Fiscal Year 2009 Report

National Communications System

National Communications System

Ensuring Essential Communications for the Homeland

Prepared by the Office of the Manager,
National Communications System

Foreword

As the National Communications System (NCS) prepares to move into the second decade of the 21st Century, we continue to evolve our role and mission in support of the Nation's national security and emergency preparedness (NS/EP) communications community. Working closely with its industry partners, the NCS maintains a strong public/private partnership – now in its 46th year of service – and continues to build toward the future.

During Fiscal Year (FY) 2009, the 24 NCS-member Departments and Agencies, the Office of the Manager and NCS' industry partners actively executed the mission of the NCS. We coordinated and provided recommendations to White House and Department of Homeland Security (DHS) officials on critical emergency communications issues; trained emergency response personnel to ensure the effectiveness of critical emergency preparedness and response efforts; and prepared to respond to disasters that could result in degraded or destroyed communications, such as flooding, hurricanes or earthquakes.

On January 20, Barack H. Obama became the 44th President of the United States – the 10th Chief Executive since the creation of the NCS by President John F. Kennedy in 1963. President Obama acted quickly in making cybersecurity and communications efforts a priority – initially commissioning a Cyberspace Policy Review which assessed the policy, procedures, and infrastructure surrounding the Nation's cybersecurity. The NCS coordinated with private industry stakeholders through the National Security Telecommunications Advisory Committee (NSTAC) to compile a thorough response that included a range of recommendations relating to cybersecurity and communications. NSTAC provided the NCS, DHS and the White House with valuable input regarding cybersecurity issues and efforts, such as the importance of public-private partnerships in mitigating threats and strengthening national cybersecurity.

Partnerships play a significant role in executing the mission of the NCS. In addition to NSTAC, these partnerships include the National Coordinating Center (NCC) and the Communications Information Sharing and Analysis Center, the NCS Committee of Principals (COP), the Government and Communications Sector Coordinating Councils (CGCC and CSCC), and the Network Security Information Exchanges (NSIEs).

In addition to our ongoing partnership activities, we remained focused on an array of emerging and persistent threats in FY 2009. For example, in early 2009, the H1N1 Pandemic Flu caused great concern throughout the world. The NCS publicly released its *Pandemic Influenza Impact on Communications Networks*, which provided suggested practices on minimizing network congestion duting a pandemic event. Interested parties can read the report online at: *www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20(December%202007).pdf*.

During FY 2009, the COP engaged in numerous activities. It examined the operating status of NCS priority services, conducted hurricane preparedness discussions focusing on individual Department and Agency preparedness strategies, and completed the Communications Dependency on Electric Power Working Group *Long Term Outage Study*. The report provided a detailed analysis of long- and short-term electric power outages and their affect on communications infrastructure, and provided recommendations for mitigation.

The NCS also focused on testing and identifying areas for improvement within its priority service offerings. During the presidential inauguration, the Government Emergency Telecommunications Service (GETS) successfully enabled key personnel to receive and send priority calls during periods of network congestion. Additionally, the inauguration allowed the NCS to test the Wireless Priority Service (WPS) offering and identify areas for analysis and improvement.

Another NCS priority during fiscal year 2009 was ensuring the resiliency of the communications infrastructure. The NCS continued to facilitate hurricane preparedness, aid, and ensured that lessons learned from the devastating 2005 hurricane season were implemented in current hurricane preparedness plans. Other events, such as providing support to communities during the Kentucky ice storms, the Midwest floods last spring, and the G-20

summit in Pittsburgh demonstrated the NCS' continuing capability to provide active response, support, and analysis during high security and disaster situations.

The NCS applied its technical expertise in conducting route diversity assessments for several Federal Department and Agency locations. The assessments identified vulnerabilities within network infrastructure and examined ways to mitigate apparent risks and increase communications infrastructure diversity at these sites.

The NCS also aided Federal Government disaster preparedness personnel in Emergency Support Function #2 (communications) training. By using distance-learning seminars, web-briefings and conference calls, the NCS provided training support to many Federal Departments and Agencies, conducted training exercises, and developed analytical products designed around a variety of NS/EP communications scenarios.

On March 11, 2009, Secretary of Homeland Security Janet Napolitano appointed Philip R. Reitinger as the National Protection and Program Directorate's Deputy Under Secretary and Director of the National Cybersecurity Center (NCSC). Three months later, she named Gregory Schaffer as the Assistant Secretary for Cybersecurity and Communications (CS&C). Soon after Fiscal Year 2010 began, Secretary Napolitano designated Mr. Reitinger as the Manager of the NCS and Mr. Schaffer as the NCS Principal Deputy Manager.

From the beginning of the new administration on January 20, 2009 through the end of Fiscal Year 2009, I served as the Acting Manager of the NCS while also performing my duties as the CS&C Deputy Assistant Secretary. During my time at the helm, we actively engaged in endeavors and partnerships critical to our NS/EP mission. While the threats to the Nation's security posture continue evolving, the NCS remains vigilant in its mission to strengthen and support the Nation's vital communications infrastructure and capabilities. I know – through the NCS' strong, long-standing relationships and innovative efforts – that we will exceed the challenges of developing and providing effective protection, preparation, response, recovery, and coordination of the Nation's critical communications systems.

Michael A. Brown, RADM, USN
Deputy Assistant Secretary
Cybersecurity and Communications

NCS Leadership

Rear Admiral Michael A. Brown, U.S. Navy
DHS Deputy Assistant Secretary for Cybersecurity and Communications, and Acting Manager

Mr. James J. Madon
Director and Deputy Manager

Mr. Allen F. Woodhouse
Chief of Staff

Mr. Richard Bourdon
Chief, Technology and Programs Branch

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

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

Mr. Michael Echols
Chief, Customer Service/ Government Industry Planning and Management Branch

NCS Committee of Principals

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

Department of the Treasury (TREAS)
Ms. Vicki Waizenegger

Department of Defense (DOD)
Ms. Cheryl Roby

Department of Justice (DOJ)
Mr. Eric Olson

Department of the Interior (DOI)
Mr. Timothy Quinn

Department of Agriculture (USDA)
Ms. Susan A. Moore

Department of Commerce (DOC)
Ms. Suzanne Hilding

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

Department of Transportation (DOT)
Mr. Tim Schmidt

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

Department of Veterans Affairs (VA)
Mr. Andres A. Lopez

Department of Homeland Security (DHS)
Mr. Michael Brown

Office of the Director of National Intelligence (ODNI)
Ms. Pricilla Guthrie

Federal Emergency Management Agency (FEMA)
Mr. Damon Penn

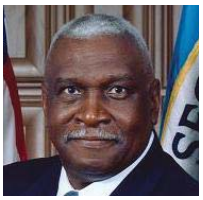
The Joint Staff (JS)
LTG Dennis L. Via, USA

General Services Administration (GSA)
Mr. Ed O'Hare

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

Nuclear Regulatory Commission (NRC)
Mr. Melvyn Leach

National Telecommunications and Information Administration (NTIA)
Ms. Anna Gomez



National Security Agency (NSA)
Mr. John Mathews

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

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

United States Postal Service (USPS)
Mr. Charles McGann

NCS Council of Representatives

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

Department of the Treasury (TREAS)
Ms. Vicki Waizenegger

Department of Defense (DOD)
Mr. Bill Gunnels

Department of Justice (DOJ)
Ms. Lisa Schmitt

Department of the Interior (DOI)
Mr. Stuart A. Ott

Department of Agriculture (USDA)
Mr. Roy Allums

Department of Commerce (DOC)
Mr. Earl Neal

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

Department of Transportation (DOT)
Mr. Michael Dammeyer

Department of Energy (DOE)
Mr. Al Cerrone

Department of Veterans Affairs (VA)
Mr. James Lacey

Department of Homeland Security (DHS)
Mr. Keith Jones

Office of the Director of National Intelligence (ODNI)
Mr. Gary D. Strohm

Federal Emergency Management Agency (FEMA)
Ms. Ann Buckingham

The Joint Staff (JS)
Lt. Col. Christopher J. Keeton, USAF

General Services Administration (GSA)
Mr. David Jarrell

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

Nuclear Regulatory Commission (NRC)
Mr. Robert Miller

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

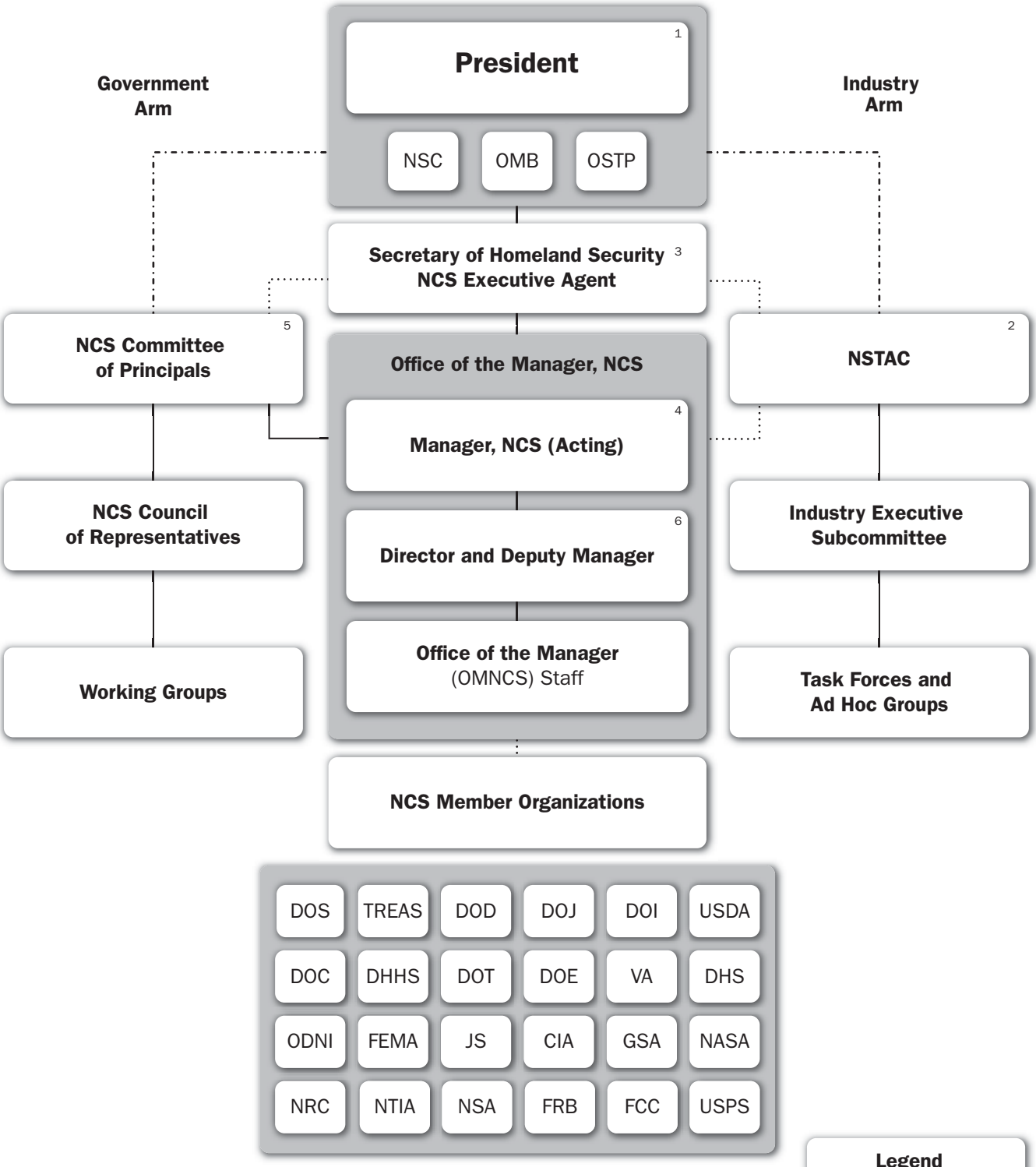
National Security Agency (NSA)
Mr. Andy Caufield

Federal Reserve Board (FRB)
Ms. Sheree D. Jones

Federal Communications Commission (FCC)
Mr. Allan Manuel

United States Postal Service (USPS)
Mr. Warren Schwartz

The NCS Structure



1. Policy Direction and Direct Execution of War Powers Function
2. The President's National Security Telecommunications Advisory Committee created by Executive Order 12382
3. Executive Agent, NCS responsibilities assigned to Secretary of Homeland Security by E.O. 13286, February 28, 2003
4. Deputy Under Secretary for National Protection and Programs, 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

1 Introduction: The History of the National Communications System

The Office of the Manager, National Communications System, prepares this annual report to describe the agency's national security and emergency preparedness activities and telecommunications events, including highlights of the organization's innovations, programs, and achievements during fiscal year 2009.

