 3-10-1, *Required Minimum Continuity Communications Capabilities*; (must be published by September 25, 2007).
- 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).

The following issuance was issued by OSTP:

- NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* (issued by OSTP on July 25, 2007).

HSPD-7 Coordinating Councils

The Communications Sector Coordinating Council (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. Working together, the CSCC and CGCC finalized the Communications Sector-Specific Plan (CSSP) in December 2006 (published in May 2007). The CSSP outlines the process for risk management in the Communications Sector, including infrastructure identification, risk assessments, protective programs, performance measurement, and research and development.

In the first half of 2007, the CSCC and CGCC established a steering committee and the CSSP Implementation Working Group to direct the implementation of the CSSP and carry out the National Sector Risk Assessment (NSRA). The CSSP Implementation Working Group first developed the methodology to perform the NSRA, including architectural elements that will be assessed. The working group then began working closely with subject matter experts to conduct the risk assessment, which is anticipated to be complete in early 2008. The results of the NSRA will help guide the priorities of the CSCC and CGCC and may lead to the augmentation of current risk mitigation efforts, or the development of new protective programs.

Over the last year, the CSCC was successful in expanding its membership to include representatives from the satellite, cable and broadcast sectors. These entities have supplied the CSCC the ability to capture issues of concern across the entire sector. Expanding the scope of the CSCC was essential to be able to represent all of the different aspects of the sector, which is especially important when conducting the NSRA.

Independent of the CSSP efforts, the CSCC collaborated with the Banking and Finance sector on a network congestion study to determine the impact that increased telework may have on the network in the event of a pandemic flu. Some of the expected outcomes of the study include the identification of possible mitigation tools and the awareness of sector preparedness and capabilities. The CSCC also established a State and Local Working Group, which is focusing on three issues: access to disaster areas for purposes of recovery and service reactivation, protocols for shutdown of wireless networks, and Sector involvement in State and local fusion centers.

NCS Communications and External Affairs

The NCS–through coordination with the Department of Homeland Security's Office of Public Affairs–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 National Protection and Programs 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. Inquiries focused on NSTAC, the National Coordinating Center for Telecommunications and its Communications ISAC; WPS, GETS, and TSP programs; the SHARES High Frequency 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 National Protection and Programs Directorate and the CS&C Branch dealing with external affairs activities.

Even though information services for the NCS personnel are hosted on two different computer networks (DHS and DISA), the NCS continues to keep its employees informed and DHS internal communications issues. Those assigned to DHS facilities receive much of their DHS information the "DHS-ALL" distribution maintained by the Department. This includes the weekly "DHS Today," press releases and fact sheets, and through DHS Online–the department's internal web site. However, the remaining NCS members (about 30 percent) at the DISA compound cannot access DHS Online from their personal computers and must 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 both the DHS CS&C External Affairs Director and the DHS National Protection and Programs Directorate communications director before being released by the department.

Outreach

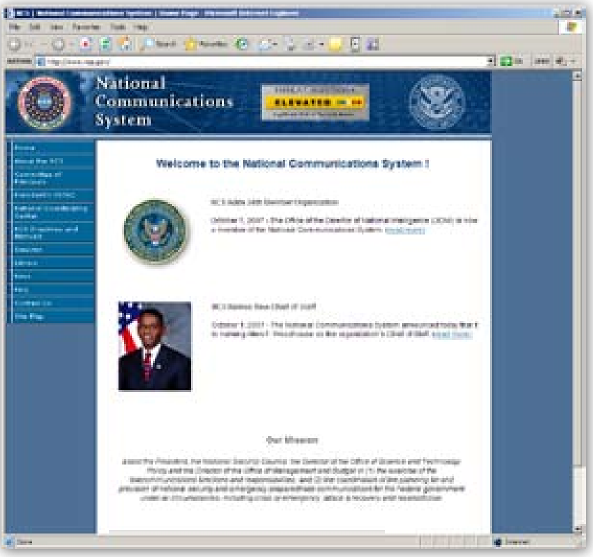
The NCS continues to spearhead an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and

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 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.

Aiding considerably in the outreach efforts are the five GETS/WPS Regional Outreach Coordinators and the three NCS Regional Emergency Communications Coordinators who address NS/EP communications issues at the State, regional and local areas. The eight outreach coordinators travel throughout the year to promote NCS priority communications programs, provide guidance to local government officials on the Federal Government involvement for ESF-2 (Communications) of the NRF, and participate in local, regional and national-level exercises designed to test emergency communications readiness.

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 and information about NCS programs and NSTAC activities, as well as online versions of NCS and NSTAC publications. The NCS also continues to work with DHS to show an NCS presence on the Department's own public site (*http://www.dhs.gov*), and in upgrading DHS Interactive (extranet) and DHSOnline (intranet).



Footnotes

1. Lockheed Martin Planning Letter (PL)- PL-NANP-172 dated 26 April 1999, "710 Numbering Plan Area (NPA) for the U.S. Government"

2. NSC Minutes from October 5, 2001 Meeting on Selected NS/EP Telecommunications Projects, October 9, 2001

3. 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)

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

5. 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

6. 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

IV

NS/EP Telecommunications Support and Activities of Member Organizations

Department of State (DOS)

NS/EP Telecommunications Mission

Secure Voice Program

The Department continues its Operations and Maintenance phase of the Secure Terminal Equipment (STE) program in fiscal year (FY) 2007. All Secure Telephone Units (STU) have been recalled from the field for destruction or transfer to the National Security Agency (NSA). The Department currently has 4891 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 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. The program has acquired engineering models of secure VoIP instruments for in-house engineering testing. The program continues to sponsor the Secure Voice Products Community of Interest Group (SVP-COI) to address the technical and other factors associated which will provide the Department a secure VoIP solution.

Anti-Virus Program

The Department's AntiVirus Program has detected and eradicated more than **1,211,303** viruses and blocked an all time record high of **122,958,602** spam messages so far in FY 2007. Robust network design, perimeter and desktop anti-virus tools have resulted in a very successful program. In an effort to provide security awareness to the end users and to prevent unknowingly introduction of malicious code, nearly **24,826** home use anti-virus software CDs have been distributed. This proactive measure controls virus incidents from emails or documents prepared by employees at home. The AntiVirus Program is currently performing a Symantec AntiVirus Corporate Edition (SAVCE) v.10.1 Pilot Program. This pilot currently has **2,754** systems participating. The AntiVirus Staff is also evaluating new state of the art perimeter appliance and software to replace the current scanning technology. Together, this Secure AntiVirus Equipment Refresh (SAVER) will bring the Department scanning technology up to date, while constituting a cost savings.

Communication Security (COMSEC) Modernization

The Department is continuing its effort to modernize its national security encryption systems by using the NSA certified Inline Network Encryption (INE) devices, (for example, KG-235s, KG-75s, and KG-175s). These new devices replace our aging serial based encryption systems with internet protocol (IP) 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 State Messaging Archive Retrieval Toolset (SMART) and Internet Virtual Private Network (VPN) programs, the INEs will provide the Department a gateway into the Department of Defense (DOD) sponsored Global Information Grid (GIG) providing state of the art real time interagency secure communications of classified information. The program completed the worldwide deployment of the KG 235 software version 3.1 which will provide the capability to push future software releases remotely *via* the network.

The Department has implemented the NSA mandated Electronic Key Management System (EKMS). The Department's primary communications hub, Beltsville Management Center (BMC), 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 (EUR), Near Eastern Asia (NEA), and East Asia and Pacific (EAP), and Western Hemisphere (WHA) regions and is being successfully utilized to encrypt their command and control data. The EKMS program has successfully piloted the distribution of "black" electronic keymat over the existing Department of State network infrastructure. This will provide the capability to distribute keying material in near real time without the security risks and time associated with physical keymat distributed and the Diplomatic pouch system.

Communication Security (Public Key Infrastructure)

The Department is currently operating a Public Key Infrastructure (PKI) at the high assurance level as outlined by the Federal PKI Policy Authority (FPKIPA). Working as partners, the Information Resource Management (IRM) and Diplomatic Security (DS) Bureaus have issued more than 35,000 Smartcard IDs to employees for building access and logon to the Department's Sensitive But Unclassified (SBU) system. PKI functionality has been installed on over 17,000 domestic workstations, and over 18,000 workstations overseas. Projected completion for initial deployment is planned for the end of FY 2009. The FPKIPA has cross-certified the Department's X.500 directory-based PKI and has allowed it to connect to the Federal Bridge Certificate Authority (FBCA) at the high assurance level. Efforts are currently underway to receive an additional cross-certification at the high assurance level for the Active Directory PKI. The Department's PKI user base of more than 35,000 has the ability to securely exchange digitally signed and/or encrypted SBU information with more than 10 federal agencies, the State of Illinois, and several non-government entities and certificate providers. The Department also uses PKI to secure its websites, update mobile code, patch applications, and provide access to a growing number of applications. It also provides support for smartcard-based access to the Department of Justice, whose Bureau of Citizenship and Immigration Services (BCIS) has 103 sites around the country. BCIS estimates that PKI services provided by the Department of State have saved taxpayers more than $800,000 annually. In addition, the PKI program actively supports the ePassport initiative spearheaded by the Consular Affairs Bureau. This initiative, enabled through the Machine Readable Travel Document (MRTD) system, digitally signs the new ePassport so that U.S. immigration officials can verify that the passports presented to them are authentic and have not been tampered with. In the FY 2007 timeframe, this system will produce approximately 10 million US passports. As the MRTD system expands to passport offices nationwide, this figure is expected to grow exponentially. The Department continues its implementation of the Biometric Logical Access Development and Execution (BLADE) program. This application is coupled with the Department's PKI and allows users to logon to the unclassified system with only a scan of their finger and no password. This program improves system security by increasing accountability in system use and eliminating password sharing among users. Biometric logon is moving forward in several domestic offices and is currently in use at 31 overseas locations. BLADE will be an ongoing component of new overseas deployment efforts. To conclude, the PKI Office plays a key role in supporting the Personal Identity Verification (PIV) program, which was mandated for all federal agencies by Homeland Security Presidential Directive (HSPD) 12. The PIV PKI authenticates and verifies all Department of State employees by digitally signing all new employee identification badges.

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 the 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. The success of this program continues to grow, 149 foreign SVDC installations out of 250 possible locations. The SVDC Program Office continues to explore opportunities to expand and to improve the technologies and capabilities of this program.

Technical Security and Safeguards (TSS)

Responding to the new security vulnerabilities from the reality of the global IT production, the Department employs dynamic Defensive Technical Counter-Intelligence (DTCI) methods to provide technical security and safeguards (TSS) for the Department's Foreign Service posts and tenant agencies. These methods provide cost-effective, life-cycle risk management for technical integrity of IT equipment used inside the Controlled Access Area (CAA) and ensure the Department's IT security in a multi-faceted multi-cultural business environment. Coordination between the Department's IRM, A and DS Bureaus provide valuable information on new technology advancements to identify products that meet the requirements of the Foreign Affairs Community and the Intelligence Community's (IC) operational needs while ensuring that security is incorporated. Among the programs supported by the TSS initiatives are: the Department's interagency collaboration efforts, the Secure Voice Program, the Secure Video Program, COMSEC Modernization, Secure Video and Data Collaboration, and the GITIM Program.

Domestic Radio Program

The Department of State's domestic radio program supports twenty-four Bureau of Diplomatic Security Service (DSS) 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 Department of State has recently completed an upgrade of all domestic Land Mobile Radio systems to comply with the new National Telecommunications and Information Administration narrow-banding requirements. The Department of State's Radio Program office is currently implementing a project plan for the migration of all domestic Land Mobile Radio systems from Data Encryption Standard (DES) to Advance Encryption Standard (AES).