Background

President John F. Kennedy created the National Communications System (NCS) to remedy critical communications difficulties he and his administration experienced during the 1962 Cuban Missile Crisis. The President commissioned the National Security Council (NSC) to examine the infrastructure and processes behind critical Government communications, leading to the establishment of the NCS through National Security Action Memorandum 252, *Establishment of the National Communications System*. The White House issued the memorandum on August 21, 1963, and mandated that the NCS would be the provider of critical Federal Government communications for all types of situations—from day-to-day communications to national emergencies, such as nuclear attacks. The evolving telecommunications environment through the past 47 years keeps the NCS involved as a critical player in ensuring the strength of our national security and emergency preparedness (NS/EP) telecommunications posture.

President Kennedy confers with National Security Advisor McGeorge Bundy. White House, Northwest Gate on June 13 1962. (Photograph by Abbie Rowe, National Park Service)

In the 1980s, the divestiture of AT&T and the emergence of advanced network technologies led to major changes for the NCS. On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. This E.O. reworked the existing structure of the NCS by installing a variety of new positions, including the Secretary of Defense as the Executive Agent; the Manager, NCS, and staff; and a Committee of Principals (COP), which would represent the Federal member organizations with NS/EP responsibilities.

E.O. 12472 also recast the position and mission of the NCS, and determined that it should expand its role to assist the Executive Office of the President (EOP), the NSC, the Office of Science and Technology Policy, and the Office of Management and Budget (OMB) in the exercise of wartime and non-wartime emergency telecommunications responsibilities, and to become the coordinator of NS/EP communications planning and provisioning to the Federal Government during all situations and circumstances. The NCS' mission expanded again in 1998 as a result of Presidential Decision Directive 63, *Protecting America's Critical Infrastructure*, to reflect an increased role in critical infrastructure protection and homeland security activities.

The September 11, 2001, attacks on the World Trade Center and the Pentagon marked a new era for the country as well as for NS/EP communications. As a result of these attacks, President George W. Bush signed E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, on October 8, 2001. This E.O. established the Office of Homeland Security and tasked the office with a multitude of responsibilities, including coordinating protection efforts for

both privately owned and public U.S. critical infrastructure information systems and coordinating rapid restoration of telecommunications and critical information systems after a terrorist attack. President Bush also signed E.O. 13231, *Critical Infrastructure Protection*, which established the President's Critical Infrastructure Protection (CIP) Board and re-established the NCS COP as a standing committee.

On November 25, 2002, President Bush signed the *Homeland Security Act of 2002*. This Act dramatically shifted the organization of Government by establishing the Department of Homeland Security (DHS) and reorganizing Government departments and agencies that held homeland security missions. In 2003, President Bush signed omnibus E.O. 13286, *Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*. This E.O. officially transferred the NCS Executive Agent responsibilities from the Department of Defense to DHS. Initially placed within the Office of the Under Secretary for Information Analysis and Infrastructure Protection, the Office of the Manager, NCS (OMNCS) eventually became part of the DHS Office of Cybersecurity and Communications (CS&C)—an element of the National Protection and Programs Directorate—under the *Department of Homeland Security Appropriations Act of 2007*.

NCS Environment

New Administration

During fiscal year (FY) 2009, the Obama Administration set out a number of goals it wished to address, many of which focused on NS/EP communications and cybersecurity issues. The President commissioned a 60-day cyber review to gather and analyze information on the cybersecurity of the Nation by analyzing the current status of networks within the public and private sectors. The NCS participated in this assessment by coordinating a response with organizations such as the President's National Security Telecommunications Advisory Committee (NSTAC). To develop its response, the NSTAC conducted a thorough examination of its past work and selected multiple recommendations that its members felt best addressed the Obama Administration's request, offering a wide range of ideas and priorities.

The results of the 60-day cyber review focused on the need for a national cybersecurity strategy, increased cyber research and development, and a cybersecurity response plan in which the Government and industry work together to mitigate potential cybersecurity risks. The NCS began to focus on analyzing the results of the review, and identifying cybersecurity areas and efforts where its capabilities can be best utilized.

Barack Obama became the 44th President of the United States on January 20, 2009. (Photo by Pete Souza)

The NCS and its programs were also highlighted in the Government Accountability Office's (GAO) report 09-022, *National Communications System Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened*, released in August 2009. Specifically, the NCS' roles as coordinator for Emergency Support Function 2 (ESF #2) and provider of the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) were highlighted. The programs were described as important support offerings that assist during disaster response, but they have encountered difficulty with cost and network congestion. Based on its findings, the GAO supported the development and implementation of an NCS Strategic Plan in order to clearly define methods for rectifying these issues. The GAO also recommended that the NCS further define performance measures that will successfully identify progress within the GETS and WPS programs. The NCS has begun to take steps towards addressing the issues raised by the GAO report and is continuing to strengthen the NCS Priority Service programs.

National Coordinating Center

The National Coordinating Center (NCC) reached a milestone in its involvement with NS/EP communications during FY 2009, celebrating its 25th anniversary. Since its inception, the NCC has provided a mechanism for critical information-sharing efforts between industry and Government in preparation for and response to national security events. The NCC—a 24x7 operation—continues to evolve in a variety ways, growing from a small membership pool operating in a circuit-switched environment to more than 50 members engaging in communications and cyber information sharing. During emergency events, the NCS acts as the coordinating agency for ESF #2, making the NCC, as the operational arm of the NCS, responsible for executing ESF #2 responsibilities and coordinating the restoration and provisioning of NS/EP communication services. The NCC continues to serve as the primary focal point for all NCS emergency response operations, and continues to provide a venue for industry and Government personnel to communicate requirements and receive status updates on the communications infrastructure during a response.

The NCC also collaborates with the National Cyber Security Division's (NCSD) U.S. Computer Emergency Readiness Team (US-CERT) through participation in daily information exchanges. During FY 2009, the NCC and US-CERT coordinated to address security issues presented by the Conficker worm by providing information on how best to protect systems from the malicious application.

In FY 2009, rising waters threatened to flood the Red River Valley in North Dakota. The NCC aided the Federal Emergency Management Agency's Disaster Emergency Communications team in its flood preparedness efforts. During preparation activities, the NCC communicated critical information to key officials and communications carriers regarding facilities that needed stacked sandbags to hold off flood waters. In addition, The NCC provided carriers with critical information about the location and time of detonations in the river, which were to break up ice blockages. The NCC's communication activities maintained awareness in a dangerous area and ensured the safety of industry personnel in North Dakota.

Technological Advancements and Testing

During the past fiscal year, the NCS continued to enhance its technology-based programs, particularly emphasizing the transition to the next generation network (NGN) environment. In response to the changing infrastructure, the NCS conducted and developed models and simulations to ensure the effectiveness of various priority service features in the event of a disaster. The OMNCS incorporated the results of the modeling efforts into the GETS/WPS program's industry requirements process and briefed those requirements at various CS&C conferences.

The OMNCS also conducted tests of GETS and WPS capabilities before, during, and after the 2009 Presidential Inauguration in Washington. These tests revealed valuable information regarding the call completion rate and frequency of use of these priority services. The results allowed OMNCS staff to identify areas that continue to successfully function as well as areas for improvement. For example, approximately 4,032 GETS calls were made from the Washington metropolitan area during the Inauguration weekend. The calls had a 99 percent call completion rate, which demonstrated the continuing successes of the program. Comparatively, only 1,615 WPS calls were made over the weekend, and many users experienced blocked calls because of access channel congestion. As a result, the service had a 65 percent call completion rate. The NCS is continuing to collaborate with partners to develop technical solutions to the WPS congestion issue. Over the upcoming year, the NCS will begin to build and test these solutions. Priority services continue to be an

President Barack Obama gives his inaugural address to a worldwide audience from the West Steps of the U.S. Capitol after taking the oath of office in Washington, January 20, 2009. (DOD photo by Senior Master Sgt. Thomas Meneguin, U.S. Air Force)

integral part of the NS/EP mission, and the NCS remains committed to improving these offerings based on evolving technologies and updated test results.

Prior to the inauguration, the Operational Analysis (OA) Team—part of the NCS' Critical Infrastructure Protection Branch—conducted a telecommunications infrastructure analysis focused on the examination of the public voice and data communications infrastructure sites involved in the inaugural areas. The OA team also examined the status of the telecommunications infrastructure along the inaugural parade route.

The NCS continued to work to examine and mitigate communications risks and vulnerabilities during FY 2009. To identify risks within key buildings' network infrastructures, the NCS conducted route diversity assessments in various DHS buildings in the Washington metropolitan area, and the Federal Bureau of Investigation's J. Edgar Hoover building. As a result of these tests, the NCS provided recommendations on how to improve those communications networks' route diversity.

Additionally, the NCS partnered with NCSD to perform research and data discovery efforts in support of the Trusted Internet Connection (TIC) initiative under the purview of Homeland Security Presidential Directive 23. The Trusted Internet Connections initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal Government's external access points (including those to the Internet). This consolidation will result in a common security solution which includes facilitating the reduction of external access points; establishing baseline security capabilities; and, validating agency adherence to those security capabilities. Agencies participate in the TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle.

NCS Partnerships

The NCS continues to collaborate with its industry and Government partners to examine NS/EP communications issues. These partnerships are critical to the NCS' information-sharing, emergency preparedness, and emergency response activities. The NSTAC examined a variety of critical issues from an industry perspective during FY 2009, including satellite security, the need for cybersecurity collaboration between industry and Government, and methods for mitigating identity theft risks. The NSTAC's reports and recommendations submitted during FY 2009 provided valuable information to the OMNCS, the NCS COP, DHS, and the EOP regarding these subjects.

During FY 2009, the COP's Communications Dependency on Electric Power Working Group (CDEP WG) completed its *Long-Term Outage Study*, in response to the NSTAC's *Report to the President on Telecommunications and Electric Power Interdependencies*. Additionally, the 24 COP members discussed a variety of key issues such as updating current NCS Directives, priority services communications updates and policies, and testing requirements under NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*.

During FY 2009, the Network Security Information Exchanges (NSIE) discussed the threats and vulnerabilities associated with the public network (PN) and identified ways to improve the overall security of the PN. The NSIEs held six bimonthly meetings during FY 2009 and participated in a variety of efforts, such as actively supporting a forum to address the recent sharp increase in circuit-card thefts in the United States and abroad. The goal of the ongoing NSIE-led effort was to identify the root cause of the problem and to determine whether the NSIEs could provide solutions. The forum worked closely with industry and Government partners to construct a database of stolen-card information that vendors could use to identify illicit material being sold. The NSIEs are currently planning their 2010 multilateral meeting, which representatives from the United States, Canada, the United Kingdom, Australia, and New Zealand attending this large-scale meeting.

The NCS also continued to coordinate the activities of the Communications Sector Coordinating Council (CSCC) and the Communications Government Coordinating Council (CGCC) to complete activities in conjunction with the goals detailed in the Communications Sector-Specific Plan (CSSP). The CSCC and CGCC also began to collaborate in preparation for the 2010 triennial rewrite of the CSSP, and the 2010 Sector critical infrastructure and key resources (CI/KR) protection annual report. The report highlights the sector's progress over the past three years related to CI/KR protection and risk mitigation activities.

NS/EP communications issues remain critical to the overall security of the Nation. The NCS is committed to ensuring the resilience of the Nation's infrastructure through information-sharing, partnerships, and technological advancements as it moves toward 2010.

2 Emergency Response Activities

All National Communications System's activities pursue a single goal—ensuring our Nation has the telecommunications services needed for responding to crises that jeopardize lives, property, or our country's national security and emergency preparedness posture. This section describes the impact of the National Communications System's emergency response activities on that critical objective.

Real events and emergencies are the true test of national security and emergency preparedness (NS/EP) telecommunications planning and response capabilities. Fiscal Year (FY) 2009 saw a number of large-scale events—most importantly, the Presidential Inauguration—where security and crowd-management activities were essential to the event's success and the ability to respond rapidly to an incident occurring during the event would be critical. The year also offered the usual types of emergency situations requiring a coordinated response, such as ice storms, floods, wildfires, earthquakes, and hurricanes. Under normal conditions, the absence of communications capabilities can be a substantial inconvenience, but under stressed conditions, the inability to communicate can threaten lives as well as the ability to govern and secure the Nation. As the descriptions of events and emergencies below illustrate, the National Communications System (NCS) provided the Federal, State, and local government agencies, and their industry and non-government organization partners, with the reliable, robust telecommunications capabilities they needed to protect our Nation, its citizens, and its resources.

Presidential Inauguration

The Inauguration of President Barack H. Obama represents an operational success for the Federal entities and private industry companies charged with protecting the President and the Nation's critical infrastructures. As many as two million people converged on the National Mall and along Pennsylvania Avenue in Washington to witness the Inauguration of the 44th President. Because of the record

Hundreds of thousands gather on the National Mall prior to the start of the 56th Presidential Inauguration in Washington, January 20, 2009. (DOD photo by Senior Master Sgt. Thomas Meneguin, U.S. Air Force)

crowds—and the potential impact any incident might have on communications critical infrastructure and key resources under these circumstances—the National Coordinating Center (NCC) for Communications was at the forefront of engagement with its Government and industry partners to ensure that NS/EP telecommunications services would be available to those who needed them.

The President's Inauguration was designated a National Special Security Event (NSSE) by the Secretary of Homeland Security. Upon designation, the United States Secret Service (USSS), in conjunction with other Federal departments and agencies, assumed its role as the lead Federal agency for the operational security plan. The NCS took part in a series of USSS and FEMA planning activities, to include participation in the Inaugural NSSE Critical Infrastructure Subcommittee.

Chris Geldart, Director, Office of National Capital Region Coordination, FEMA Headquarters, briefs former Department of Homeland Security Deputy Secretary Paul Schneider on security and safety measures in place for response as needed during the Presidential Inauguration activities in Washington. (Photo by Barry Bahler/FEMA)

In addition, Emergency Support Function 2-Communications (ESF #2) was activated for the event. The NCC coordinated with ESF #2 support agencies to provide logistics, personnel, and communications resources in support of Presidential Inauguration activities. The NCS also staffed seats at the USSS Multi-Agency Communications Center (MACC) and the FEMA Regional Response Coordination Center. Through its representatives at the MACC, the NCS verified and validated communications reports, and provided situational awareness through direct inputs from carriers. Before, during, and after the event, the communications infrastructure sustained unprecedented demands on the wireless infrastructure. Nonetheless, the infrastructure accommodated the high demand, with sufficient capacity to support first responders if an emergency had occurred during the event.

Winter Storms

In late January 2009, powerful snow and ice storms swept across the Midwest states, including Kentucky, West Virginia, Oklahoma, and Missouri. Storms left many residents without power and subsequently without communications, including wireline or wireless phone service. President Obama declared more than 90 counties as major disaster areas. In coordination with the Federal Communications Commission (FCC), the NCS activated the Disaster Information Reporting System (DIRS) for reporting communications outages. DIRS is a voluntary, web-based system under which communications service providers report communications infrastructure and service operational data to the FCC when requested (typically during times of crisis). Additionally, the Federal Emergency Management Agency (FEMA) deployed its Mobile Emergency Response System to assist the National Guard and State and local law enforcement agencies that had tactical communications needs.

Winter storms also hit the Northeast United States, including Vermont, New Hampshire, Massachusetts, and Maine. The ice storms shut down power and communications capabilities in the region. While ESF #2 was not activated, the NCS monitored the situation closely, by developing situation reports (SITREP), forwarding advisories, and requesting information on the developing situation and the subsequent response and relief efforts.

Red River Valley Floods

In response to a combination of heavy rain and spring snowmelts in March 2009, the National Weather Service issued flood warnings in the Fargo, North Dakota area.

Home owners sift through debris after wildfires destroyed their home in Mission Hills, Yorba Linda, California, December 12, 2008. (FEMA/Michael Mancino)

Statewide disasters were declared ahead of any flooding, but ESF #2 was not activated at the national level. To mitigate the flooding risk, local responders used sandbags to raise levees and built emergency dikes at danger points. Additional efforts included breaking up major ice jams acting as dams in an attempt to alleviate flooding.

The NCS coordinated with FEMA Disaster Emergency Communications personnel in FEMA Regions VIII and V to identify potential impacts to communications facilities at risk from the floods. Additionally, the NCS worked with communications carriers to ensure that no communications assets, including fiber lines running under the river, were damaged when clearing the ice blocks. In this instance, the NCS had two objectives—to ensure communications assets needed to respond to this emergency were protected, and to prevent damage to communications assets in this area from adversely affecting the overall telecommunications infrastructure. These carrier facilities received assistance for sandbagging and did not experience any communications impacts.

California Wildfires

In late August 2009, the California wildfires began in the Angeles National Forest and quickly spread throughout the surrounding area. The Angeles fire burned more than 250 square miles of land, making it the 10th largest fire in California since 1933. Three key communications locations—Mount Wilson, Mount Disappointment, and Mount Lukens—were at risk. These sites contain critical radio and television antennas, private land mobile radio towers, and other Government communications assets.

Although ESF #2 was not activated for this event, the NCS initiated its information-sharing process and distributed an RFI, an advisory, and subsequent SITREPs to convey the communications status of areas affected by the wildfires. Throughout the event, the NCS continued to coordinate with its Government and industry partners to assess and mitigate impacts to communications assets.

American Samoa Earthquake/Tsunami and Typhoon Melor

On September 29, 2009, the U.S. Geological Survey (USGS) reported an 8.0 magnitude earthquake in the Pacific Ocean near American Samoa. Following the earthquake, the USGS reported more than 30 aftershocks with magnitudes greater than 5.0. The earthquake resulted in a tsunami that caused significant damage to American Samoa. The events sparked widespread power outages across the island and affected approximately 6,000 customers. President Obama signed a disaster declaration for American Samoa for individual assistance, public assistance, debris removal, and emergency protective measures.

Responders from Federal agencies prepare to board a U.S. Coast Guard plane heading for American Samoa, September 30, 2009. (FEMA/Casey Deshong)

FEMA activated ESF #2 at both the national and regional levels. The NCS deployed personnel to the National Response Coordination Center in Washington, and the Region IX Regional Response Coordination Center in Oakland, California. Given the direct impact on the telecommunications infrastructure, exacerbated by the indirect impact caused by power outages, responders experienced difficulty establishing contact with individuals on the island during response activities. However, they overcame this obstacle by using NCS' SHAred RESources High Frequency Radio Program to contact an amateur radio operator on the island, who passed information on to other emergency responders. In addition, the NCS successfully used the Government Emergency Telecommunications Service (GETS) to contact local carriers and the local broadcast station responsible for Emergency Alert System capabilities to help coordinate the deployment of generators and fuel until commercial power was restored.

During the ESF #2 effort for American Samoa, FEMA also activated ESF #2 for Typhoon Melor, which subsequently developed into a Category 2 storm in the Western Pacific, threatening the Mariana Islands. Throughout the event, the NCC monitored the situation, and disseminated information through an RFI, an advisory, and SITREPs.

Hurricane Season 2009

The 2009 hurricane season was relatively calm and did not require the activation of ESF #2. By the end of the season on September 30, eight named storms had formed in the Atlantic Ocean, with only two designated as Category 3, or higher, hurricanes. Tropical Storm Claudette was the only storm to make landfall in the United States in 2009. In the Pacific Ocean, there were 16 named storms, six of which became hurricanes. Among these, Hurricane Felicia was the only storm that threatened to make U.S. landfall. However, Felicia eventually passed over Hawaii as a tropical depression, and the State sustained negligible impact to communications.

During the 2009 hurricane season, the NCS participated in a number of full-scale exercises in Florida, Louisiana and Texas in preparation for potential hurricane landfall.

Other Events

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:

- Potential Howard Hanson Dam flooding, January 2009;
- Super Bowl XLII, February 1, 2009;
- Presidential Address to the Joint Session of Congress, February 2009;
- Mount Redoubt, Alaska, eruptions, Spring 2009; and
- G-20 Economic Summit in Pittsburgh, Pennsylvania, September 2009.

The Presidential Address and the G-20 Summit were designated NSSEs. The NCC Watch notified and distributed SITREPs to Communications Information Sharing and Analysis Center (COMM ISAC) members during these events. In addition to these events, the NCC Watch responded to a number of cyber incidents, including the Conficker Worm incident in March 2009. The NCC Watch distributed requests for information (RFI), advisories, and SITREPs to COMM ISAC members. The Watch also coordinated with and provided situational awareness on NCS operations to incident response organizations, including the Department of Defense's Joint Task Force for Global Network Operations and the United States Computer Emergency Readiness Team.

3 NS/EP Telecommunications Support, Activities, and Programs

The ability of the National Communications System to fulfill its mission has significant implications for everyone in our country, whether for an individual—trapped under debris after an earthquake—or for the Nation—facing threats from terrorists. This section describes the Office of the Manager, National Communications System's actions in fiscal year 2009 to fulfill that mission.

The National Communications System (NCS) has a well-defined mission—*to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in…the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.*1

Among other characteristics specified by Executive Order (E.O.) 12472 establishing the NCS, the national communications infrastructure must…*be capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources [and must] [i]ncorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency.*[2]

To fulfill that mission and accomplish those objectives, the NCS takes into account:

- The complexity and extent of the communications infrastructure itself;
- The need to ensure a higher level of availability, reliability, robustness, and flexibility than that required for day-to-day operations; and
- The challenges of successfully coordinating with a diverse stakeholder community that includes Federal, State, local, and tribal governments (and, in some cases, foreign governments), non-government organizations, and private industry, when NCS has only moderate—if any—direct authority over its stakeholders.

To implement a strategy that encompasses these factors, the NCS created a structure that organizes activities in a way that optimally addresses the key aspects of its mission.

- **Technology and Programs Branch.** The dynamic technology environment presents both opportunities and challenges for the communications infrastructure, each of which must be addressed from a national security and emergency preparedness (NS/EP) perspective. For example, the growing availability of wireless communications is a tremendous advantage to emergency responders. However, such growth brings corresponding network congestion, a critical challenge during emergencies. NCS subsequently developed a Wireless Priority Service (WPS) for emergency officials and responders to give them priority access to congested wireless networks. The Technology and Programs Branch analyzes technology issues and identifies solutions, which are often implemented through NCS programs.
- **Critical Infrastructure Protection (CIP) Branch.** While the Technology and Programs Branch has a more forward-looking perspective—focusing on what the NCS needs to do tomorrow to keep up with a dynamic environment—the CIP Branch focuses on what the NCS needs to do today to protect the existing infrastructure. For example, the Network Security Information Exchanges (NSIE) address cybersecurity threats and vulnerabilities that affect the telecommunications

infrastructure. Contingency planning also falls within the purview of the CIP Branch, as does conducting training and exercises for emergency communications responders. Other activities focus on analysis that supports real-time emergency response activities. Often the CIP Branch's real-world experiences offer a view into the future, identifying both opportunities and challenges affecting emergency response capabilities, which are then addressed by the Technology and Programs Branch.