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 (NSDD-38), the Department of State owns and operates Land Mobile Radio and High Frequency (HF) radio systems at two hundred and sixty overseas United States diplomatic missions. These systems are designed to support citizen services, security, and emergency activities of the individual diplomatic missions. The Department of State's Radio Program office is currently implementing a project plan for the migration of all overseas Land Mobile Radio systems from DES to AES.

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. The GITM will complete the initial four-year life-cycle refresh in FY 2007. Planning has begun for the next refresh cycle starting in FY 2008. GITM modernizes existing LANs using emerging technologies to keep pace with new business requirements, not just replacement of existing equipment. In FY 2007 alone, 167 domestic and overseas LANs will be modernized. 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.

NS/EP Telecommunications Mission

The 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 (TSP) program service are summarized as follows:

- Promote prosperous U.S. and World economics;
- Promote a stable U.S. and World economy;
- Manage the U.S. Government's finances effectively;
- Maintain, manage and preserve the economic and financial management institutions of the United States, including all monetary, credit, and financial systems;
- Serve as one of the principal economic advisors to the President;
- Perform international economic and monetary control as it pertains to the well-being of the Nation;
- Manufacture currency, coins, and stamps; 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). 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 serves as a member of the Federal CIO Council and is responsible for ensuring the deployment of an enduring telecommunications capability and associated E-government application services for maximizing cross-functional department integration between and among the Federal Departments of the U.S. Government. In this role, the Treasury OCIO guides, directs and develops information technology (IT) management policies, standards, practices, and procedures for enabling the financial business functions of the U.S. Government.

Ongoing NS/EP Telecommunications Activities include:

Treasury Communications System (TCS)

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

Security Operations Center (TCS-SOC)

Fiscal Year (FY) 2007 was an exceptional year for the TCS Computer Security Operation Center (TCS SOC). The staff continued to provide cyber security monitoring for the Treasury wide area network, numerous Treasury enterprise applications, and their supported Bureaus. TCS SOC staff continued to define and refine procedures, policies, and infrastructure for security monitoring and incident response. The TCS Security staff provided full network security monitoring and reporting support to the Office of the Controller of the Currency (OCC), the Bureau of Public Debt (BPD), and Departmental Offices (DO). This support includes enterprise systems located at the Qwest Cyber Center, Community Development Financial Institution (CDFI), and Treasury HR Connect. The TCS SOC successfully completed a significant architecture upgrade, improving the operational efficiency, scalability, and operationally protective presence within the infrastructure, ensuring maximum monitoring and response coverage without increasing resources.

To ensure the security of Treasury's extended applications hosted at other contractor facilities, the TCS SOC deployed host- and network-based security monitoring and vulnerability management capabilities at key contractor facilities where critical Treasury applications are hosted, thus ensuring disparately managed systems are collectively monitored and operationally secure.

At a higher level, TCS SOC continued to forge relationships with DHS *via* US-CERT's Government Forum of Incident Response and Security Teams (GFIRST) community. Working closely in partnership with US-CERT and other Federal and Department of Defense organizations, TCS achieved a more defined mission focus and committed resources to thwarting numerous classified threats that posed significant risk to the Federal Government. Significant investments were made throughout FY 2007 including "network flow" analysis, continued utilization and upgrades of EINSTEIN data (conducted in joint partnership with the Department of Homeland Security [DHS]), raw packet capture and analysis, and development of a forensic recovery and analysis capability.

The TCS-SOC deployed new technology, processes, and procedures across the program to meet the ever-expanding set of compliance standards required to process Treasury data. TCS incident response procedures have been expanded to cover DO HQ operations, HR Connect and all Enterprise Services. The TCS SOC recently completed a first phase analysis aimed at defining a strategy to meet current configuration management mandates. The final solution is targeted to be in place by the first quarter of 2008.

Another significant effort during the second quarter of FY 2007 was the TCS SOC staff's participation in a successful TCS Disaster Recovery (DR) exercise where all Treasury Bureaus were transitioned to the alternate operating facility (AOF) for a 24 hour period. TCS fully demonstrated the ability to operate in disaster recovery mode, and the TCS SOC staff demonstrated the ability to ensure continuous monitoring and incident response capability for the infrastructure in a DR situation.

Certification and Accreditation

TCS' Security Assurance Program continued to make great strides in keeping its systems, and those of its Bureaus, compliant with Federal and Treasury certification and accreditation (C&A) policies and procedures. By maintaining assurances that its infrastructure and networks remained secure and protected, TCS continued to provide and enhance its protective environment with a security posture conducive to processing sensitive-but-unclassified information.

In FY 2007, the TCS Security Assurance Program maintained its own accredited environment by re-certifying and re-accrediting the TCS infrastructure, and ensuring that new services or changes to the general support system or major applications go through the complete C&A process. In addition, the TCS Security Assurance Program provided C&A expertise by conducting and creating C&A packages for other Treasury Bureaus and Federal agencies.

The TCS Security Assurance Program performed annual updates to the system security plans (SSP) of enterprise applications that did not already have an updated SSP and performed continuous monitoring testing for all thirteen enterprise applications. All POA&M items from the previous FISMA year that were resolved were also tested. The annual audit of the Treasury Public Key Infrastructure (PKI) system was performed. The Security Assurance Program is in the process of certifying the Budget Formulation and Execution Manager (BFEM) system hosted at EPA, and anticipates certifying the Fiscal Projections System hosted at BPD.

The TCS Security Assurance Program is preparing to meet the requirements of the forthcoming National Institute of Standards and Technology Special Publications (NIST SP) 800-53A by creating test procedures for all NIST SP 800-53 controls in the NIST recommended format.

Digital Telecommunications Switching System (DTS)

During FY 2007, the DTS Program continued to carry out its wide ranging responsibilities, providing secure access to Treasury's complex voice telecommunications infrastructure within local Treasury sites in the Washington, D.C. area, sites in suburban Maryland and Northern Virginia, and the physical interfaces to other telecommunications programs and services. The DTS network provided voice, data, and video services *via* analog, Integrated Services Digital Network (ISDN), Basic Rate Interface (BRI), and ISDN Primary Rate Interface (PRI) services to the Treasury user community.

DTS IT Security

The information transmitted and generated by DTS, and the DTS-specific information in Verizon's operations, administration, maintenance, and provisioning support systems are considered sensitive but unclassified (SBU). Treasury developed the DTS Security Program to meet all essential 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;
- DTS-specific policies and procedures set forth in the DTS System Security and Authorization Agreement (SSAA) and its appendices.

The DTS network met Treasury's original requirements for the Authority to Operate (ATO) in December 2003. The DTS SSP continuously defines the necessary actions for which Treasury is responsible and provides an overarching security framework and objectives. The DTS System Security Authorization Agreement and its appendices describe security measures that are currently in place, or that the DTS Program Management Office (PMO) and Verizon plan to implement to ensure the confidentiality, integrity, and availability of DTS services and to fulfill contract requirements (for example, Government requirements such as FISMA, OMB A-130, and guidance from the 800 series of NIST Special Publications). Verizon's documentation complements the DTS SSP by describing how Verizon implements Treasury's DTS security framework and achieves the Department's security objectives for the enterprise voice network.

Treasury Emergency Management Center Capability

As part of Treasury's Continuity of Operations Plan (COOP), Treasury Headquarters established emergency management centers (EMC's) for responding and reacting to crises, disasters and emergencies. The local EMC is a "warm site" that has equipment in place and is tested at least once a week. A second EMC is located within the Department of the Treasury's primary COOP location; this is a cold site. Both sites are fully integrated with the TCS 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 new center will be improved and modernized based on changes in the Treasury Department's operating principles and practices and in the associated information technology systems. The new center will accommodate changes that will enhance business management information systems. Both Treasury EMCs (local and COOP) are capable of secure voice, facsimile, and SIPRNet communications as well as unclassified voice, facsimile, mobile satellite, 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 (OEP). The issuance of Government Emergency Telecommunications Services (GETS) cards continued to increase in FY 2007. All Successors to the Secretary of the Treasury have Wireless Priority Service (WPS) on their cellular telephones, and WPS has been made available to specific Departmental Offices as well as Treasury Bureaus. The acquisition of a new, expanded 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 FY 2007 and FY 2008 are:

- A larger, modernized Treasury local EMC with associated system monitoring and management tools;
- Additional contingency office space for senior Treasury leadership and their core emergency staff equipped with secure and unclassified equipment;
- Additional contingency communications capability;
    - Treasury is in the process of installing, testing, and implement a Treasury high frequency radio network in support of a FPC-65 requirement for emergency back up communications
    - High frequency (HF) radios have been procured and installed at Treasury Headquarters and the Treasury Headquarters COOP site. HF radios are being installed at all Bureau COOP sites and selected Bureau headquarters locations
    - This network will facilitate communications between Treasury headquarters and Bureau COOP sites at the secure level, as well as between the Treasury headquarters COOP site and FEMA at the TS level
- Additional GETS Cards and PINS pre-positioned at all Treasury alternate operating facilities (AOF's) and EMC's so that cards can be transferred to Treasury staff to respond to immediate crises;

- Secure cell phones for senior staff (Secretary Successors) of Treasury Bureaus
- WPS phones for senior staff of Treasury Bureaus;
- Secure and non-secure video teleconferencing capability for the primary and alternate Treasury Headquarters COOP site;
    - Full installation and quarterly testing of unclassified voice, secure voice and secure facsimile for its primary COOP site and EMC;
- Acquisition of fixed-station satellite communications for the primary Treasury COOP site; and
    - Treasury plans to equip its newer, expanded EMC with the same capability as soon as it is occupied and operational
- 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 exercises Forward Challenge 2006 and Forward Challenge 2007.

Support for the Federal Public Key Infrastructure Development

The Department of Treasury continued 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 employees and contractors, and to date it has had active participation by 11 of its 12 Bureaus. For this and other reasons, Treasury's PKI will be a critical component in the General Service Administration's (GSA's) Personal Identity Verification (PIV) Managed Service Offering (MSO), as required by the Homeland Security Presidential Directive (HSPD) 12. Significant progress was made in FY 2007 to position Treasury's PKI components for integration with the HSPD-12 solution. Treasury, recognized as a leader in PKI, is working with GSA to assist other agencies with efforts to integrate solutions with the GSA MSO.

During FY 2007, Treasury continued to work with other agencies through the Federal PKI SSP program. Treasury's involvement in this program allows the Department to reduce its ongoing operation, policy, and management costs by offering digital credential services to partnering agencies and sharing its PKI resources. This approach has proven highly successful. Treasury continues to develop a successful partnership with the National Aeronautics and Space Administration (NASA) and is working with the Social Security Administration (SSA). 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 (FBCA) that supports conducting "trusted" business with member agencies *via* a common PKI architecture. Additionally, Treasury accomplished policy and technical efforts to ensure that its PKI is aligned with the goals of the Federal Common Policy. This alignment is important to Treasury's role as an issuer of PIV certificates.

Treasury continues to expand 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. Treasury's critical Certification Authority (CA) hosts have undergone significant recalibration over the past year; this effort will continue over the coming months to meet PIV integration objectives.

Treasury continues its efforts with GSA 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. To address its internal business community, in FY 2007 Treasury has increased its efforts to promote the benefits of its PKI technology. Value-focused promotional material has been developed and will be distributed to Treasury Bureau business owners in the near future.

Public Safety/Law Enforcement Wireless Activities

The Department of the Treasury's Wireless Program Office (WPO) assists, coordinates, and serves as the primary technical, operational, and managerial advisor and executor for Department-wide wireless communications, specifically land mobile radios (LMR). The WPO has been successful in increasing its presence throughout the Department and across other Federal entities. For example, the WPO established the WPO Governance Board to provide Treasury Bureaus with a forum to coordinate wireless activities and discuss wireless communication needs to meet the Bureaus' public safety and law enforcement missions. 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 LMR equipment to meet the narrowband and advanced encryption standard (AES) mandates.

In FY 2007, the WPO assisted Treasury Bureaus in procuring equipment, including the AES upgrade software for subscriber units and encryption key loaders to secure the transmission of sensitive law enforcement related information (such as, tax payer information). Additionally, the Internal Revenue Service—Criminal Investigation (IRS-CI) upgraded communications interoperability and encryption capabilities in several field offices. IRS-CI has begun to enhance interoperable communications capabilities by programming subscriber units with federal interoperability channels identified by the Department of Justice's 25 Cities Project.

Additionally, Treasury continues to participate in the Interdepartment Radio Advisory Committee (IRAC) and other Federal committees (for example, the Federal Partnership for Interoperable Communications [FPIC]). Treasury's presence and participation 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 (NTIA) narrowband mandate, as well as participating in activities related to the Presidential Determination on Improving Spectrum Management in the 21st Century.

Treasury has increased participation within the IWN Program (a partnership including Treasury, the Department of Justice, and the Department of Homeland Security) to implement a joint law enforcement voice and data network to meet 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 it remains up-to-date on rapidly evolving wireless technologies and standards and to address public safety and law enforcement activities in collaboration with other Federal law enforcement agencies.

In conjunction with participation in the IWN, the WPO is also in the process of developing an implementation roadmap that describes a unified approach to continue to upgrade Treasury Bureaus' current LMR systems. Once completed, these enhancements and modernization initiatives will allow Treasury to respond, operate, and function in a crisis, emergency, or national disaster more effectively.

Summary

FY 2007 NS/EP telecommunications activities contributed to providing a cost-effective, technologically sound telecommunications infrastructure for executing the Department of the Treasury's essential functions.

The TCS Program provided a secure, encrypted nationwide business communications infrastructure for Treasury Headquarters and its associated Bureaus.

The TCS Security Operations Center provided cyber security monitoring for the Treasury-wide network, successfully completed a significant architecture upgrade, deployed host- and network-based security monitoring and vulnerability management capabilities at key hosting facilities, implemented new processes to meet ever-expanding compliance requirements, and continued to forge relationships with DHS US-CERT and other federal and Defense organizations.

The TCS Security Assurance Program continued to make great strides in keeping its systems, as well as Bureau systems, compliant with certification and accreditation policies and procedures.

The DTS Program continued to provide secure access to Treasury's complex voice telecommunications infrastructure in the Washington, D.C. metropolitan area. Planned activities in FY 2008 include increased use of TSP to identify critical infrastructure on this program.

The Treasury Office of Emergency Preparedness saw an increase in GETS cards in FY 2007 as it supported continuity of operations requirements and made plans for a newer, larger, more capable local emergency management center.

Treasury continued supporting development of the Federal PKI infrastructure and made significant progress in positioning Treasury's PKI components for integration with the GSA's PIV MSO.

The Wireless Program Office assisted Treasury Bureaus in upgrading their land mobile radio equipment and assisted in the procurement of equipment to secure the transmission of sensitive law enforcement related information (for example, tax payer information). In addition, the WPO represented Treasury in IRAC, FPIC, and other key groups to ensure effective management of Treasury's spectral assets.

NS/EP Telecommunications Mission

Under the provisions of Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* 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 (OSD), the military departments and services within them, the combatant commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Networks and Information Integration (NII)/DOD Chief Information Officer (CIO).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD HD&ASA) and the ASD(NII)/DOD CIO.

Current/Ongoing NS/EP Telecommunications Activities

Critical Infrastructure Protection

The Deputy Secretary of Defense (DSD) 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&ASA) serves as the principal senior advisor to the SECDEF 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).

A key accomplishment this past year was the approval and publication of the *Defense Industrial Base Critical Infrastructure and Key Resources Sector Specific Plan (DIB SSP)*. The DIB SSP, developed in collaboration with industry and government partners, provides a framework and roadmap to ensure the ability of the DIB to support DOD missions and eliminate unacceptable risk to national security through informed infrastructure risk-management decisions. The DIB SSP outlines the DOD approach to executing SSA and forms an annex to the *National Infrastructure Protection Plan* published in 2006 by the Department of Homeland Security (DHS). It complements other DOD critical infrastructure policy.

DOD has also initiated action to form Defense Security Information Exchanges (DSIEs) patterned after the extant National Security Information Exchanges (NSIE). In 1991, the NSIEs were formed at the joint request of the National Communications Systems (NCS) and the President's National Security Telecommunications Advisory Committee (NSTAC). One NSIE was limited to government members, while the other was strictly for industry counterparts. The intent was to develop organizations that would enable the sharing of information to counter the "hacker" threat to the nation's critical telecommunications infrastructure. Today, these organizations have grown to become effective information sharing vehicles. The current NSIE organizations not only comprise telecommunications companies and their government counterparts, they also include 65% of the defense contractors and DOD agencies, such as U.S. Strategic Command, U.S. Northern Command, Joint Task Force-Global Network Operations (JTF-GNO), and the Defense Intelligence Agency. In an effort to counter the growing threat from cyber attacks unique to the defense industry, members of the two NSIE organizations have began discussions concerning the formation of DSIEs. The new DSIEs would follow the same concept, that is there should be one government DSIE and one industry DSIE. The intent is for the two organizations to co-exist with each other and conduct joint meetings to share information that would benefit the protection of the critical infrastructure and key resources (CI/KR) of the DOD.

With the formation of the NSIE, there was a recognized need for real-time information sharing along with a higher level strategic planning body. Although a strategic body that meets at least bi-monthly in the new DSIEs is desired, member organizations will need to engage the subject matter experts within their respective organizations and share threat information immediately through a trusted secure channel.

Most recently, DOD has partnered with DHS and the private sector to form a DIB Information Assurance (IA) Working Group of the DIB Critical Infrastructure Protection Advisory Committee (CIPAC). This Working Group will operate under the National Infrastrucutre Protection Plan to assess vulnerabilities of networks in the DIB and to share threat information and network best practices.

Crisis Management system (CMS)

CMS is a secure, dedicated, high performance network that provides Net-Centric exchange of high-interest, time-sensitive information among the highest level of government decision makers. CMS, owned and operated by the National Security Council (NSC), extends the White House Situation Room point of presence to approximately 100 fixed and deployed locations worldwide. It is the President's hands-on system of choice for day-to-day and crisis management.

CMS is comprised primarily of real-time interactive applications operating over a dedicated Internet Protocol (IP) backbone. The core CMS applications are the Secure Video Teleconferencing System (SVTS), the Crisis Management Network (CMN), the Executive IP Phone System, the National Operational Intelligence Watch Officers Network (NOIWON), and the Big Shot Desktop Video Network. There are several NSC Network Operations Centers available 24X7 that provide control technical, security, and system monitoring services such as video and phone call manager, system maintenance, red and black HP OpenView monitoring, and an administrative conference meeting maker.

The tremendous growth in CMS services and sites is in direct response to a post-9/11 world. CMS provides a number of entry points for remote users particularly those that are not IP continuous presence subscribers, and who will "dial-in" through a variety of media into the network. The rendezvous point or "Meet Me" interface allows the gateways to interface large fixed network sites to contingency or mobile sites. The new digital gateways now being deployed are designed to respond to the growing number of contingency sites, most of whom will require dial-in capability. These gateways can support large numbers of participants in a single call. Additional participants can be placed in a virtual waiting room and invited to join conferences as required. In the not too distant future, CMS will introduce High Definition Video Teleconferencing to key users and will dramatically expand the Executive IP Phone Network including additional interfaces to other voice networks. CMS will also offer expanded collaboration in a presentation mode.

Net-Centric Operating Environment

In 2007, ASD NII/DOD CIO, in coordination with the Joint Staff, 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.

Global Information Grid Mission Assurance (GIG-MA)

DOD has established the GIG Mission Assurance tiger team to review the mission assurance posture of the GIG and its ability to support DOD mission essential functions when faced with attacks by sophisticated adversaries.

Joint Task Force-Global Network Operations (JTF-GNO)

JTF-GNO leads and directs continuous Enterprise Services Management/Network Management (ESM/NM), Information Assurance/Computer and Network Defense (IA/CND), throughout the GIG. JTF-GNO provides Situational Awareness (SA) of the GIG through the Network Common Operational Picture (NETCOP). It also 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 (NCCC)

DOD continued its support to DHS and the National Command and Coordination Capability (NCCC) effort. NCCC is the 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.

Exercise Ardent Sentry 2006

A major focus of Exercise Ardent Sentry—Northern Edge 2007 was to test crisis-response coordination between federally controlled military forces and National Guard units that come under the command of state governors. The exercise, directed by the Chairman of the Joint Chiefs of Staff, was co-sponsored by U.S. Northern Command and included participation by the U.S. North American Aerospace Defense Command, DHS and the Canadian armed forces.

This year's Ardent Sentry—Northern Edge 2007 exercise, the biggest yet, featured a nuclear-weapon explosion scenario that involved deployment of more than 2,000 active-duty troops and almost 1,000 Guard members to Camp Atterbury and the Muscatatuck Urban Training Area in Indiana. This deployment included a Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Consequence Force.

The exercise also addressed the capabilities of the Incident Command System during operations in Fairbanks, Alaska. This unified command and control system is designed to help in domestic incident management activities and included military communications that are networked to local, state, Federal, and private organization systems.

The Committee on National Security Systems (CNSS)

DOD is the Executive Agent for the 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.

CNSS Policy No. 21 (March 2007)

Policy No. 21 is the central policy to coordinate and clarify the development and integration of IA components of enterprise architectures across the CNSS community, focusing on the Federal Enterprise Architecture (FEA) as the framework to make this integration possible. It enumerates responsibilities and requirements for Federal Departments and Agencies in their development of collaborative, integrated IA components of enterprise architectures that handle National Security Information.

CNSS Policy No. 19 (February 2007)

This policy provides governance for the procurement of IP encryption products for fiscal year (FY) 2009 and beyond. The intent of this policy is to ensure that all IP products procured after FY 2008 are compliant with the appropriate version of the High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification (IS). The U.S. Government's communication infrastructure is becoming more reliant upon network communications. Legacy government owned and operated circuit switched communications channels are being replaced with packet switched infrastructures. National Security Systems (NSS) users are also starting to leverage commercial and foreign public IP infrastructures. These networks will provide a converged transport infrastructure for data applications, as well as real-time services. As this transition occurs, legacy link encryptors must be incrementally replaced with network encryption products. The interoperability of network-layer encryption devices is vital to enabling net-centric capabilities, while maintaining end-to-end protection of NSS traffic. The HAIPE IS defines requirements for a modular suite of traffic protection, networking, and management features that provide secure interoperability between users, content repositories, and net-centric enterprise services.

National Security Presidential Directive 51/Homeland Security Presidential Directive 20, National Continuity Policy. DOD, in coordination with the Department of Homeland Security, is tasked to provide secure, integrated Continuity of Government communication's capabilities. The document articulates a significant change from the Cold War posture and acknowledges a new view of the world in terms of no-notice, all-hazards scenarios and capabilities required to support National Essential Functions.

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 (ATF), Bureau of Prisons, Drug Enforcement Administration (DEA), the 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 was substantially completed in July 2007 with the remaining sites to complete transition by December 2007. The FBI maintains separate secure network facilities.