- **Plans and Resources Branch.** Within the NCS, the Plans and Resources Branch is responsible for providing centralized management and oversight to the Office of the Manager, NCS (OMNCS) for acquisition and financial matters, strategic and performance management planning, and resource allocation. This branch also interfaces between the NCS and its parent organizations—Cybersecurity and Communications (CS&C), the National Protection and Programs Directorate, and the Department of Homeland Security (DHS).

- **Customer Service/Government-Industry Planning and Management (GIP&M) Branch.** The most fundamental aspect of NCS' mission is coordination. The activities of both the Technology and Programs Branch and the CIP Branch involve substantial coordination with all levels of government and with industry. The Customer Service/GIP&M Branch supports the mechanisms facilitating that coordination—within the Federal Government; among the Federal, State, local, and tribal governments; and between the Federal Government and industry. The NCS Committee of Principals (COP) focuses on coordination among Federal departments and agencies. The President's National Security Telecommunications Advisory Committee (NSTAC) focuses on coordination between the Federal Government and industry. As the sector specific agency for communications, NCS coordinates among Federal, State, local, and tribal governments, and industry, under the auspices of the Customer Service/GIP&M Branch. This branch also handles external communications and affairs for the NCS, including outreach activities.

Section 3 presents the details about OMNCS' accomplishments during fiscal year (FY) 2009, describing each branch's NS/EP communications support focus, activities, and programs.

Technology and Programs Branch

The Technology and Programs Branch develops programs, technical studies, modeling capabilities/analyses, and standards that promote the reliability, security, interoperability, and priority treatment of NS/EP communications. Branch objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs and evaluating emerging technologies to alleviate impediments to interoperability. NCS provides this information to industry and international standards organization meetings to ensure that recommendations incorporate NS/EP communications requirements.

This section reflects how the Technology and Programs Branch contributes to the overall mission of the NCS, including highlights on the major projects, activities, and accomplishments undertaken by the Technology and Programs Branch during FY 2009.

Government Emergency Telecommunications Service (GETS)

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 priority access and processing in the local and long distance public switched telephone networks (PSTN). Although GETS did not reach full operational capability until September 30, 2001, it had earlier achieved initial operational capability and played an integral role in the response to the terrorist attacks on September 11, 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.

In addition to implementing priority treatment and enhanced routing features in the interexchange carriers' (AT&T, Verizon Business, and Sprint) and local exchange carriers' networks, the NCS worked with the American National Standards Institute (ANSI) to ensure NS/EP calls receive priority in the Signaling System 7 networks. ANSI approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993, which provided a classmark for NS/EP-related signaling messages. At least 90 percent of the access lines in the Nation now have the capability to process and enhance completion of GETS calls.

Functional Description

The GETS Program Office issues a GETS calling card to government officials, emergency responders, as well as designated industry and non-governmental personnel, which gives them priority access to NS/EP voice and voice band data services. 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 calls.

GETS Benefits to the NS/EP Community

The most significant NS/EP event of FY 2009 was the January 20th Presidential Inauguration. Unprecedented crowds descended upon the National Mall, necessitating law enforcement and intelligence officials at the Federal, State and local levels to coordinate tight control of the area's security. In any large-scale event, communications is critical for crowd control. The Inauguration offered rich opportunities for terrorists to mount an attack with maximum impact and visibility, given the large crowds, the high-profile individuals participating in the various events, and the symbolic importance of this event for our Nation. Therefore, reliable communications was critical for coordinating security activities for the event, and the OMNCS worked with emergency planners throughout the region to ensure that they would have the critical communications capabilities they needed to accomplish their missions.

In preparation, the GETS Program Office issued its first advisory on December 23, 2008, recommending all subscribers test their GETS cards prior to the Inauguration. Then, on January 13, 2009, the GETS Program Office issued its second Inauguration advisory warning of potential congestion in the PSTN during the Inaugural weekend. GETS program staff managed an increase in service requests for new GETS PINs from both the public and private sectors leading up to the Inauguration, which included requests from law enforcement agencies and high-ranking officials associated with the incoming administration. The NCS expedited 1,188 GETS PIN requests just prior to Inauguration day.

During Inauguration weekend (January 16–20), 4,032 GETS calls originated from the Washington metropolitan area. GETS performed as designed and thus provided authorized users a high call completion rate of 99 percent. On Inauguration Day, 771 GETS calls were placed within the Washington metropolitan area with a 99 percent call completion rate.

GETS served an ongoing role in emergency planning and response incidents throughout the year, including:

- In March, 2009, North Dakota experienced record flooding. The NCS expedited issuance of 88 GETS cards to North Dakota state and local government personnel to give them priority access to the communications services they needed to coordinate their response to this disaster.

- In late April 2009, the U.S. Department of Health and Human Services (HHS) declared a public health emergency for H1N1 flu. Those government organizations that would be responsible for responding to a significant outbreak took measures to ensure that they would have access to communications services needed to respond effectively, so many requested GETS cards in advance of a crisis. Consequently, the NCS experienced an immediate increase in GETS requests, including six requests for emergency PINs and 701 requests for new GETS cards. Most of these cards were requested by the Immigration and Customs Enforcement branch of the Department of Homeland Security (DHS) and by HHS to be distributed in emergency operations centers across the Nation.

FY 2009 Accomplishments and Improvements

In the past year, the GETS program continued to make significant progress in its outreach to all levels of government (Federal, State, and local) and other qualified NS/EP industry and non-profit organizations. At the end of FY 2009, there were 244,341 active GETS cards—an 18 percent increase since FY 2008. These numbers include 2,425 expedited activations that NCS Services Center personnel processed after normal duty hours. In addition, 30 emergency GETS PINs were distributed in FY 2009. PINs are provided when there is not sufficient time to mail a GETS card.

Table 1 GETS User Breakdown as of September 30, 2009

GETS NS/EP Category	GETS NS/EP Users
Federal	109,524
State/Tribal	27,567
US House and Senate	825
Local	51,850
Industry	52,881
Other NS/EP Organizations	1,694
Total	**244,341**

Highlights and Status of Ongoing Activities

NCS continues to expand GETS capabilities in the PSTN and participates in activities that facilitate these efforts:

The NCS is working with additional service providers to provide GETS capabilities in their networks. Providers include Shenandoah Telecommunications Company, Fairpoint Communications, Panhandle Telephone Cooperative, and Alaska telephone companies. The NCS is also in discussions with several more service providers to obtain agreements to deploy GETS capabilities.

As the PSTN evolves to next generation networks (NGN), the NCS continues to work with Sonus Networks to enhance NS/EP features in its NGN products. In furtherance of this goal, Sonus completed PSX software development, in support of Resource Priority Header (RPH) and HPC services, in FY 2009.

The NCS continues to participate in the Alliance for Telecommunications Industry Solutions (ATIS) Network Interconnection Interoperability Forum (NIIF) to promote NS/EP communications needs. The NCS works with the ATIS NIIF on inter-carrier network signaling and management procedures used during times of network traffic congestion.

Partnership Activities

Consistent with the NCS' mandate to coordinate with all levels of government and with industry, the GETS Program Office issues GETS cards to stakeholders throughout the NS/EP community, giving them priority access to NS/EP communications services. GETS helps ensure that these stakeholders have ready and reliable access to communications services to fulfill their NS/EP responsibilities:

- **Federal Departments and Agencies.** Federal departments and agencies have various responsibilities related to continuity of government (COG), continuity of operations (COOP) national security and emergency preparedness and response. They are also responsible for ensuring the continuing performance of their own mission-critical functions during crises.

- **State and Local Agencies and Organizations.** State and local government organizations and officials have responsibilities similar to those of Federal departments and agencies, but with a focus on their own jurisdictions.

- **Private Sector.** The private sector owns and operates the vast majority of critical infrastructures, such as nuclear facilities, regional and national airports, ports, railroad, communications, and information technology. Even those components of the critical infrastructures owned or operated by the Federal Government have substantial dependencies on the critical infrastructure elements owned and operated by the private sector, such as those within the communications and electric power sectors. Therefore, it is critical for the private sector to have communications capabilities to coordinate the restoration of damaged critical infrastructure elements.

- **International.** Both the Departments of Defense and State have facilities worldwide that depend on NS/EP communications capabilities. Likewise, the U.S. financial services sector interacts not only within the United States, but also with international central banking entities. Officials of our international allies, including Canada and the United Kingdom, also need reliable communications with their counterparts in the United States.

Wireless Priority Service (WPS)

WPS is a nationwide wireless telephone service that interoperates with GETS and provides priority NS/EP telecommunications via selected commercial mobile radio service (CMRS) providers. Like GETS, WPS supports NS/EP emergency response and recovery operations.

WPS provides end-to-end nationwide wireless priority communications capabilities to authorized NS/EP personnel during natural or man-made disasters. WPS also supports emergencies that cause congestion or network outages in the commercial cellular network. WPS is 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 networks.

Photo courtesy of photodisc®

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) enabling WPS to be developed.

During the days following the tragic events of September 11, 2001, the National Security Council (NSC) issued guidance to the NCS regarding the development and implementation of WPS.[3] In response, 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. Events of this magnitude offer opportunities for terrorists to launch an attack with maximum impact and visibility, as has been the case in previous Olympics. By December 2002, the NCS had achieved nationwide WPS capabilities within the first carrier network available, T-Mobile.

NS/EP users can currently subscribe to WPS in all of the major wireless markets in the continental United States and in U.S. territories served by the major nationwide carriers (AT&T Mobility, Sprint Nextel, T-Mobile, and Verizon Wireless).

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 prefix plus the destination number to originate and authenticate a WPS call.

WPS provides queuing to congested PSTN interfaces for calls originated at a mobile switching center (MSC) and traversing another carrier's network. Queuing is also applied when terminating a WPS call into a cell where all radio channels are busy, regardless of whether the call traverses the PSTN or simply connects within the same MSC. WPS and GETS integration provides end-to-end priority treatment for NS/EP calls, including calls that originate, transit, and/or terminate in wireless and/or landline networks.

WPS priority functionality in the commercial cellular networks includes priority-based radio access queuing, trunk queuing, priority-based radio egress queuing, and enhanced routing schemes, while preserving the capability for public access.

The requirement for nationwide WPS coverage necessitated enlisting multiple carriers and multiple access technologies. WPS is available in both of the access technologies most widely available in the United States—Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). The NCS continues to work with regional carriers to provision WPS. Full operational capability requirements for GSM are complete.

By defining a standards-based priority queuing capability, the IP (Internet Protocol) Multimedia Subsystem (IMS) Industry Requirements (IR) process provides a method that allows NS/EP personnel to use the Nation's cellular telecommunications networks without interfering with the public's use of these networks during such times. 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 continuously proved to be effective for the NS/EP community. In preparation for the 2009 Presidential Inauguration, the WPS Program Office issued its first advisory on December 23, 2008, recommending that all subscribers test the WPS capability on their phones prior to the Inauguration.

On January 13, 2009, the WPS Program Office issued its second Inauguration Advisory warning of probable wireless congestion during the Inaugural weekend. WPS Program staff expedited 3,678 requests for WPS to Federal, State, and local government and private industries in the Washington metropolitan area. These requests ranged from Federal agencies, including the incoming White House Administration and the Federal Bureau of Investigation (FBI), down to local-level medical centers and police and fire departments.

During the 2009 Presidential Inauguration weekend (January 16–20), 1,615 WPS calls originated from the Washington metropolitan area with a 65 percent completion rate. On Inauguration Day, January 20, over one million people crowded onto the National Mall to observe President Barack Obama's swearing-in. On that day, 658 WPS calls originated from the Washington metropolitan area with a 60 percent call completion rate. These calls experienced extreme congestion (many blocked), indicating access channel congestion.

Photo courtesy of iStockphoto®

WPS was also used to support the response to record flooding in North Dakota in March 2009. The NCS processed 52 expedited requests for WPS activation for State and local government personnel in the affected areas. With the public health emergency caused in April by the H1N1 flu, the NCS activated WPS on four to six cell phones for Federal personnel responsible for responding to a potential pandemic.

FY 2009 Accomplishments and Improvements

In the past year, the WPS program continued to make significant progress in its outreach to all levels of government and other qualified NS/EP industry and non-profit organizations. By the end of FY 2009, there were 98,942 authorized WPS users—a 17 percent increase since FY 2009. These numbers include 1,285 expedited activations that NCS Service Center personnel processed after normal duty hours.

Table 2 WPS User Breakdown as of September 30, 2009

WPS NS/EP Category	WPS NS/EP Users
Federal	70,823
State/Tribal	5,202
US House and Senate	73
Local	9,428
Industry	13,351
Other NS/EP Organizations	65
Total	**98,942**

Additional WPS accomplishments during FY 2009 include:

- Completed testing and deployment of the WPS CDMA Nortel/Motorola interoperability specification (IS) solution in both the Verizon Wireless and Sprint PCS Nextel (CDMA) networks;
- Continuing Alltel (now Verizon Wireless) IS market upgrades;
- Achieved Cellcom WPS CDMA full operational capability;
- Completed documentation and development efforts (Ericsson) for Universal Mobile Telecommunications System (UMTS) Directed Retry Handover (DRH) solution with relevant vendors—Nokia Siemens Networks, Alcatel-Lucent (Lucent and Spatial products), and Nortel;
- Finalized IRs and issued a Request for Proposal (RFP) for a WPS Enhanced Overload Performance Solution;

- Coordinated with major wireless carriers regarding expanded wireless service capacity in support of the Presidential Inauguration;
- Held kick-off meeting and executed a "Letter of Understanding on WPS Interoperability" with Industry Canada regarding international WPS cross-border roaming;
- Completed functional testing between U.S.-based GSM carriers and Rogers Wireless of Canada to expand NS/EP cross-border service and international interoperability; and
- Completed inter-carrier roaming testing with Cellcom and Cellular South.

Activities begun in FY 2009 and continuing into FY 2010 include:

- Working with T-Mobile to expand WPS coverage in former SunCom areas not previously supported—North and South Carolina, Puerto Rico, and the U.S. Virgin Islands.

Highlights and Status of Ongoing Activities

The NCS completed WPS CDMA Nortel/Motorola IS solution development and testing; Verizon Wireless (including some former Alltel IS markets) and Sprint PCS (CDMA) networks have successfully deployed this solution. CDMA WPS IS development, begun in 2007, was completed in July 2008 in time for deployment in the relevant Verizon Wireless markets for the 2008 political conventions. In addition, Qualcomm's CDMA-based QSec-2700 Secure Phone Release 4 software, with WPS Timer Extension, is now available.

With the completion of the activities above, full IS network deployment and WPS full operating capability was achieved in April 2009 for Verizon Wireless (excluding some Alltel IS markets) and in September 2009 for Sprint PCS (CDMA).

Many of the significant challenges facing the WPS Program stem from technology upgrades, requiring the NCS to assure continued availability of WPS capabilities as wireless carriers move to third generation (3G) wireless technologies. The UMTS DRH functionality is an example of this effort to extend existing WPS to NS/EP community users using 3G UMTS handsets. DRH solutions from a number of vendors, such as Nokia-Siemens Networks and Alcatel-Lucent, completed product testing and are awaiting captive office testing. The remaining vendors of note, Nortel and Ericsson, joined the DRH effort in FY 2009. Following completion of Ericsson DRH development efforts, captive office testing for all the above-listed vendors' equipment is scheduled for the fourth quarter of calendar year 2009.

In cooperation with Industry Canada as it prepares for the 2010 Winter Olympic Games in Vancouver, British Columbia, the NCS and Industry Canada have executed a "Letter of Understanding on WPS Interoperability" to define the framework regarding cross-border interoperability between U.S.-based and Canadian-based WPS providers. To this end, the NCS continues to coordinate cross-border roaming testing, issue resolution, implementation, and operation activities.

Partnership Activities

Like GETS, the OMNCS coordinates WPS use with the principal groups within the Executive Office of the President (EOP) and serves NS/EP users within the Federal, State, and local governments, and other qualified NS/EP organizations. The community supporting NS/EP mission requirements includes industry and non-government emergency response organizations plus industry owners and operators of critical infrastructures. Further, as with GETS, 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 Mobility, Sprint Nextel, Cellcom, Cellular South, Southern LINC, T-Mobile, Verizon Wireless, Hewlett-Packard, Alcatel-Lucent, Motorola, Ericsson, Nokia-Siemens Networks, Nortel, and Qualcomm.

NS/EP Priority Services in Next Generation Networks (NGN)

Historically, NS/EP priority services (GETS and WPS) were specified, engineered, and implemented based exclusively on circuit-switched technology. However, in recent years market forces have combined with advances in technology to cause an industry-wide evolution away from the existing public switched telephone network to an IP-based technology, known as NGN, that will allow not only telephone (voice) communications but also video and media (such as messaging, browsing, text, and images). The new NGN technologies will offer communications companies cost savings and vastly enhanced transmission capacities, in addition to enabling new services for consumers. To continue providing NS/EP users with the

Photo courtesy of iStockphoto®

capability to communicate during crises, the legacy NS/EP priority communications services (GETS and WPS) must also transition to NGN.

The NCS initiated a set of activities to define and deploy priority capabilities for voice communications in the packet-network environment similar to the priority capabilities currently available in the circuit-switched networks. In anticipation of the emerging transition of the circuit-switched public telephony networks to the packet infrastructure of the NGN, the NGN NS/EP Priority Services Program (PSP) addresses the convergence of voice, video, and data networks while continuing the mission of the current generation NS/EP PSP Program.

Functional Description

The NCS expects the invocation of priority voice for NGNs to be very similar to that of GETS and WPS described previously. Because the current dialing methods for both GETS and WPS will remain the same in the new network technologies, the transition of GETS and WPS will be seamless and transparent to the users.

The NCS envisions priority video services as extensions of corresponding commercial video services. Public video services will enable subscribers to establish video sessions with other subscribers. The subscriber initiating the session may use a method similar to those used to make a traditional voice call, by dialing a number unique to the subscriber with whom he wants to establish the session. Alternatively, these sessions may be set up through Web- or message-based requests.

Messaging services include several forms of store-and-forward communications such as electronic mail (e-mail), instant messaging (IM), and short message service/multimedia message service (SMS/MMS). The priority messaging service will permit an NCS-authorized subscriber to send messages to a destination user (who may or may not be a priority-services subscriber), and to retrieve messages that have been received from other users (who may or may not be priority-services subscribers). The priority nature of the communications implies that priority-services subscribers can successfully and expeditiously send and receive messages, even in situations when non-priority users may be experiencing severe service degradation.

Priority data access services will provide priority treatment to NS/EP users' Web browsing to ensure near-normal service performance in virtually all circumstances. Achieving this result will require both: (a) priority treatment during request/response processing by the data server(s); and (b) priority treatment in the transport of data packets between user device and server.

Given the inability to determine which applications will be critical in the future, the functionality of a transport priority, independent of the application, will differ from the other priority data services in that it provides this priority treatment for transport but not for service processing. Priority transport treatment is expected to be provided not only to bearer packets that carry the voice, video, or data associated with the service, but also (and perhaps more importantly) to the packets that carry the signaling messages used to set up and control each priority session.

Regardless of the type of priority service, the invocation of any priority treatment by an NS/EP user will require user authentication—whether done automatically via pre-subscription (like the WPS model), or manually via user entry of authorization information such as a PIN (as used in the GETS model) or a password.

NGN Effects on the NS/EP Community

The effects of the NGN effort on the NS/EP community are twofold. First, the evolution of today's networks from circuit- to packet-switching will require updates to the current GETS and WPS priority voice services to maintain the current level of availability and reliability. Second, NGN capabilities will enable the addition of priority data and video applications not available today, expanding NS/EP user mission capabilities in all critical situations. Continued

development of NGN Priority Services will ensure the NS/EP community can engage in state-of-the-art priority voice, video, and data communications over NGNs.

FY 2009 Accomplishments and Improvements

Working with accredited standards organizations (such as ATIS), service providers, and equipment vendors, the OMNCS completed the development of the priority voice service (Phase I) IR for the IMS core network. To implement GETS/WPS functionality onto carriers' NGNs, the OMNCS also began to develop and standardize IR for priority voice and video in the wireline, wireless and satellite access networks. Phase I of the Access IR effort is expected to be completed by December 2009.

Working with AT&T, the OMNCS continued development of an NS/EP packet priority capability over AT&T's Voice over IP (VoIP) and common backbone networks. It also completed the planning, definition, and design for a path priority capability.

The NCS continues to collaborate with industry to analyze and experiment with new technologies applicable to NS/EP services. NCS activities include (but are not limited to):

- Developing an IMS prototype lab to assess the feasibility of NS/EP video service;
- Modeling and analyzing NGN Priority Services;
- Attending the President's NSTAC 2008 Research and Development Exchange Workshop, 2009 Voice of Network (VoN) Convergence Conference and Expo, and 2009 Wireless CTIA to evaluate advances in services technology and promote consideration of priority services for advanced technologies;
- Prototyping, evaluating and demonstrating satellite services applicable to NGN Priority Services; and
- Developing and analyzing engineering prototypes:
  - NCS co-hosted one of the two North American test sites of the Global MultiService Interoperability event, a global test event interconnecting test sites in Asia (China and Korea), Europe (the United Kingdom), and North America. During this GMI event, the NCS prototyped and demonstrated the ability to achieve anonymity in the IP environment, inter-domain transfers (necessary to support toll-free destination numbers on GETS), priority implementation on call forwarding and on 3-way calls, priority video telephony, and priority video teleconferencing.
  - NCS collaborated with Sprint-Nextel's Advanced Technology Laboratory in Burlingame, California, to develop a proof-of-concept prototype of NGN priority voice and video services on an IMS platform.

The NCS continues to support its cause in standards, as illustrated by the accomplishments below:

- Continued the standardization of its IMS Core NS/EP IR in ATIS;
- Collaborated with Cisco to standardize the priority "EF-ADMIT" code-point in the Internet Engineering Task Force (IETF);
- Provided a representative to serve as the elected Vice Chair of the MSF Services Working Group;
- Received the MSF's Award of Excellence;
- Participated in the ATIS annual meeting of the committees (AMOC); and
- Provided an IETF draft contribution on session initiation protocol (SIP) overload control

The NCS described its NGN priority services activities and obtained feedback from the NS/EP community at the 3-day NGN GETS Plenary held June 9–11, 2009, in Herndon, Virginia. The NCS briefed the community about its recent access IR activities and obtained feedback from the community on many topics.

Highlights and Status of Ongoing Activities

The NCS is currently working with industry to:

- Continue the development of detailed service descriptions for NGN priority services such as video conferencing, Web browsing, and e-mail;
- Develop the IRs for NGN priority service access requirements for seven access technologies;

- Update the IMS core network requirements to align with the forthcoming access requirements;
- Collaborate with Sprint-Nextel's Advanced Technology Laboratory to develop Phase II of a proof-of-concept demonstration prototype of NGN priority voice and video services on an IMS platform;
- Collaborate with the MSF Services- and Management Advisory working groups to develop a suite of priority services-oriented network measurements, to be tested and evaluated in 2010; and
- Work with network-equipment vendors and carriers on the technical specifications of the Nortel CS2000 softswitch, which will comply with NGN Priority Services requirements and help implementation.

Partnership Activities

The NCS is participating in standards development organizations and fora such as ATIS, Third Generation Partnership Project (3GPP), and the IETF, to ensure that the appropriate standards include the needs of NGN Priority Services.

The NCS continues to participate in the activities of the MSF, to include hosting one of the two North American test sites of the Global MSF Interoperability (GMI) testing event. GMI 2008, held in early FY 2009, interconnected test sites in Korea, China, the United Kingdom, and North America. The NCS and industry partners demonstrated proof-of-concept priority capabilities that address NGN priority services needs such as video teleconferencing, media packet priority, anonymity in the IP environment, priority 800 calling, and priority three-way calling. The NCS demonstrated these features using commercial NGN equipment.