Telecommunications Staff Organization

The Deputy Chief Information Officer, Enterprise Services Staff operates and manages DOJ's consolidated data transport network. The law enforcement message processing system and the Telecommunications Services Center are managed by the Deputy Chief Information Officer (CIO), Operations Services Staff (OSS). 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 (SIPRNET), Justice Automated Message System and JWICS. The FBI continues to administer their communication security program. DEA 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 (NCS) Committee of Principals (COP);
- OSS provides representation for DOJ on the NCS 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 national security and emergency preparedness support in their normal duties (for example, remote security alarm sensing; 911 and enhanced 911 services in several Midwestern states; and for environmental and emergency response services for cleanup of waste at clandestine drug laboratories.); and
- Additionally, the department is an active participant in the Government Emergency Telecommunications Service Program, the Wireless Priority Service Program, the TSP Program, and the Shared Resources High Frequency Radio Program.

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 U.S. 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. 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 FTS2001 contract. We are completing consolidation of our bureau backbone data communications networks to a single Department-wide Multi Protocol Label Switched based architecture with enhanced network security functionality. We have 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. STE secure telephones are used to support DOI national security programs and HF 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

In 2007 we signed separate memorandums of understanding with the states of Montana and Wyoming for interoperability 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. In addition DOI met with the National Governors Association and National Association of Counties to coordinate public safety interoperability. These agreements significantly improve interoperability between federal, state, local and tribal public safety radio users.

DOI is in the final phase of establishing a jointly 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 deployment is in the optimization phase. This included removing network address translation at the interior of the network, completing multi protocol label switching deployment, and transferring all network devices to managed services. In 2006 DOI received and reviewed the National Communications System (NCS) provided FTS2001 Traffic Analysis as part of the ongoing effort to provide critical infrastructure analyses for the NCS Committee of Principals. The findings of this excellent analysis are now being used to identify carrier diversity requirements for mission critical sites.

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 for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment; inspect livestock, poultry, and other products to ensure the safety and wholesomeness of food; and, manage the protection and use of national forests, national grasslands, wilderness areas, and other public lands and facilities under USDA jurisdiction. This includes managing wild land fire control activities in coordination with state and local authorities.

Current/Ongoing NS/EP Telecommunications Activities

The USDA continues with its role in the NS/EP Priority Telecommunications, Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) Programs sponsored by the National Communications System (NCS). The USDA is currently maintaining, on average, 1,400 GETS accounts and approximately 260 WPS accounts. The Department has identified and trained primary and secondary TSP representatives for every USDA component agency and staff office.

The USDA Office of the Chief Information Officer's Telecommunications Services and Operations continues to work closely with the Office of Security Services to meet information technology requirements related to continuity of operations activities. This year USDA is completing the construction of a shared facility to provide component agencies with shared access to a secure network for internal and external communications. Additionally, USDA invested in secure satellite equipment and network services to demonstrate progress in meeting the NCS Directive 3-10.

NS/EP Partnership Activities

The Departments of the Interior (DOI) and USDA maintain telecommunication systems that enable the effective delivery of public safety services to citizens. With the increase in threats to national security, as well as the enormous capital investments involved with the establishment and continued operation of these networks, the Departments are working to identify options that reduce overhead and achieve technical interoperability. Additionally, USDA and DOI are seeking alternative methods to integrate business processes for more effective operations.

USDA made arrangements for five USDA representatives to take part in the National Response Plan, Emergency Support Function 2 (ESF-2) conference held in New Orleans during the month of June, and is planning to conduct an outreach to its thirty agencies to recruit additional telecommunications specialists as ESF-2 volunteers.

The NCS has partnered with USDA to warehouse a dedicated cache of fly-away kits for ESF-2 emergency operations at the National Interagency Fire Center (NIFC) in Boise, Idaho. NIFC also houses large caches of radio equipment and serves as the headquarters for wild land fire fighting personnel, who coordinate with federal, state and local personnel in performing joint emergency support operations.

USDA continues to support SAFECOM, one of the President's three top Electronic Government initiatives focused on interoperable public safety radio communications.

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 affects the daily lives of Americans in many ways. Examples include making it possible that weather reports are released and accessible by millions on a daily basis. Commerce facilitates technology that Americans use in the workplace, in industry, and at home every day. DOC supports the development, gathering and transmitting of information essential to competitive business, and makes possible the diversity of companies and goods found in America's (and the world's) marketplaces. Commerce also 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 (NOAA), National Telecommunications and Information Administration, Patent and Trademark Office, Technology Administration, National Institute of Standards and Technology, National Technical Information Service, and the Office of the Secretary.

The Department continues to support the efforts of various cross governmental organizations including the National Communications System 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.

Current/Ongoing NS/EP Telecommunications Activities

The following current/ongoing DOC activities support national security and emergency preparedness (NS/EP) objectives:

- 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 IP (VoIP), Private Branch Exchange (PBX), and other agency managed telecommunications services.

- The DOC is actively involved in Homeland Security initiatives and efforts to enhance preparedness with the necessary information technology equipment, software and hardware upgrades. The Department of Commerce Headquarters is located in the Herbert C. Hoover Building (HCHB) located in Washington D.C. The Commerce Office of Security located in the Headquarters facility manages and supports the Commerce Emergency Broadcast System (EBS) that sends pre-recorded or ad hoc messages to every Voice Over Internet Protocol telephone in the 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, the White House Visitors' Center, and the National Aquarium located in the Commerce headquarters building.

- To enhance our Continuity of Operation Planning, the Employee Notification System is fully operational today and is tested during each of the Federal government-wide Test Training and Exercises (TTX). The system automatically notifies all identified employees using any of several available means (for example, telephone, cell phone, pager, e-mail) within a pre-determined 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.

- NOAA has initiated a program that is referred to as "UrbaNet." in response to Congressional guidance to explore the utility of using local meteorological data in forecasting for urban areas. The first study was focused on the National Capital Region and involves the installation of monitoring stations within Washington, D.C. These stations collect and analyze meteorological data (including wind speed, direction and turbulence data) at frequent intervals to help define downwind areas of potential high risk. In so doing, DCNet is being used to help protect people from hazardous trace gases and particles dispersed in urban areas.

- The Department's Emergency Operation Center (EOC) uses the Plume Modeling system to track serious hazmat incidents (with accompanying toxic cloud release) in and around the metropolitan area. It is used by the EOC to develop information for senior Commerce officials to make tactical decisions on shelter-in-place or evacuation of the HCHB. The system operates using numerous NOAA sensors strategically located throughout the Washington, D.C. area. The Plume Modeling system provides information on plume directional feedback, times of travel to the targeted location, and the areas that would be affected in its path.

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 National Communications System services and programs, especially in light of recent hurricane disasters and post 9/11 security programs.

NS/EP Telecommunications Mission

The national security and emergency preparedness (NS/EP) mission of the Department of Health and Human Services (DHHS) is to provide the necessary strategic and technical capabilities to prepare for and respond to, public health emergencies across all hazards. This includes assisting internal and external stakeholders in obtaining sponsorship for various priority telecommunications programs, and assisting operating and staff divisions of DHHS with NS/EP requirements.

Current/Ongoing NS/EP Telecommunications Activities

Each core operating division of HHS is focused on developing and implementing the necessary strategies to provide for:

- Communications on Public Health issues within the Federal Government;
- Communications on Public Health issues with State and local Cooperators; and
- Communications on Public Health issues with Non-Governmental Organizations.

The National Disaster Medical System returned to DHHS early this year and Congress established the Office of the Assistant Secretary for Preparedness and Response (by passage of the Pandemic and All Hazards Preparedness Act). Current emphasis is on enhancing disaster communications during all hazards events.

Some of the areas include:

- Re-entry to the SHAred RESources (SHARES) High Frequency (HF) Radio Program. DHHS has HF communications installed at our headquarters building, various alternate facilities and field teams. The Center for Disease Control (CDC) and Prevention has the National Public Health Radio Network using HF to provide the CDC, state, territorial, and local health departments with wireless communications capability. This back up communications system utilizes specific radio channels within the high frequency radio spectrum.
- Government Emergency Telecommunications System (GETS) and Wireless Priority Service (WPS). Our goal is to ensure all NS/EP members in the Department have GETS cards and are trained on their use. DHHS continues to work with wireless contractors to activate WPS services. By connecting the on-boarding and exit procedures for staff with NS/EP roles, we hope to increase efficiency in card issuance and cancellation.
- Assisting the Health care industry with Critical Infrastructure protection and program support (including grants) through the Hospital Preparedness program. This includes working with the Federal Communications Commission to publicize available systems and best practices.
- Updating our cache of Land Mobile Radio equipment. DHHS is working with the Federal Emergency Management Agency to create one standard "code plug" or list of frequencies for use across the divisions. By adding the National Telecommunications and Information Administration and FCC approved interoperable frequencies to improve communications during a disaster.
- Updating Pre-Staged, truck based caches and ensuring that DHHS Incident Response Coordination Teams have adequate technical capabilities. The portable and mobile radios, repeaters and base stations across the very high frequency, ultra high frequency, and 800 Megahertz range, diesel generators, laptops, information technology equipment, such as switches, printers, peripherals, cellular phones, satellite phones and Cellular and Satellite Internet.
- Assist the Public Health Service with training team members in disaster communications. These teams staff Federal Medical Stations that provide special needs care on a long term basis.
- Continue implementation applicable portions of National Communications System Directive 3-10, such as Secure Satellite phones, Secure HF radio and GETS/WPS and Telecommunications Service Priority for all personnel and circuits involved with continuity of operations. In the areas where external sponsorship is required, such as classified data networks, work with partners to obtain sponsorship.

NS/EP Telecommunications

The Department's mission as outlined in the Department of Transportation (DOT) Strategic Plan, asserts that the Department will "serve the U.S. by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people." 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 of the Department is constant. We remain flexible to the ever expanding global economic environment. Products are manufactured using the raw materials in one area of the world and transported to be assembled in another and then shipped to their final destination to be used by the consumer.

Competitive international trade depends on transportation. Disruption of transportation systems jeopardizes public safety and disrupts Americas economic well being.

The success of our transportation system depends on its ability to function in the both the private and public sectors. The transportation system increasingly uses information technology to track the movement of commodities and ensure the deliverable arrives at it planned destination. Disruption of the transportation systems during these unsettled times will jeopardize the well being of our economy and population as a whole.

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 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, as previously reported, participates in the National Communications System (NCS) Committee of Principals 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 (GETS)

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. 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 2007 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.

The Department has completed its move into the new headquarters building. The development of the new infrastructure has followed the planned guidelines instituted during the moves inception. The route diversity programs that promote the concepts of redundancy have been followed in the planning and implementation phases to better control the communications network that is vital to the Department's mission.

NS/EP Telecommunications Mission

Department of Energy (DOE) Headquarters (HQ)

DOE participated in Exercise Pinnacle, the White House sponsored 2007 Continuity of Operations (COOP) Exercise, successfully testing the agency's ability to coordinate, develop and implement continuity of staff to alternate operating facilities in the event of an emergency in Washington D.C. DOE also completed a separate COOP exercise (March 2007) creating a point-to-point virtual private network over the Internet to an off site data storage/recovery location successfully testing network & security configurations in pushing DOE data. DOE implemented a project initiative for all DOE sites to review their Government Emergency Telecommunications System (GETS) card and Wireless Priority Service (WPS) requirements for Mission Critical Personnel. DOE increased the assignment of GETS cards over the previous year by 43%. GETS card testing increased 32% for the first six months of the 2007 calendar year versus 2006. The National Communications System (NCS) invited DOE to present its successful GETS/WPS Management and Implementation Processes and Procedures as a model to other user organizations at the NCS Quarterly User's Council Meeting in March 2007.