The NCS will continue joint development of NS/EP solutions with industry partners—an approach also used during the development of the GETS and WPS programs. This will ensure the continued availability, as well as the enhancement, of priority services to NS/EP users for years to come.

NS/EP Standards Development

Presidential E.O. 12472, *Assignment of NS/EP Telecommunications Functions*, directs the NCS to develop standards "…for minimizing or removing technical impediments to the interoperability of government-owned and/or commercially-provided telecommunications systems."

Further, Office of Management and Budget (OMB) Circular A-119 directs the Government to adapt industry standards committees' products and participate in their development. The NS/EP Standards Team works with a number of national and international standards organizations to ensure evolving commercial standards are poised to support NS/EP communications.

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

Engineers designed traditional NS/EP communications services around the circuit-switched infrastructure of the PSTN; however, public networks are now merging with packet-switched infrastructures and evolving into converged NGNs. As this evolution continues to mature, commercial standards stemming from technologies based on packet-switching, such as IP-based networks, will guide future priority communications services.

The Institute of Electrical and Electronics Engineers (IEEE) 802.16 Broadband Wireless Access Working Group is working on Project 802.16m—Amended Working Document. The NCS is participating in the technical development of this standard to ensure that the Worldwide Interoperability for Microwave Access (WiMAX) network's air interface supports NS/EP priority access.

The WiMAX Forum is a non-profit organization that certifies and promotes the compatibility and interoperability of broadband wireless products based on harmonized IEEE 802.16 and ETSI HiperMAN standards. The NCS completed the ETS Stage 1 Phase 1 Requirements (with Release 1.5 Air Interface) in the Service Provider Working Group (SPWG). It is working on the ETS Stage 1 Phase 2 Requirements (with Release 2/IEEE 802.16m Air Interface) in the SPWG.

The NS/EP Standards Team provides direct support to the U.S. State Department by chairing the International Telecommunications Advisory Committee Study Group 'B.' Individual team members also serve as senior Government advisors and leaders, such as head of delegations, to a variety of international and national meetings on NGN developments. In addition to this study group, team members participate in the work of various commercial/industry standards development organizations including:

- Alliance for Telecommunications Industry Solutions (ATIS);
- Telecommunications Industry Association (TIA);
- International Telecommunication Union, Telecommunication Standardization Sector (ITU-T);
- Internet Engineering Task Force (IETF);
- TeleManagement Forum (TMF);
- Third Generation Partnership Project (3GPP); and
- The Institute of Electrical and Electronics Engineers (IEEE).

In concert with the organizations listed above, team member participation includes:

- Conducting studies, performing analyses, sponsoring industry/academic research and development of new technologies for potential NS/EP applications;
- Firmly establishing NS/EP technical requirements in standards work programs, in cooperation with industry and academia;
- Developing and providing detailed technical proposals—such as NS/EP technical contributions—within industry standards programs, encouraging industry participants in these programs to make technical proposals to augment NCS proposals;
- Encouraging and promoting independent testing and implementations of proposed technical solutions; and
- Participating in the development of contemporary communications industry acquisition tools, such as service level agreements (SLA) and associated application notes for IP-based services, to specify criteria for availability, reliability, and quality performance of delivered NS/EP communications services.

The NS/EP Standard Team participated in several standards bodies during FY 2009, where progress was made in a number of areas:

- ATIS;
- ITU-T Standards Developments
  - *(ITU-T Study Group [SG] 16).* An initial set of requirements for the Advanced Multimedia Systems for next generation and other packet-switched networks have been finalized and include support for the national security and emergency preparedness priority services.
  - *(ITU-T SG 13) 2009.* Progress was made on developing new proposed Recommendation Y.2205R1 (Next Generation Networks—Emergency Telecommunications—Technical Considerations)
  - *(ITU-T SG 9) 2009.* Progress was made on developing three draft recommendations to enable priority (GETS-like) communications using integrated broadband networks; and
- IETF Requests for Comments (RFC)
  - Progress was made on three draft RFCs, specifically:
    - Differentiated Services Code Point draft-IETF Capacity-Admitted Traffic
    - Draft-IETF Quality of Service Attributes for Diameter
    - IETF Resource Reservation Protocol (RSVP) Extensions for Emergency Service.

The NCS-led IP IMS access IR effort is continuing with a focus on various access technologies. The wireless work to address UMTS, Long-Term Evolution (LTE), and CDMA 2000 technologies is tightly coupled with the ongoing work activity in both 3GPP and 3GPP2. Scheduled for completion in December 2009, the output from the IMS IR process is brought into 3GPP and 3GPP2 as contributions in order to ensure that the developing specifications meet the NCS' NS/EP requirements. Listed below are some of the inputs into 3GPP and 3GPP2 for 2009:

- *3GPP TS 22.153, Multi-media Priority Service (MPS), Stage 1 (Release 8).* Updated to align with the NGN GETS IMS Core Network IR for trusted domain support;

- *3GPP TS 22.153, MPS, Stage 1 (Release 9).* Updated to align with the NGN GETS IMS Core Network IR for trusted domain support and mapping of priority levels across an Network-to-Network Interface;

- *3GPP TS 23.203, Policy and Charging Control (PCC) Architecture (Release 8, Release 9).* Updated to align with the NGN GETS Access IRs to reserve a range of eight Allocation-Retention-Priority (ARP) levels for priority services, including MPS;

- *3GPP TS 21.201, Technical Specifications and Technical Reports relating to an Evolved Packet System (EPS) based 3GPP System (Release 9).* Updated to include support for MPS in EPS (LTE);

- *3GPP TS 22.278, Service requirements for the EPS, Stage 1 (Release 9).* Updated to include support for MPS in EPS (LTE);

- *3GPP TS 21.202, Technical Specifications and Technical Reports relating to the Common IP IMS (Release 9)* updated to include support for MPS in Common IMS;

- *Reservation-Priority AVP.* Initiated collaboration with European Telecommunications Standards Institute to extend AVP to 15 values to align with the NGN GETS Access IRs; and

- *SC.R5003-0 Version 1.0 Date: 2 April 2009-3GPP2 Vision for 2009 and Beyond.* Codified Priority Services Requirement in 3GPP2 futures services document.

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 [NS/EP] communications objectives."

Network Design and Analysis Capability (NDAC)

Because of the NS/EP community's heavy reliance on the PSTN, the NDAC was developed to analyze current U.S. networks and technologies, and evaluate the need for additional capabilities. The NCS has invested more than 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 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 communications infrastructure? What impact will the convergence of traditional circuit-switched networks with packet-switched/IP-based networks have on NS/EP requirements? The NDAC suite includes a number of tools.

A county road in Oxbow, North Dakota has been washed away after the Red River flooded. Oxbow citizens are preparing for the possibility of additional flooding later in the week. (Photo by Patsy Lynch/FEMA)

Infrastructure Mapping Tool (IMT). This tool is a geographical information system (GIS) situational awareness tool used for both pre-event planning and analysis and post-event response. IMT provides analyses of critical infrastructures for incident management, decision support, and status tracking. When an event occurs that has the potential to disrupt network infrastructures, IMT can create detailed infrastructure analyses for specific geographic areas of concern. IMT layers near real-time data over infrastructure data pulled from numerous proprietary and government databases. The results can be used to define the scope of impact, create specific impact area views, run initial assessment reports, create up-to-date visualizations of asset status, and conduct telecommunications impact analyses relevant to specified users, businesses, and government agencies.

Communications Network Analysis Tool (CNAT). This communications analysis tool queries Central Location On-line Entry System (CLONES) data and displays the results on a map. Originally developed for the Department of Defense Mission Assurance Division (DOD MAD), CNAT is shared with the NCS to complement and extend the NDAC tool suite. Analysts can perform the basic CNAT functions through a GIS interface, support telecommunications queries, and import the results to various applications for presentation to key decision makers to generate impact assessments on a timely basis.

Traffic Analysis of Critical Federal Telecommunications Infrastructures. The Networx Pricer Infrastructure Module is a tool that enables traffic impact analyses using FTS2001 and Networx data to interactively view an agency's traffic inventory and perform critical infrastructure/sensitivity analyses if a telecommunications facility is disabled. Using this capability, the NCS performed proactive analyses, such as agency-specific critical infrastructure analyses for NCS COP department and agencies, to include graphical mapping to determine how a disabled point-of-presence (POP) or wire center might affect Government traffic. The capability also provides proactive cross-agency regional characterization analyses for cities throughout the Nation, improving the ability to provide immediate critical telecommunications assessments for NCS emergency response purposes. Used for support during critical events and exercises, these capabilities are available for ad hoc analyses requested by the NCS. Such ad hoc analyses include the on-going Internet connectivity tracking analysis and monitoring NCS' progress toward the OMB's Trusted Internet Connection (TIC) goal to limit each Federal department and agency Internet connections. The NCS also developed a feature to assess diversity options available under the General Services Administration's (GSA) Networx contract; this feature will be available to all Federal Networx customers.

Internet Analysis Capability. This capability provides situational awareness from both architectural and traffic perspectives by incorporating Government off-the-shelf software (GOTS) and commercial off-the-shelf software (COTS) products that can determine the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure. With an increasing number of Government NS/EP customers using services offered through the Internet, models of the Internet's logical and physical infrastructures are now required to support NS/EP analyses. This on-going NDAC expansion includes packet-switched networks and tools (for example, Internet Analysis Tool [IAT], Network Discovery Tool [NDT], and ScoutVision) to enable the NCS to:

- Capture physical and logical interdependencies among Internet Service Providers (ISP);
- Identify network anomalies and determine their impact on communities of interest;
- Characterize the relationships and interdependencies among ISPs and other infrastructure providers;
- Integrate and correlate internal and external routing, inventory, and activity data, and scale to include any computer network related data source;
- Access and collect global Internet routing data that provides at a minimum 90 percent coverage of usable Internet capacity;
- Collect and visualize netflow data for malicious activity investigation;
- Visualize global and local networks with functionality similar to Google Earth; and
- Provide both an interface for operational analysts and a management interface for operations center managers.

Trusted Internet Connection (TIC)

Internet Analysis Capability (IAC) support requirements have increased sharply in situational awareness reporting and assistance with network vulnerability issues. In particular, the NCS leveraged the IAC to provide analytic support for comprehensive assessments of external network and Internet connectivity to meet requirements issued by the National Cyber Security Division's (NCSD) TIC Compliance Validation Program, established by Homeland Security Presidential Directive 23 (HSPD-23), *Cyber Security and Monitoring*. The collaborative efforts of the NCS and NCSD help verify information provided to the TIC Program Office and highlight ramifications agencies may be facing in complying with TIC mandates.

In support of TIC compliance analysis, the NCS developed a customized analytic methodology and unique tools and processes tailored to meet NCSD's needs. IAC tools and datasets provide a holistic view of Federal networks, which

enables a better understanding of consolidation points associated with the TIC initiative. In addition, the IAC has the capability to develop 'dashboard' analytic portfolios to help monitor TIC access point security and network performance. By collecting data from external vantage points, the NCS has provided NCSD with agency-specific analyses as well as holistic assessments of the Federal Government's cyber capabilities, identifying its dependencies on critical sectors and prioritizing its top assets.

Priority Services Modeling (PSM)

The convergence of the PSTN's circuit-switched architecture of the PSTN with the Internet's packet-switched technologies is changing the communications infrastructure that formed the basis for NCS programs and analyses. As the infrastructure changes, NDAC tools and methodologies must evolve to enable continued analyses of NS/EP priority services during their transition to NGNs. The NDAC PSM team must address multiple new questions introduced by this evolution, including:

- Will these new architectures be able to support viable communications at 10 times 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 priority services?
- How will the program ensure priority voice, data, e-mail, video teleconferencing, and other multimedia services are provided by the carriers?

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 NS/EP priority service programs' IR process;
- Briefed at various DHS CS&C conferences, such as the GETS Team Forum and IR Plenary Forum; 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 to produce modeling studies to aid the decision making processes associated with the GETS and WPS programs. So far, the NCS has produced four studies/reports:

- *Evaluation of Call/Session Establishment Performance Values from IMS IR;*
- *Effectiveness of Throttling Algorithms to Protect Against Denial-of-Service Attacks;*
- *Survivability Dependence on Internetwork Routing Policies for NGN Priority Services;*
- *A Dynamic Algorithm to Prevent CDMA WPS Overload;*
- *NCS Internet Analysis Landscape;* and
- *End-to-End Priority Services Modeling/Testing of WiMax Model and IMS Core.*

The results of these and other modeling studies of major wireless access technologies will quantify the effectiveness of proposed priority service mechanisms and feed policy and budgetary decisions related to both the GETS and WPS programs.

Committee for Foreign Investment in the United States (CFIUS) and FCC's Team Telecom

The NCS frequently participates in reviews conducted by interagency policy coordination groups such as CFIUS and Team Telecom. These groups' objectives are to evaluate critical infrastructure risk caused by globalization of the communications sector and to respond to the unique policy challenges created as the United States continues to simultaneously encourage foreign investment and balance security priorities. This work involves conducting critical infrastructure analysis to identify key communications assets and associated vulnerabilities, and providing technical analyses of commercial communications mergers, acquisitions, and license applications by foreign companies.

Route Diversity Project

The Route Diversity Project helps Federal departments and agencies ensure that their communications networks are resilient. The Route Diversity Methodology (RDM) is an

assessment of the last-mile connection between an agency's onsite communications infrastructure and the service provider's Central Office or POP, which is one of the most critical and vulnerable parts of voice and data networks. NCS applied its RDM to the FBI's Hoover Building and three DHS CS&C sites. Completed actions include:

- Coordinating with DHS and the FBI to set up kickoff meetings and identify points-of-contact for information gathering;
- Gathering information from open sources, NCS proprietary datasets, and interviews with knowledgeable personnel at the FBI and DHS;
- Performing a risk analysis to identify focus areas for mitigations; and
- Recommending long-term mitigations that require service provider cooperation and short-term mitigations for FBI and DHS action.

Technology Assessment and Data Analysis Cell (TADAC)

The NCS maintained a fully-accredited facility with the capability to:

- *Evaluate contract deliverables.* Provided a facility to evaluate the hardware and/or software deliverables of some contracts for acceptance purposes;
- *Evaluate products.* Provided a platform to research, identify, and evaluate COTS and GOTS products that may satisfy specific NS/EP requirements, often obviating development contracts;
- *Host applications and databases.* Provided 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 included the NDAC—a set of tools, data sets, and methodologies that enable modeling and analysis of the PSN;
- *Provide surge support.* Provided an environment in which the modeling and analysis capabilities generally provided by a variety of contractors were replicated, allowing additional surge support personnel to provide on-site analysis during disaster response and recovery as well as during National Level Exercises (NLE);
- *Conduct component-level simulations.* Provided the ability to simulate the behavior and interaction of individual pieces of software and hardware;
- *Develop community research projects.* Enabled 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 the expertise of engineers and computer scientists in critical areas and increase the respect and recognition of the NCS within research and development circles; and
- *Support training.* The TADAC provided an environment to support ongoing hands-on technical training, an alternative to expensive vendor-provided training.

The facility closed in March 2009 because of CS&C space constraints; however, some of the capabilities it provided are still available, as described below.

Technology Assessment Network (TAN)

The TAN is a suite of equipment enabling PSN analyses in support of the Federal Emergency Management Agency's (FEMA) Emergency Support Function 2-Communications (ESF #2). Primarily intended to provide a surge capability, the NDAC portion of the TAN replicates the modeling and analysis capability generally provided by a variety of contractors, except that certain proprietary data sets are not available. The TAN also hosts applications, databases, and Web-based tools, and provides a highly advanced training platform. Most of the TAN functionality transitioned to the NCS' CIP Branch.

eXperimental Testbed Environment (XTE)

The XTE can emulate a scaled-down version of the Internet, converged network service provider networks, and enterprise networks. Operators first simulate severe congestion on both the network and NGN end systems, and then test and validate that emergency communications services work properly from end-to-end, using call load generators, traffic generators, and associated customized call processing systems to address the work around the congestion. The XTE is a test environment that uses the following components:

The NCS eXperimental Testbed Environment facility, located at CSC in Chantilly, Virginia. (Photo courtesy of MSF)

- Network devices (routers and switches) that simulate an ISP's backbone/core and access network;
- Security devices (authentication systems, firewalls, session border controllers, and intrusion detection capabilities) that protect network assets by enabling access control and by detecting and responding to simulated threats;
- Hosts and servers, which enable the invocation and termination of NGN Priority Services;
- Test and analysis equipment to generate voice, video, and data traffic and to gather results of the effects of congestion on NGN Priority Services and service elements;
- VoIP telephones and systems to represent a VoIP service provider's infrastructure; and
- Video endpoints and systems to access scaled-down IMS core NGN network service platforms with NS/EP functionality.

Operations and management of the XTE transitioned to the NGN Priority Services group in the 4th quarter of FY 2009.

Advanced Technology Group (ATG)

The ATG leads the effort in identifying vulnerabilities of legacy and emerging communications systems to Telecommunications Electromagnetic Disruptive Effects (TEDE) and focuses on identifying vulnerabilities or opportunities in communications systems to benefit NS/EP. The ATG supports multi-agency efforts to improve the national emergency communications infrastructure by addressing topics such as the impact of electromagnetic pulse (EMP) on telecommunications, evolving technologies, alert response, communications architecture, and communications dependencies on electric power. These activities are described below.

Telecommunications Electromagnetic Disruptive Effects (TEDE)

Title 5 of the Code of Federal Regulations (C.F.R.), Part 215, designates the Executive Agent of the NCS as the Federal Government's focal point for EMP technical data and studies concerning telecommunications. 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 continues to coordinate and conduct studies in the following areas:

- Susceptibility of the telecommunications infrastructure to EMP;
- Approaches to protecting telecommunications systems 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;
- High-power microwave vulnerability tests of supervisory control and data acquisition (SCADA) systems, PSTN switching systems, local area networks, and computer systems (in conjunction with the Congressionally-funded 'live fire' exercises);

- Tests to determine the disruption of fiber-optic telecommunications links resulting from secondary effects associated with high energy illumination;
- Internet systems vulnerability tests; and
- Aviation transportation communications systems vulnerability tests.

The ATG performs these studies in partnership with the Air Force Research laboratories and private industry, sharing results confidentially with participating companies who use the test results to modify their system components to be TEDE resistant within known parameters.

Companies owning and operating associated systems in the communications infrastructure are encouraged to participate in these collaborative efforts.

NCS continues to represent DHS as a guest subject matter expert to the Congressional EMP Commission.

Emergency Communications and Evolving Technologies Studies

The ATG evaluates the ability of different modalities of communications to support NS/EP purposes, including satellite or advanced terrestrial systems, and continues to support upper management as the subject matter experts in sudden advanced communications technologies issues. These include, but are not limited to, positioning navigation and timing (PNT), satellite communications, wireless, and landline networks.

The ATG identified vulnerabilities to: airborne passenger information networks; undersea cable communications; telecommunications power dependencies; timing issues of networks; broadband cellular; IP television (IPTV) implications for telecommunications; and multimedia traffic in cellular networks and the PSN.

Studies support ongoing efforts by governmental and industry working groups to maintain robust communications networks for NS/EP purposes

Warning Alert Response Network (WARN) Act

Americans increasingly rely on wireless telecommunications services and devices to receive critical, time-sensitive information anywhere, anytime. To ensure the ability of the Nation's wireless carriers to transmit timely and accurate alerts, warnings, and critical information to cell phones and other mobile devices, an FCC Commercial Mobile Service Alert Advisory Committee (CMSAAC) developed requirements by forming working groups composed of industry and Government personnel.

ATG staff participated in development of the Cellular Mobile Alert Service (CMAS) requirements and in the Alert Interface Group (AIG) chartered under the CMSAAC to develop CMAS interface requirements. As a result of the CMSAAC team effort, the FCC adopted a First R&O in support of the WARN Act.[4]

Transformational Communications Architecture (TCA)

The ATG supports the development of the DHS contribution to the National Security Space Office (NSSO) Transformational Communications Architecture (TCA). The TCA is an ongoing space transport-level architecture that works in concert with the Global Information Grid (GIG) to: (a) help synchronize multiple acquisitions; (b) promote standards and interoperability; (c) deliver time-phased capability in an evolutionary approach; and (d) support information architecture concepts that enable critical information sharing needs. The TCA involves: DOD's communications satellites; the U.S. Intelligence Community; commercial mobile satellite services (MSS) and fixed satellite services (FSS) services leased by DHS and the National Aeronautics and Space Administration (NASA); satellite communications (SATCOM) terminals; terrestrial infrastructure (teleports and gateways); and network management and information assurance tools and technology to control the space assets and their connectivity with the ground infrastructure.

NCS Committee of Principals Communications Dependency on Electric Power Working Group (CDEP WG)

The critical imperative to ensure NS/EP communications necessitates studies to analyze the scope and nature of the communications infrastructure's dependence on the electric power infrastructure in both short-term and long-term outage situations, and the vulnerabilities to NS/EP communications created by such outages. National emergencies such as the 2003 Northeast blackout and Hurricanes Katrina and Rita in 2005 have heightened the awareness of the interdependence of these two infrastructures. The communications industry needs electric power to operate its systems and provide communications services; the electric power industry needs communications capabilities to coordinate restoration of the electric the power infrastructure. When both infrastructures are simultaneously damaged by such disasters, the results can

have a devastating impact on everyone involved in emergency response efforts—to include emergency health care workers, law enforcement, and any other organizations that provide aid to disaster victims.

In December 2006, the President's NSTAC published its report to the President on *Telecommunications and Electric Power Interdependencies, The Implication of Long-Term Outages (LTO)*. The report provided industry's recommendations on the actions required to address the interdependencies between these two critical infrastructures.

NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, and Continuity Communications Architecture (CCA)

In order to ensure the ability of the Federal Executive Branch to communicate under all conditions, two directives mandate the continuity communications requirements all departments and agencies are obligated to achieve:

- National Security Presidential Directive 51/Homeland Security Presidential Directive 20 (NSPD-51/HSPD-20), *National Continuity Policy*, May 9, 2007; and
- National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 25, 2007.

NSPD-51/HSPD-20, National Continuity Policy

On May 9, 2007, the President issued the National Continuity Policy (NCP) in NSPD-51/HSPD-20 to establish and maintain a comprehensive capability composed of COOP and COG programs ensuring the preservation of our form of government under the Constitution and the continuing performance of national essential functions (NEF) under all conditions. The four key areas addressed include Federal Executive Branch department and agency leadership, staff, communications, and facilities.

The DHS Secretary, as Executive Agent of the NCS, is responsible for developing, implementing, and maintaining a comprehensive Continuity Communications Architecture (CCA).

The CCA is an integrated, comprehensive, interoperable framework of continuity communications requirements, based on the needs of departments and agencies for communications enabling them to perform their primary mission essential functions (PMEF) in support of NEF, during both routine and continuity conditions. The CCA objectives include surveying departments and agencies on current and future continuity communications needs, conducting gap and overlap analyses, and developing recommendations to improve departments' and agencies' voice, data, and video capabilities. These improvements will ensure that communications and business systems—including hardware and software for continuity operations—mirror those used in day-to-day business to allow continuity leadership and staff to make a seamless transition to crisis operations.

Based upon CCA development guidance from the Office of Science and Technology Policy (OSTP), the NCS will develop, implement, and begin maintenance of a CCA. The CCA will include the minimum requirements necessary to finalize selection of a secure communications system by the Defense Department.