Richland Operations Office (RL)

RL developed and deployed mobile Wireless Wind and Solar Power Platform trailers for expanded surveillance coverage into radiation zones, eliminating the need for manned Tank Farm inspections and improving operational controls and radiation safety. Additionally, RL increased and enhanced the wireless footprint to support automation and business process improvements for various cleanup projects. RL established a new 911 telephone system which provides greater voice and data identification capabilities and qualifies the system as an E911 level Public Service Answering Point center. The new system enhances safety by providing the Patrol Operations Center with automatic number/identifier information when receiving emergency calls.

Oak Ridge Office (ORO)

ORO continues to move all reservation radio users over to the Wide Area Radio System currently with more than 3600 users. ORO installed a District 2 Homeland Security Net radio that operates on the 800 Megahertz Mutual Aid Channels and acts as a party line between all East Tennessee County Emergency Response Centers for dispersal of vital information during emergencies and disasters.

Savannah River Site (SRS)

SRS Site Communications began implementation of its P-Reactor communications system. This system when fully implemented will provide in house telephone, radio and SAS/PA capabilities *via* a distributed Voice of Internet Protocol cable/RF system. New equipment was installed as part of an SRS project to replace the 12 year old paging system infrastructure that supports approximately 9,000 site pagers - including the pagers for ERO, remote workers on site, on-call personnel, for security, fire groups, operations, and projects.

SRS completed a major upgrade to the South Carolina Relay Station. The Station Communications Redesign MICOM Replacement project involved the installation and configuration of new communications equipment expected to enhance the complex-wide communications network of the DOE/NNSA/Office of Secure Transportation's Transportation and Emergency Control Center. These infrastructure improvements were required to support the next generation of vehicle communications presently being deployed through out the NNSA/OST fleet.

Kansas City Plant (KCP)

DOE HQ acquired Frequency Authorization (FA) from the National Telecommunications and Information Administration to link DOE sites for emergency communication on the high frequency band of frequencies. NNSA sites, including KCP, have been issued FA's. KCP now has equipment installed that could provide communication with even more local public safety agencies.

Rocky Mountain Oilfield Testing Center (RMOTC)

RMOTC initiated a Calling Post Messaging System that is an automated emergency call out service. All DOE Managers are issued GETS cards to support emergency response/preparedness, and they participate in the GETS program quarterly practice calls.

NS/EP Telecommunications Mission

Deployable Communications

The Department of Veterans Affairs (VA) has designed, developed, and procured a standardized set of technologies and services to support emergency preparedness and response activities as well as day to day operations. These Very Small Aperture Terminal Satellite packages provide voice, video, and data network service in a single package that can be deployed to an affected area during a disaster. To extend their effectiveness, they are also used in day to day clinic operations when not supporting emergency preparedness activities. By leveraging a standard set of tools throughout the Department, VA staff can be sent in from anywhere across the country to setup and maintain the systems so that staff in the locally affected area can take care of their families if necessary.

Centralization of Systems

VA has made great progress towards the centralization of its information technology resources. This move to highly redundant data centers will produce a more consistent implementation of these healthcare systems and will result in a significant cost savings. The movement of systems builds upon VA's great success in the centralization of its Wide Area Networking infrastructure over the past 3 years. Additionally, the VA has augmented that infrastructure by adding Multiprotocol Label Switching and a redundant carrier to provide diversity and redundancy to its network.

Continuity of Services

The VA Nationwide Teleconferencing System (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 the Department of Defense. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 Kilobit per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 1,512 audio ports for voice teleconferencing.

To expedite the engineering of new radio frequency assignments, the VA uses the latest frequency management software, Spectrum XXI. The 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 (GMF) of Radio Frequency Authorizations in real time over the public switched telephone network.

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 satellite 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.

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 Services

As a result of the "Post-Katrina Emergency Management Reform Act of 2006," the functions of the DHS Wireless Management Office were divided between the new DHS Office of Emergency Communications (OEC) and the Wireless Services Section (WS) under the DHS Office of the Chief Information Officer (CIO). WS supports the NS/EP mission by providing spectrum-related services (frequency management, spectrum policy and planning), funding for special projects, department-level coordination for projects that involve multiple DHS Components, representation at DHS working groups, and, in coordination with the OEC, DHS representation to intergovernmental committees, and international organizations.

WS leads internal DHS initiatives to improve communications for homeland security and emergency preparedness and works to ensure that comprehensive planning and coordination of critical communications resources and equipment occur to support law enforcement and key government staff.

In fiscal year (FY) 2007, NS/EP accomplishments by WS included:

- Provided personnel to support the Federal Emergency Management Agency's (FEMA) creation of the Gulf Coast Emergency Communications Plan and other regional plans;
- In cooperation with the OEC, developed the National Interoperability Frequency Guide and the National Interoperability Field Operations Guide;
- Initiated and led department efforts to vacate the radio spectrum between 1710-1755MHz within the timelines established in accordance with the provisions of the statutes governing the Advanced Wireless Services program and the procedures prescribed by the Office of Management and Budget, the Federal Communications Commission, and the National Telecommunications and Information Administration (NTIA);
- Coordinated with NTIA to establish a consolidated joint government-industry interference testing program; and
- DHS CIO provided funding for the second phase of a multi-year program to upgrade the FEMA National Radio System (FNARS), FEMA's nationwide high frequency radio system. Execution of this phase of the upgrade will occur in FY 2008, concentrating primarily on State Emergency Operations Centers (EOCs) in hurricane-prone regions. FNARS provides long-range tactical communications support during all major hurricanes, as well as Continuity of Operations and other NS/EP communications exercises and events. The National Emergency Coordination Net, which utilizes FNARS equipment and frequencies, is activated during hurricanes to provide a common calling channel for all Federal responders and State EOCs to coordinate their activities.

Homeland Secure Data Network

As of the end of FY 2007, the DHS deployment of the Homeland Secure Data Network (HSDN) reached 95 government sites, providing a unified system and program that enables the sharing of secret-level data between its Federal partners. The HSDN continues to significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the Department's dependence on networks external to DHS.

Office of Emergency Communications

The DHS OEC was established by Public Law 109-295, the ‘‘Post-Katrina Emergency Management Reform Act of 2006’’. The Acting Director is Colonel Victoria Velez, U.S. Air Force, formerly Chief of Staff of the DHS National Communications System. OEC absorbed some of the functions of the former Wireless Management Office, Project SAFECOM, and the Federal Partnership for Interoperable Communications. OEC commenced operations on April 2, 2007.

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 Director of National Intelligence, 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
- World-wide quick reaction in support of crisis and special operational requirements.

Telecommunications Staff Organization

The Global Communications Service (GCS) operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities.

GCS 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 Principles/Council of Representatives.
- Continued support of the Government Emergency Telecommunications Services, the Wireless Priority Service, and the Telecommunications Service Priority system.
- Continue to transition our legacy secure telephone units to the new Secure Terminal Equipment.
- Continue to expand secure video teleconferencing to our workforce 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.

Continued to add redundancy and eliminate single points of failure in our commercial and secure voice and data networks.

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. FEMA's main mission is to manage federal response and recovery efforts following any national incident and to serve as the nation's portal for emergency management information. FEMA evaluates and adopts new telecommunications technologies annually, to ensure that government agencies can accomplish their missions effectively, even in the event of a catastrophic commercial telecommunications Infrastructure Loss.

Current/Ongoing NS/EP Telecommunications Activities

FEMA provides critical infrastructure support to communities, county's and States affected by natural or man-made disasters, before, during, and after destructive incidents to minimize the loss of life, assist in clean-up and recovery, and help victims return to normal activities.

FEMA helps communities plan for and face the threat of terrorism, weapons of mass destruction, and natural incidents preparing communities to respond to all types of hazards. FEMA also 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) systems, telecommunications services and facilities as part of the National Emergency Management Information System (NEMIS);
- Designs and develops emergency networks and information systems;
- Works with the commercial telecommunications industry to provide quick recovery from telecommunications infrastructure failures or outages through the Telecommunications Service Priority process;
- Provides communications support to State and local officials to help disseminate warnings of risks and hazards to the general public;
- Accumulates and assesses damage information after an incident has occurred;
- Deploys emergency telecommunications and IT network assets to incident areas to provide incident command and control during the initial hours of a disaster, and coordinates with State and Local responders to place assets where needed; and
- Coordinates the assignment and use of all Federal radio frequencies at an incident site to include high frequency (HF), ultra high frequency, very high frequency, 700 Megahertz (MHz) and 800 MHz radio frequencies. This coordination reduces area interference, crosstalk and jammed networks, creates bandwidth for outside agency utilization, and promotes interoperability among response groups.

Significant Achievements

A Common Alerting Protocol was developed for use by public television, cellular phones, pagers, and satellites to improve the existing public Emergency Alerting System.

NEMIS supported 102 disaster and emergency declarations in fiscal year (FY) 2007. NEMIS added the EMC FAN to significantly increase data storage capability. Finally, FEMA consolidated four NPSC's into two NPSC's to improve NEMIS operations and reduce replication of data.

The Mobile Disaster Response Center program was moved under the command and control of the Disaster Response Team. This move will improve coordination for deployment and implementation of these systems throughout a disaster area. These self contained communications vehicles are used to insert command, control, communications, and interoperability into an incident area without interconnectivity to other disaster management assets. The Disaster Response Team also assumes responsibility for operations and maintenance of these systems insuring that the latest equipment, software and operating systems are available for use.

Mobile Emergency Response Support (MERS) enhancements included the establishment of interoperability requirements with other Federal, State and Local entities. This communications coordination was executed through four major communications exercises. MERS also validated the air-lift capability of the Incident Response Vehicle in 3 of the 6 MERS detachments.

The FEMA National Radio System (FNARS) multiphase upgrade project continued in FY 2007. Additional (Gulf Region) State Emergency Operating Center's were upgraded with new HF radio systems. Additional funding was secured to continue the project in FY 2007-2008. Finally, operational control of the FNARS upgrade was transferred to ONCP to put the entire program under one office.

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)

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.

GSA is comprised of two integral components—The Public Building Service (PBS) and the Federal Acquisition Service (FAS). Within the FAS, the Integrated Technology Services (ITS) organization provides a broad spectrum of telecommunications and network services to the Federal departments and Agencies. The mission of the FAS-ITS is to deliver best value and innovative acquisition solutions for Information Technology (IT), Network Services (telecommunications), and Professional Services to support Government agency requirements worldwide. FAS-ITS works with agency customers to understand their requirements, simplify the development of acquisition strategies, conduct the acquisition, provide assistance throughout implementation, and manage the associated funding. FAS-ITS services help agencies achieve best value solutions and avoid doing costly, time-consuming acquisitions, save taxpayer dollars, and enable them to devote more of their own staffs directly to their agency missions and programs.

The GSA mission support functions for national security and emergency preparedness (NS/EP) are detailed in following authoritative documents:

- 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: National Plan for Telecommunications Support in Non-Wartime Emergencies
- Communications Act of 1934 (as amended), Section 706, War Emergency Powers
- National Response Plan

Current/Ongoing NS/EP Telecommunications Activities

FAS-ITS continues to help its client agencies develop solutions using a variety of IT and Network Services contracts. FAS-ITS assists with defining requirements, reviewing alternatives, developing performance based statements of objectives/statements of work, awarding tasks, project management, and managing project funds

FAS-ITS provides a variety of network services, information technology, and professional services that presently support 135 Federal agencies around the world. GSA's newly awarded, and highly anticipated Networx Universal and Networx Enterprise contracts are now available to provide voice and data services over terrestrial, wireless, and satellite transports supporting both classified and unclassified applications with integrated security features. Augmented by the availability of recently awarded SatCom-II contract, GSA Schedule 70 acquisitions, GSA Government-wide Acquisition Contracts and other integrated technology resources, GSA's Integrated Technology Services division is a one-stop shopping facility for virtually any IT requirement.

FAS-ITS provides emergency telecommunications support under the authority of the National Response Plan as detailed in the Office of Science and Technology Policy's "National Plan for Telecommunications Support in Non-Wartime Emergencies."

A Telecommunications Specialist is appointed by GSA in each Region to serve as National Communications System (NCS) Regional Manager (NCSRM). The NCS is the lead agency for Emergency Support Function (ESF) 2-Communications. The NCSRM represents the NCS ESF-2 responsibility and efforts for regional emergency disaster response planning, training, and exercise activities. Additionally, the NCSRM builds working relationships with the telecommunications industry within their respective Federal region. This ensures a seamlessly coordinated government/telecommunications industry emergency response effort. During the pre-deployment phase, the NCSRM coordinates and assesses potential emergency telecommunications requirements throughout their assigned region. Upon activation of ESF-2 by the Federal Emergency Management Agency (FEMA), the NCSRM may transition to the role of Federal Emergency Communications Coordinator (FECC), reporting to the NCS and the FEMA Federal Coordinating Officer (FCO). During disaster response efforts, the FECC is the single Federal point of contact in the incident area to coordinate ESF-2 response and recovery with the FCO and Principal Federal Official, as necessary.

GSA/FAS Significant Accomplishments

- GSA supported FEMA and the NCS during the 2007 calendar year for disaster relief and training efforts.
- GSA provided the NCSRM/FECC from almost all the regions to staff Regional Response Coordinating Centers, Joint Field Offices, and State Emergency Operations Centers as needed.
- GSA provided support for Continuity of Operations Planning and NS/EP exercises throughout the country and provided telecommunications support to FEMA for declared disasters.
- GSA continued FAS-ITS 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. Reservists augment the FAS-ITS staff or other Federal departments and agencies when organizations must rapidly mobilize to respond to national security emergencies.
- FAS-ITS participated in activities of the Committee on National Security Systems, the Priority Service Working Group, the Joint Telecommunications Resources Board, Continuity of Operations and Continuity of Government exercises, the Continuity Communications Working Group, the Communications Government Coordinating Committee, the National Coordinating Center, the National Security Information Exchange, the NCS Committee of Principals and the NCS Council of Representatives.

Other Significant Activities

FAS-ITS is presently engaged in modifying current IT and Network Services contracts to include any anticipated needs that may arise during emergency situations and ensure these contracts are readily accessible to FEMA and the NCS to facilitate rapid recovery efforts.

FAS-ITS continues to provide industry components, Federal departments and agencies current information regarding available services, including disaster support, contingency planning, and continuity of operations services through participation in a number of multi-agency committees, working groups, and the GSA website (*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.

Current/Ongoing NS/EP Telecommunications Activities

NASA continues to support the National Communications System in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. This includes Telecommunications Service Priority, Wireless Priority Service, 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, the Network Design and Analysis Capability, and the Interagency Committee on Search and Rescue.

NASA/EP Telecommunications Assets

NASA Integrated Services Network 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. The telecommunications services provided are primarily obtained through the General Services Administration contracts with the commercial sector.

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

NASA Deep Space Network supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.

NASA Near Earth Network (NEN) supports Low-Earth orbiting space flight missions. NASA obtains a significant portion of NEN services from the commercial market.

NASA Significant Accomplishments

- Participated in Sharers Exercises from multiple continental U.S.-dispersed NASA facilities; and
- Participated in the Telecommunications Service Priority System.

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 National Communications System 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 (ETS), 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 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. NRC continues to conduct quarterly testing of GETS, Satellite phones, and WPS.

NRC Significant Accomplishments

- Installed a new private branch exchange;
- Installed a new telephone recording system;
- Upgraded telephone conferencing system software;
- Upgraded automatic notification system software and hardware; and
- Renewed satellite service agreement and installed new sim cards in all telephones.

National Telecommunications and Information Administration (NTIA)

NS/EP Telecommunications Mission

The National Telecommunications and Information Administration (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 use of the radio frequency spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board (JTRB). 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. Part of the OSM vision is to use information technology (IT) 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 identify IT requirements of the Federal spectrum management community and appropriate plans to satisfy those requirements, for example, this year NTIA developed the Federal Spectrum Management System (FSMS) Transition Plan.

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

- Acquiring the necessary IT infrastructure equipment to establish the new FSMS environments.

- Continuing to plan and implement a phased series of FSMS 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 spectrum during NS/EP and normal conditions.

In addition, NTIA is continuing to:

- Serve as a non-resident member of the National Communications System (NCS) National Coordinating Center for Telecommunications.

- 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 Communications Dependency on Electrical Power Working Group.

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

Significant Accomplishments

- Fully supported the NCS relative to the National Response Framework Emergency Support Function 2 (ESF-2), Communications, for example, five NTIA personnel actively participated in the ESF-2 Spring Conference in June 2007.

- Coordinated and assisted in developing the spectrum management portions of numerous State and regional emergency communications plans (ECPs) such as the Gulf Coast ECP and the Federal Frequency Quick Guide for AL-LA-MS Coastal Counties.

- Published the report "A Public Safety Sharing Demonstration" under the President's Spectrum Policy Initiative.

- Developed the second Federal Strategic Spectrum Plan.

- Completed a major Department-wide project to enhance continuity communications capabilities by providing authorized users access to the Secret Internet Protocol Router Network, and initiated another project to provide authorized users access to the Joint Worldwide Intelligence Communications System.

- Participated in Exercise PINNACLE 2007 by activating the primary NTIA alternate operating facility, deploying over 50% of NTIA emergency employees as exercise participants, and testing all interoperable communications with partner agencies.

- Regularly participated in quarterly Title Globe exercises to test NTIA interoperable communications at its primary and alternate operating facilities.

- Participated as a principal member of the JTRB and its senior staff working group.

- 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 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 Worldwide Enterprise partners with academia, industry, and Government to provide IA solutions in an effort to keep U.S. national security systems safe from harm. This mission involves detecting and reporting on 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 (DOD) emerging Global Information Grid (GIG); developing secure audio and video communications equipment; developing tamper protection products; and providing trusted micro-electronic products.
- The ITD plans and operates the telecommunications systems and networks that link NSA elements worldwide, as well as provides connectivity to other Government services.
- The NSA has twice exercised both continuity of operations and recovery during the past year, employing appropriate emergency preparedness practices, tools, and telecommunication services.

Current/Ongoing NS/EP Telecommunications Activities

In accordance with its National Security Telecommunications and Information Systems Manager responsibilities under National Security Directive 42, the NSA provides IA products and services that are applicable across the Government for the protection of national security systems. 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 IA responsibilities. Information assurance should be an integral part of continuity of operations and/or recovery in the event of a national crisis or emergency. In support of these roles, the NSA is maintaining a leadership role in the following activities:

NSA Commercial Solutions for NS/EP Telecommunications

- The NSA collaborates with industry and Government to identify commercial solutions for national security system customers. This collaboration involves the design, development, procurement, and deployment of commercial technology and IA-enabled end products, devices/components, specifications, and guidance needed to satisfy customer's mission requirements. A significant mission element of this effort is to create a collaborative environment with commercial Information Technology firms to foster solutions to national security problem sets.
- A major focus has been the development of the Secure Mobile Environment Portable Electronic Device (SME PED). SME PED will provide transformational capability allowing secure mobile voice and Internet Protocol (IP) based services critical to sustaining interoperability with State, Local governments, and first responders.
- In addition to new secure mobile and wireless solutions, the NSA has initiated multiple IP encryption design specifications and equipment developments.
- The newly released High Assurance IP Encryption (HAIPE) interoperability specification features a variety of management, cryptographic and networking enhancements.
- High-level security design requirements to guide vendors developing non-Cryptographic Controlled Items IPsec and HAIPE compliant products were

defined. The requirements and specifications define the future of encryptor development efforts.

- HAIPE vendors successfully completed numerous contract tasks associated with the HAIPE spiral development. Specific equipment availability information can be provided as appropriate *via* request to your agency's NSA IA Client Advocate.

NSA Indications and Warning to NS/EP Telecommunications

The NSA provides real-time global network awareness and threat characterization capabilities to forecast, alert, and guide risk mitigation and countermeasures in response to activities directed against U.S. national security systems. NSA activities include the discovery and reporting of possible malicious network behavior.

The NSA provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique, tailored, time-critical and term reporting.

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 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 IA component of the DOD GIG architecture.

Electronic Key Management System (EKMS) for NS/EP Telecommunications Systems

- The 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.

- Initiation of EKMS Phase 5 capabilities this past year has enhanced keying material accountability and management to the local operational units.

- Additionally, EKMS capabilities enhancements have improved the ability to respond to dynamic interoperability requirements as well as automating the rekey process for some additional secure communication products.

Security Assessments Supporting NS/EP Telecommunications

- The NSA continues to perform security assessments to evaluate the security of national security customers' information systems and operations. Security assessments can include IA assessments, network technology analysis, technical security evaluations, Technical Security Countermeasures Operations, and TEMPEST services. Technical advice and assistance in support of assessments and evaluations within annual exercises have also been provided.

IA Services Supporting NS/EP Telecommunications

- The Cyber Defense Exercise (CDX) took place in April 2007 and special congratulations went out to the United States Military Academy at West Point as the winner of the annual event. CDX tested and evaluated the IA knowledge of cadets and midshipmen enrolled in Computer Science programs at each of the Armed Forces Service Academies. Overall, cadets and midshipmen did an outstanding job securing and defending their networks.

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

- The NSA and the NIST jointly announced the public availability of the Extensible Configuration Checklist Description Format (XCCDF). The NSA and the 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.

Global Information Grid (GIG)

- The NSA's Enterprise IA Systems Engineering effort leads the Community toward developing an enterprise level IA architecture strategy, technical framework, transition plan, and enterprise level IA systems engineering implementation requirements for the DOD's GIG. The goal is to enable the Defense-in-Depth to achieve an assured, integrated and survivable GIG Enterprise. This effort should assist in achieving information superiority and enable Net-Centric Warfare. An assured GIG will transform the way DOD operates, communicates and uses information to accomplish its mission. Accordingly, it is broadly applicable to achieving an Information Sharing Environment across Federal, State, Local, and other entities, and to the protection of our critical infrastructures upon which the national security community depends.

Cross Domain Solutions (CDS)

- The NSA has a long history of helping national security systems customers resolve Assured Information Sharing problems between network domains. The Collaborate Access and Browse (CAB) CDS and the Assured File Transfer (AFT) CDS were successfully received at the 2007 Coalition Warrior Interoperability Demonstration receiving a Superior Performing Warfighter Technologies Rating from the judges. Both the CAB and the AFT products are in the final stages of development and will be available to all customers in 2008.

Vulnerability Analysis and Operations Assessments

- The NSA provides vulnerability analysis and operational assistance to the national security community regarding computer network defense. These activities were accomplished through unique leadership and technical expertise in the areas of operations, technology analysis, community coordination, policy, as well as analysis and reporting. NSA provides, through close partnership with DOD and national security customers, operational, crisis, and exercise planning to ensure that cyber defense activities and responses promoted good actionable countermeasures and recovery. These assessments provided a unique look at U.S. Government systems, operations, personnel, and current technology, which enabled the protection and defense of information by mitigating risks. Expert operational analysis and guidance is sustained through state-of-the-art technology evaluations covering a wide range of communication components, network applications, and software applications.

NS/EP Telecommunications Mission

The Postal Service delivers to every household and business in the United States (300 million people at 146 million homes, businesses, and Post Office Boxes in every state, city and town, and in Puerto Rico, Guam, the American Virgin Islands and American Samoa). 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 213 billion pieces of mail to over 146 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 46% 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 9 million customers daily at more than 37,000 Post Offices™.
- 1,450 of our Post Offices now stay open later in response to customer needs. This has improved customer service and satisfaction.
- Provide stamps at:
  - More than 27,800 vending machines;
  - Nearly 33,000 commercial retail outlets;
  - Nearly 17,000 banking and credit union ATMs; and
  - 2,500 Automated Postal Centers®.
- Have annual operating revenue of nearly $73 billion.
- Employ nearly 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 2 weeks.

Benefits

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 a 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 United States Postal Service (USPS) 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.

USPS Significant Accomplishments

Upgrading the Telecommunications Infrastructure (Voice)

After the extensive improvements to the USPS 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 Internet Protocol environment. Presently these systems are operating with conventional Digital Primary Rate Interface trunks for commercial and within network calling. By the end of FY 2007, all of the Postal Service's PBX's will have been updated.

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 2007, USPS has replaced more than 1550 key telephone systems in Main Post Offices, Stations and Branches throughout the Postal Service. This effort was designed to update systems that were over ten years old and no longer adequate for the activities of a 21st Century facility. The replacements included in some cases new improved paging systems as well as wiring in order to improve employee communication and customer service.

PBX Security

All PBX's in the USPS 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 that 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 may be issued to advise employees and business partners of any outage or malfunction.

Government Telecommunications Service (GETS)

There is an ongoing effort 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.

Wide Area Network Upgrades

Since the beginning of this fiscal year we have upgraded the telecommunications service at 7005 Postal facilities. Most of the facilities moved from a low speed (VSAT, 56k frame, DSL) connection to a 768k dedicated service with fixed performance service level agreements. This increase in service level has reflected in increased computer performance at Postal locations nationwide

Conversion from Dial up to Broadband

The USPS has additionally increased the level of network capacity and security at all upgraded sites by converting from dial and installing a managed Virtual Private Network (VPN) firewall router at each location—thus protecting USPS computer assets from any malicious internet activity. Total number of broadband enabled locations now reaches over 8,000 USPS locations; 2,236 sites were upgraded in FY 2006.

There are currently 7,500 VPN/Firewall Routers deployed and managed by USPS not including the critical back-office VPN and security gear that make this huge web of nationwide VPN sites possible.

Dial up to Broadband Stats Recap

- Total Number of dial-up sites upgraded to Broadband: 8,000+ and growing

- Broadband upgrades in the last two years: 2,236
- Total Number of VPN routers deployed and managed internally by USPS: 7,500 and growing
- Consolidated 5 broadband providers into just 2 providers thus simplifying troubleshooting and problem resolution.

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 (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.

FRB Significant Accomplishments—2007

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
- Circuits used by ACH operators and the CLS bank that meet the FRB's eligibility criteria
- Circuits connecting customers of sponsored payment system, foreign exchange, and clearing and settlement utilities that meet the FRB's eligibility criteria
- Circuits used by capital and futures exchange utilities and key participants that meet the SEC and CFTC eligibility criteria

- Circuits used by market data providers that supply critical information needed by financial institutions
- Circuits used by the World Bank to ensure continuity of operations

By the end of this fiscal year, there will be approximately 5,000 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 60 institutions.

During the last fiscal year, the FRB continued to participate in the evolution of the WPS program. The FRB has sponsored approximately 35 institutions for WPS.

National Diversity Assurance Initiative/Diversity Assurance Analysis

In 2005 and early 2006, the National Diversity Assurance Initiative (NDAI), led by the Alliance for Telecommunications Industry Solutions Chief Information Officer's 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 NDAI 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. In early 2007, the NCS initiated the Diversity Assurance Analysis (DAA) to analyze several models for carriers to establish methods to record circuit diversity data and to exchange diversity data between carriers, when applicable. The DAA initiative is currently considering technology advancements, security, policy, and legal concerns related to several possible diversity assurance solutions. The Federal Reserve serves on the advisory group of subject matter experts.

The Federal Reserve Board 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. In late July 2006, a Systemwide three-day tabletop exercise was conducted to test the readiness of the System to operate critical business functions during a pandemic flu situation.

Federal Communications Commission (FCC)

NS/EP Communications Mission

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

- Developing policies and promulgating regulations for effective communications through wire and radio for the national defense and promotion of safety of life and property.
- Evaluating and strengthening measures for protecting and preserving critical communications infrastructure and associated systems.
- Facilitating rapid restoration of critical communications infrastructure and systems following disruptions, regardless of the cause.
- Participating in international organizations and conferences to coordinate global communications issues and promote the Nation's interests.
- Coordinating with industry and other federal, tribal, state, and local entities regarding public safety, homeland security, and disaster preparedness and response.
- Serving as the Federal collector of real-time communications infrastructure and service outage and restoration information from wireline, wireless, cable, broadcast, satellite, and other communications service providers.
- Coordinating with the National Telecommunications and Information Administration in assigning radio frequencies, determining priorities for the use of those frequencies, and managing the use of the same.
- Providing expert technical advice to policymakers on wireless and wireline matters.

Current/Ongoing NS/EP Communications Activities

- In February of 2007, FCC Chairman Kevin J. Martin announced the appointment of Derek K. Poarch as new Chief of the FCC's Public Safety and Homeland Security Bureau (PSHSB). Chief Poarch comes to the FCC with significant experience in law enforcement; most recently he served as Director of Public Safety at the University of North Carolina at Chapel Hill.

  The priorities Chief Poarch has set for the PSHSB include, among other things, public safety spectrum management (700 Megahertz (MHz) interoperability broadband and 800 MHz rebanding), digital television transition (clearing spectrum for public safety licensees), public alert and warning (for example, the Emergency Alert System (EAS), E911 (functionality and location accuracy), and to serve as an Information Clearinghouse for emergency preparedness and response information. *See http://www.fcc.gov/pshs*
- In April of 2007, the FCC created a new federal advisory committee, the Communications Security, Reliability and Interoperability Council (CSRIC). The CSRIC will provide recommendations to the FCC to ensure optimal security, reliability, and interoperability of communications systems, including telecommunications media and public safety. The CSRIC replaces the Network Reliability and Interoperability Council and the Media Security and Reliability Council.
- On June 8, 2007, the FCC issued an Order implementing recommendations from its *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks* (*Katrina Panel*). In the *Order*, the FCC tasked the PSHSB with many NS/EP action items on which the PSHSB has been working or has taken on. *See http://www.fcc.gov/eb/hkip*
- The FCC published emergency communications planning guides for the public safety community, communications industry, and healthcare sector. *See http://www.fcc.gov/pshs/clearinghouse/index.html*
- To promote the Priority Services programs, (Government Emergency Telecommunications Service, Telecommunications Service Priority [TSP], and Wireless Priority Service), the FCC published FAQs and Enrollment Guides crafted for specific audiences (for example, police, fire, and emergency medical service) on its website. *See http://www.fcc.gov/pshs/emergency/priorityservices.html* Senior PSHSB officials promote these programs in their speeches and presentations. Further, the FCC supports seeking a grant funding source for the $8 million estimated to enroll all Public Safety Answering Points (PSAPs or 911 Call Centers) and state Emergency Operations Centers into the TSP program.

- Rollout of the Disaster Information Reporting System (DIRS). The FCC will use DIRS to collect voluntarily submitted communications industry information on outages and other situational awareness metrics from service providers affected by a disaster. The FCC will share—on a confidential basis—DIRS information with the NCS. *See https://www.fcc.gov/nors/disaster*

- Senior PSHSB officials are working to raise awareness of access and credentialing issues within all levels of government.

- The FCC is publicizing the value of National Communications Center (NCC) membership and encouraging suitable entities to apply for membership. In August of 2007, the National Association of Broadcasters submitted its application for NCC membership.

- In its *EAS Second Report and Order and Further Notice of Proposed Rulemaking* of July 2007, the FCC expanded the defined EAS participants to include wireline video service providers.

- The FCC established a Commercial Mobile Service Alert Advisory Committee (CMSAAC) as required by the Warning Alert and Response Network Act. The CMSAAC is charged with developing and recommending technical standards to facilitate voluntary commercial radio service transmission of emergency alerts to subscribers.

- Under the *Communications Assistance for Law Enforcement Act* (*CALEA*), the FCC now requires broadband internet access and voice over internet protocol service providers to comply with CALEA.

- The FCC was a key NCS partner in developing and implementing the 2007 Emergency Support Function (ESF) 2 Training Conference held in New Orleans. The FCC team coordinated the exercise portion of the training and designed the injects based on real-world experience from the ESF-2 response to Hurricane Katrina.

- FCC field engineers and Headquarters staff have been working with fourteen states along with the U.S. Virgin Islands and Puerto Rico to assist them prepare emergency communications plans. This process includes validation of existing frequencies and systems, command-and-control structures, staging areas, evacuation centers, and the like.

- In July of 2007, the FCC revised the 700 MHz band plan and service rules to promote the creation of a nationwide interoperable broadband network for public safety and to facilitate the availability of new and innovative wireless broadband services for consumers. The FCC is establishing a framework for a 700 MHz Public Safety/Private Partnership between the licensee for one of the commercial spectrum blocks and the licensee for the public safety broadband spectrum. As part of the Partnership, the commercial licensee will build out a nationwide, interoperable broadband network for the use of public safety. Under the Partnership, the Public Safety Broadband Licensee will have priority access to the commercial spectrum in times of emergency, and the commercial licensee will have preemptible, secondary access to the public safety broadband spectrum.

- The *Implementing Recommendations of the 9/11 Commission Act of 2007* charged the FCC with several duties, including:

  - Consulting with NCS and assessing the nation's critical communications and information systems infrastructure and evaluating the feasibility of creating a back-up emergency communications system that complements existing communications resources and takes into account next generation and advanced communications technologies.

  - Working with the Department of Commerce, and consulting with the Department of Homeland Security (DHS) and the Department of Health and Human Services, to form a joint advisory committee to examine the communications capabilities and needs of emergency medical and healthcare facilities.

  - Consulting with DHS Office of Emergency Communications, Office of Management and Budget, and the Department of State, to report on cross border interoperability and related issues, including treaty negotiations, concerning Canada and Mexico.

A

NCS Related Acronyms

NCS Related Acronyms

A

ACH	Automated Clearing House
ACR	Alternate Carrier Routing
AES	Advance Encryption Standard
AFCEA	Armed Forces Communications and Electronics Association
AFT	Assured File Transfer
AGG	Alert Gateway Group
ANSI	American National Standards Institute
AOF	Alternate Operating Facility
ART	Analysis Response Team
ASD (HD)	Assistant Secretary of Defense for Homeland Defense
ASH (NII)	Assistant Secretary of Defense for Networks and Information Integration
ATG	Advanced Technology Group
ATIS	Alliance for Telecommunication Industry Solutions
ATO	Authority to Operate

B

BCIS	Bureau of Citizenship and Immigration Services
BFEM	Budget Formulation and Execution Manager System
BLADE	Biometric Logical Access Development and Execution Program
BMC	Beltsville Management Center
BPD	Bureau of Public Debt
BRI	Basic Rate Interface
BRM	Business Reference Model

C

C4	Command, Control, Communications, and Computer Systems Directorate
C&A	Certification and Accreditation
CA	Certification Authority
CAA	Controlled Access Area
CAB	Collaborate Access and Browse
CALEA	Communications Assistance for Law Enforcement Act
CCA	Continuity Communications Architecture
CCPC	Civil Communications Planning Committee
CDC	Center for Disease Control
CDEP WG	Communications Dependency on Electric Power Working Group
CDFI	Community Development Financial Institution
CDMA	Code Division Multiple Access
CDS	Cross Domain Solutions
CDX	Cyber Defense Exercise
CEP	Civil Emergency Planning
CEPTAG	Civil Emergency Planning Telecommunications Advisory Group
CFIUS	Committee for Foreign Investment in the U.S.
CFTC	Commodities and Futures Trading Commission
CGCC	Communications Government Coordinating Council
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CI/KR	Critical Infrastructure/Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Protection Advisory Committee
CLS	Continuous Linked Settlement
CMN	Crisis Management Network
CMO	Coordination and Management Office
CMS	Commercial Mobile Service
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CNSS	Committee for National Security Systems
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
COTS	Commercial Off-The-Shelf
CP	Contingency Planning
CS&C	Cyber Security and Communications
CS&T	Cyber Security and Telecommunications
CSCC	Communications Sector Coordinating Council
CSRIC	Communications Security, Reliability, and Interoperability Council
CSSP	Communications Sector-Specific Plan
CWIN	Critical Warning Infrastructure Network

D

DAN	Data Analysis Network
DEA	Drug Enforcement Administration
DES	Data Encryption Standard
DHS	Department of Homeland Security

DHHS	Department of Health and Human Services
DIB	Defense Industrial Base
DIRS	Disaster Information Reporting System
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
DR	Disaster Recovery
DSD	Deputy Secretary of Defense
DSIE	Defense Security Information Exchanges
DS	Diplomatic Security
DSS	Diplomatic Security Service
DTCI	Defensive Technical Counter-Intelligence
DTS	Digital Telecommunications Switching System

E

EAS	Emergency Alert System
EBS	Emergency Broadcasting System
ECITF	Emergency Communications and Interoperability Task Force
ECPs	Emergency Communications Plans
ECT	Emergency Communications Teams
ECT-F	Emergency Communication Teams-Field
ECT-N	Emergency Communication Teams-National
EKMS	Electronic Key Management System
EMC	Emergency Management Centers
EMP	Electromagnetic Pulse
E.O.	Executive Order
EOC	Emergency Operations Center
EOP	Executive Office of the President
ESF	Emergency Support Function
ETS	Emergency Telecommunications System
EU	European Union
EWP	Emergency Wireless Protocol

F

FA	Frequency Authorization
FAS	Federal Acquisition Service
FBCA	Federal Bridge Certificate Authority
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCO	Federal Coordinating Officer
FDIC	Federal Deposit Insurance Corporation
FEA	Federal Enterprise Architecture
FEB	Federal Executive Branch
FECC	Federal Emergency Communications Coordinator
FEMA	Federal Emergency Management Agency
FNARS	FEMA National Radio System
FOC	Full Operational Capability
FPIC	Federal Partnership for Interoperable Communications
FRB	Federal Reserve Board
FPKIPA	Federal PKI Policy Authority
FSMS	Federal Spectrum Management System
FTS	Federal Technology Service (Section III)
FY	Fiscal Year

G

GCCC	Government Communications Coordinating council
GCS	Global Communications Service
GETS	Government Emergency Telecommunications Service
GFIRST	Government Forum of Incident Response and Security Teams
GIG	Global Information Grid
GITM	Global IT Modernization
GNO	Global Network Operations
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act
GSA	General Services Administration
GSM	Global System for Mobile Communications

H

HAIPE	High Assurance Internet Protocol Encryptor
HCHB	Herbert C. Hoover Building
HF	High Frequency
HPM	High Power Microwave
HQ	Headquarters
HSDN	Homeland Security Data Network
HSPD	Homeland Security Presidential Directive

I

IA	Information Assurance
IAM	Initial Address Message
IC	Integration Contractor
IC	Intelligence Community
IES	Industry Executive Subcommittee
IMA	Individual Mobilization Augmentee
IMS	IP Multimedia Subsystem
INE	Inline Network Encryption
IOS	Interoperability Specification
IP	Internet Protocol
IR	Industry Requirements
IRAC	Interdepartment Radio Advisory Committee
IRM	Bureau of Information Resource Management
IRS-CI	Internal Revenue Service-Criminal Investigation
IS	Interoperability Specification
ISDN	Integrated Services Digital Network
IT	Information Technology
ITD	Information Technology Directorate
ITS	Integrated Technology Services
IWN	Integrated Wireless Network
I-WPS	Immediate Wireless Priority Service
IXC	Interexchange Carrier

J

J6	Command, Control, Communications, and Computer Systems Directorate
JCG	Joint Contact Group
JFO	Joint Field Office
JTRB	Joint Telecommunications Resource Board
JUTNet	Justice Unified Telecommunications Network

K

Kbps	Kilobit per second
KCP	Kansas City Plant

L

LAN	Local Area Network
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
LRTF	Legislative and Regulatory Task Force
LTO	Long-Term Outage

M

MCO	Management Coordination Office
MERS	Mobile Emergency Response Support
MHD	Magneto Hydro Dynamics
MHz	Megahertz
MOA	Memoranda of Agreement
MRTD	Machine Readable Travel Document
MSC	Mobile Switching Center
MSF	MultiService Forum
MSO	Managed Service Offering
MXU	Multi-Exchange Units
MYSMP	Multi-Year Strategy and Program Management Plan

N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCCC	National Command and Coordinating Capability
NCCTF	National Coordinating Center Task Force
NCS	National Communications System
NCSD	NCS Directive
NCSD	National Cyber Security Division
NCSRM	National Communications System Regional Manager
NCUA	National Credit Union Administration
NDAC	Network Design and Analysis Capability
NECP	National Emergency Communications Plan
NECS	National Emergency Communications Strategy
NEF	National Essential Functions
NEMIS	National Emergency Management Information System
NEN	Near Earth Network
NGN	Next Generation Network
NGO	Non-Governmental Organizations
NIFC	National Interagency Fire Center
NIIF	Network Interconnection Interoperability Forum
NIST	National Institute of Standards and Technology

NOAA	National Oceanic and Atmospheric Administration
NOIWON	National Operational Intelligence Watch Officers Network
NOTF	NSTAC Outreach Task Force
NPPD	National Protection and Programs Directorate
NRC	Nuclear Regulatory Commission
NRF	National Response Framework
NSA	National Security Agency
NSC	National Security Council
NSDD	Network Security Decision Directive
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSPD	National Security Presidential Directive
NSRA	National Sector Risk Assessment
NSS	National Security Systems
NSTAC	The President's National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration

O

OA	Operational Analysis
OCC	Office of Comptroller of Currency
OCIO	Office of the Chief Information Officer
OEC	Office of Emergency Communications
OEP	Office of Emergency Preparedness
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPLAN	Operation Plan
ORO	Oak Ridge Office
OSD	Office of the Secretary of Defense
OSM	Office of Spectrum Management
OSS	Operations Services Staff
OSTP	Office of Science and Technology Policy
OTS	Office of Thrift Supervision

P

P25	Project 25
PAS	Priority Access Service
PBS	Public Building Service
PBX	Private Branch Exchanges
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMEF	Priority Mission Essential Functions
PMO	Program Management Office
PPBE	Planning, Programming, and Budgeting Execution System
PO	Program Office
PRM	Performance Reference Model
PSAP	Public Safety Access Points
PSHSB	Public Safety and Homeland Security Bureau
PSTN	Public Switched Telephone Network
PSWG	Priority Services Working Group

R

R&D	Research and Development
R&O	Report and Order
RCC	Regional Communications Coordinator
RDM	Route Diversity Methodology
RDTF	Research and Development Task Force
RDX	Research and Development Exchange
RFCs	Request for Comments
RL	Richland Operations Office
RMOTC	Rocky Mountain Oilfield Testing Center

S

SAVCE	Symantec AntiVirus Corporate Edition
SAVER	Secure AntiVirus Equipment Refresh
SBU	Sensitive But Unclassified
SEC	Security and Exchange Commission
SHARES	Shared Resources
SHARES-HF	Shared Resources High Frequency Radio Program
SMART	State Messaging Archive Retrieval Toolset
SME PED	Secure Mobile Environment Portable Electronic Device
SOC	Security Operations Center
SP	Special Publication
SPP	Security & Prosperity Partnership
SRM	Service Component Model
SS7	Signaling System 7
SA	Situational Awareness
SSA	Social Security Administration
SSP	Sector Specific Plan (Section III)
SSP	System Security Plans (Section IV)
STE	Secure Terminal Equipment

STU	Secure Telephone Unit
SVDC	Secure Video and Data Collaboration
SVP-COI	Secure Voice Products Community of Interest
SVTC	Secure Video Teleconferencing

T

TADAC	Technology Assessment and Data Analysis Cell
TAN	Technology Assessment Network
TCA	Transformational Communications Architecture
TCS	Treasury Communications System
TEDE	Telecommunications Electromagnetic Disruptive Effects
TEPITF	Telecommunications and Electric Power Interdependencies Task Force
TRM	Technical Reference Model
TSC	Telecommunications Service Center
TSP	Telecommunications Service Priority
TSS	Technical Security and Safeguards
TTX	Test, Training, and Exercises

U

USDA	U.S. Department of Agriculture
USMS	United States Marshals Service
USPS	U.S. Postal Service

V

VA	Department of Veterans Affairs
VANTS	VA Nationwide Teleconferencing System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

W

WARN	Warning, Alert, and Response Network Act
WP	Work Program
WPO	Wireless Program Office
WPS	Wireless Priority Service
WS	Wireless Services Section

X

XTE	eXperimental Testbed Environment
XCCDF	Extensible Configuration Checklist Description Format

B

Photo Credits

Photo Credits

Section I Divider – page 1

October 1962 Executive Committee of the National Security Council meeting. Clockwise from President Kennedy: President Kennedy; Secretary of Defense Robert S. McNamara; Deputy Secretary of Defense Roswell Gilpatric; Chairman of the Joint Chiefs of Staff Gen. Maxwell Taylor; Assistant Secretary of Defense Paul Nitze; Deputy USIA Director Donald Wilson; Special Counsel Theodore Sorensen; Special Assistant McGeorge Bundy; Secretary of the Treasury Douglas Dillon; Attorney General Robert F. Kennedy; Vice President Lyndon B. Johnson (hidden); Ambassador Llewellyn Thompson; Arms Control and Disarmament Agency Director William C. Foster; CIA Director John McCone (hidden); Under Secretary of State George Ball; Secretary of State Dean Rusk. White House, Cabinet Room. (Photo by Cecil Stoughton, White House, October 29, 1962.)

Section II Divider – page 7

Ocean Springs, Miss., September 6, 2005—FEMA representative Jarvis Thomas sets up computers at a Disaster Recovery Center (DRC) in Ocean Springs, Miss. DRCs help guide residents affected by Hurricane Katrina through the FEMA recovery process.
(Photo by Mark Wolfe/FEMA)

Section III Divider – page 11

Telecommunications Tower
(Source: gettyimages®, "Science, Technology, & Medicine" Photodisc® CD Collection – image# ST000869)

Section IV Divider – page 53

Key West, FL, November 4, 2005—FEMA Individual Assistance information specialists help local residents impacted by Hurricane Wilma fill out information at the Disaster Recovery Center set up next to the City. (Photo by Hall. Jocelyn Augustino/FEMA)

Note—Unless indicated all other images were obtained from a stock image library.