National Continuity Policy—Highlights and Status of Ongoing Activities

In the past year, the NCS has made significant progress in developing analytical capabilities in preparation for departments' and agencies' surveys and subsequent analyses, in particular, NCS has:

- Conducted proof-of-concept testing of the data capture tool with DHS' Business Continuity and Emergency Preparedness (BCEP) Team in support of the development of DHS mission-essential functions (MEF) and primary MEFs (PMEF);
- Enhanced data capture tools to support mandated business process and impact analyses; and
- Conducted gap and overlap analyses of National Continuity Coordinator-approved PMEFs and *Continuity of Operations (COOP) Communications Plan* (CCP) data.

NCS Directive 3-10 Minimum Requirements for Continuity Communications Capabilities

NSPD-51/HSPD-20 requires the incorporation of continuity requirements into daily operations of all departments and agencies. NCS Directive 3-10 establishes the minimum communications requirements (non-secure voice, data and video, mobile/in-transit backup communications, and priority access and restoration services) for Federal departments' and agencies' headquarters and continuity alternate operating facilities. The intent is to establish a

Federal inter-agency communications baseline of minimum requirements that support the execution of PMEFs and enable senior leadership to collaborate, develop policy recommendations, and act under all circumstances. In addition, NCS Directive 3-10 requires the departments and agencies to produce a quarterly compliance report and to participate in monthly tests of the operational capabilities at their headquarters and all alternate operating facilities.

The OMNCS publishes supporting implementation guidance, conducts testing, develops a quarterly compliance report, and submits annual recommended NCS Directive 3-10 updates to the NCS COP and the Executive Agent. A COOP Communications Managers Group (CCMG), established in December 2004 and co-chaired by the NCS Manager and FEMA, provides a forum to address departments' and agencies' COOP communications issues, including NCS Directive 3-10 implementation planning, compliance testing and reporting, and interoperability.

Minimum Requirements for Continuity Communications Capabilities—Highlights and Status of Ongoing Activities

In the past year, the NCS has made significant progress in supporting the departments and agencies in implementation activities by publishing implementation guidance including:

- NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Access Networks*, February 20, 2009; and
- NCS COP revisions to NCS Directive 3-10, April 7, 2009, for OSTP's consideration. The NCS has also been conducting monthly communications testing and developing quarterly reports on compliance with NCS Directive 3-10. The objective for the new fiscal year is to sustain progress in releasing directive updates and subsequent implementation guidance to the departments and agencies.

Critical Infrastructure Protection Branch

As noted earlier, the CIP Branch focuses on what the NCS must do today to protect the existing infrastructure. This branch provides feedback to the Technology and Programs Branch on needs that arise in the real-world environment and then takes advantage of tools and methods initiated by the Technology and Programs Branch to meet those needs. The CIP Branch supports a number of ongoing efforts to achieve its objectives. It also engages in several ad hoc, issue-driven activities. The following pages describe those efforts and activities and how they have supported the NCS' mission during FY 2009.

Network Security Information Exchanges (NSIE) Activities

In 1991, the NCS and NSTAC recommended the establishment of an industry-Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NCS and NSTAC formed separate Government and industry NSIEs to exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network (PN) and its supporting infrastructures.

In FY 2009, the NSIEs held six joint information sharing meetings and several ad hoc sessions to discuss topics of interest to members. These topic included digital forensics, protection of critical infrastructure information, netflow analysis, and the NSIEs' security priorities. During FY 2009, the NSIEs made frequent use of the United States Computer Emergency Readiness Team (US-CERT) secure portal to collaborate when urgent security concerns arose.

The NSIEs also engaged in international outreach activities. In FY 2009, representatives from the United Kingdom and Canadian NSIE organizations participated regularly in the U.S. NSIE meetings. In April 2010, the United States will host the NSIE international meeting to include multi-lateral information sharing among representatives from the United States, the United Kingdom, Canada, Australia, and New Zealand.

Over the last year, the NSIEs have leveraged their domestic and international partnerships on a number of efforts that have improved the security of the PN. In early 2008, NSIE members established a forum to address the recent sharp increase in circuit card thefts, both in the United States and abroad. The goal of the ongoing NSIE-led effort was to identify the root cause of the problem and to determine whether or not the NSIEs could collectively provide solutions. The forum worked closely with industry and Government partners to construct a database of stolen card information that vendors could use to identify illicit material being sold on the market. The group continues to engage major vendors and is working on deploying a Web interface for the database.

Periodically, the NSIEs assess the risks to the PN from electronic intrusions; they completed the last risk assessment in 2007. The NSIEs currently are developing their latest assessment on how changes in technology and the overall environment in the past 2 years have affected the network. The NSIE issued this risk assessment in August 2009.

Contingency Planning (CP) Team

The CP Team focuses on developing doctrine and operational plans within the CIP Branch. The team also translates these plans into tools and learning aids to effectively disseminate key concepts, roles, and responsibilities to emergency communications team members.

Contingency Planning

The CP Team focuses on contingency communications planning and has primary responsibility for developing and publishing the ESF #2 Communications Annex to the *National Response Framework* (NRF), the ESF #2 Standard Operating Procedures (SOP), the NCS COOP Plan, the COOP Multi-Year Strategy and Program Management Plan (MYSMP), and numerous communications support documents:

- The SOP augments the NRF's ESF #2 Communications Annex, which replaced the National Response Plan. The SOP defines the organizational structures that form when FEMA activates ESF #2 in response to an incident. It further 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 mission essential functions (MEF) that must be performed to continue the NCS mission from an alternate location should NCS primary facilities become uninhabitable for a prolonged period of time. The NCS MEFs support DHS' priority mission essential functions, which supports the President's NEF. The Plan identifies personnel, critical business processes, interoperable communications, interdependencies/stakeholders, vital records, critical business processes, and other essential elements associated with relocation and requirements to perform NCS MEFs.

- The MYSMP defines the NCS roadmap for developing a viable COOP capability over the next five 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.

Regional Communications Coordinators (RCC)

Since Hurricane Katrina in 2005, RCCs have assisted their respective FEMA regional staffs in establishing and executing regional emergency communication coordination working groups (RECC-WG) as directed by Congress in U.S. House of Representatives Resolution (H.R) 5441, *Department of Homeland Security Appropriations Act of 2007*. This legislation established the Office of Emergency Communications (OEC) as well as the RECC-WGs, which the NCS supports to improve awareness and visibility of regional communications interoperability issues across the Nation. RCCs also began a data collection effort to identify nationwide procedures for access, fuel provision, and security for individual States and territories. The NCS designed this effort to provide industry with quick references and accurate points-of-contact for re-entry procedures for restoration crews immediately following any type of incident.

The RCCs have proved to be a valuable asset to the FEMA Joint Field Offices (JFO) as well as to State Emergency Operations Centers during recent disaster situations. In addition to working with States during disasters, the RCCs work to make States aware of the various Federal programs and planning efforts available to them for use in their preparedness, response, and restoration planning efforts.

Members of the armed forces and FEMA during a daily briefing in the Emergency Operations Center in St. Paul, Minnesota. Planning the response to any disaster takes teamwork and open communications; this meeting is in response to flooding along the Red River in western Minnesota on April 1, 2009. (Mike Moore/FEMA)

Operational Analysis (OA) Team

The OA Team serves as the focal point for developing assessments to help ensure the availability of NS/EP communications services under all conditions and hazards. In FY 2009, the OA Team focused on developing analytic products that addressed risks to national communications and provided infrastructure protection recommendations and support. Additionally, the OA Team continued to improve the quality, comprehensiveness, and timeliness of communications analysis products. Initiatives conducted during FY 2009 include standing up the Analysis Response Team (ART), conducting exercises, developing regional characterizations, developing short-term analytical products, and analyzing risk and dependencies. These activities are described in greater detail below.

Analysis Response Team (ART)

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, Federal Government, and industry. To address that need, the NCS established the ART. Led by the Chief of the OA Team, the ART can bring together analysts from the NCS CIP Branch, the NCS Technology and Programs Branch, DOD, the FCC, members of the communications industry, and other support elements. Each participant brings a unique set of knowledge, skills, and data that jointly contribute to a comprehensive analysis of the communications infrastructure. During an emergency response event, the ART will be activated to meet the operational needs of the National Coordinating Center (NCC) manager. During this reporting period, the ART was activated for several hurricanes during the 2008 hurricane season. In addition, the ART continued to refine a set of SOPs to ensure that all members are well prepared to respond to emergency events.

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 fully prepare to produce quality analytic products in a real-time environment to help protect and restore the Nation's critical infrastructure during the preparation, response, and recovery phases of NS/EP emergencies.

To ensure an adequate response to such events, the NCS develops government and industry exercises around specific scenarios to test and improve response and recovery capabilities. During FY 2009, the OA Team participated in planning, conducting, and evaluating multiple exercises to test and evaluate its analytic capabilities in response to various scenarios. The OA Team supported both pre- and post-impact scenario exercise analyses, used models to identify potential impacts to the communications infrastructure.

During this reporting period, the OA Team provided support for a number of activities, including: FEMA, Washington State, US Army Corps of Engineers (USACE), and Department of Energy (DOE) 2009 Dam Sector Exercise Series; the Presidential Joint Telecommunications Resources Board's (JTRB) Radiological Dispersion Device Table Top Exercise (RDD TTX); the DHS-OSTP 2009 Presidential Inauguration 2 Kiloton Blast exercise; FEMA's Eagle Horizon exercise; the Vancouver 2010 Olympics Planning nuclear scenario; the 2009 Florida Statewide/FEMA Region IV hurricane exercise; and the FEMA Region VIII Wasatch Fault catastrophic planning activities. The OA Team provided support for these exercises both on-site in the NCS TADAC and at alternate locations.

Regional Characterization

To improve the ability to provide critical communications assessments quickly and accurately—especially during an emergency response operation—the OA Team initiated a series of in-depth regional communications infrastructure characterizations throughout the country. These characterizations addressed the interactions between the communications infrastructure and various other infrastructures and sectors within the region assessed. These characterizations are intended to establish and document a comprehensive understanding of communications services supporting NS/EP missions in high-risk areas prior to an emergency event. This process significantly reduces the preliminary research and data gathering time normally associated with any analysis.

As part of these characterizations, the OA Team is coordinating with key NS/EP stakeholders to better understand their individual communications 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 communication assessments.

During FY 2009, the OA Team completed characterization studies in seven metropolitan areas (Houston, New Orleans, St. Louis, Jacksonville, Tampa, Boise, and Salt Lake City), the State of Hawaii, the Territory of Puerto Rico, and the entire Gulf Coast (including the State of Florida and all coastal zones of Mississippi, Alabama, Louisiana, and Texas). The OA Team also continued to update FY 2006, FY 2007, and FY 2008 characterizations of 10 metropolitan areas (San Francisco, Miami, Philadelphia, Boston, Chicago, Dallas, Seattle, Atlanta, New York City, and Norfolk), the National Capital Region, and the New Madrid Seismic Zone to incorporate updated findings, data, and design, and to provide the most accurate and relevant understanding of high-risk areas. In addition, the OA Team coordinated with the General Services Administration (GSA) regional managers to introduce products, capabilities, data, and methodologies and to gather suggestions and recommendations for product improvements.

Short-Term Analysis Activities

During FY 2009, the OA Team conducted short-term analyses supporting quick-turnaround information requests and emergency response operations. The OA Team used a flexible and repeatable analysis framework with defined processes and procedures, which enabled quick-turnaround capabilities. In this quick-turnaround capacity, the OA Team collaborated with the NCC to provide analyses of the communications infrastructure and determined communications impacts resulting from various classes of events.

During this reporting period, the OA Team provided support for analysis efforts such as Alaska's Undersea Cable Analysis, continuing Hurricane Ike restoration efforts, the Sprint-Cogent peering severance and federal agency isolation assessment, the 2009 Presidential Inauguration telecommunications analysis, the March 2009 Northwest flooding analysis, Infrastructure Protection's Regional Resilience Assessment Program (RRAP) efforts, and the April and July 2009 California fiber cut assessments. Following each event, the OA Team investigated lessons learned to review and update processes and procedures to ensure the readiness of the OA Team in providing quick-turnaround analytical support.

Risk and Dependency Analysis

In FY 2009, the OA Team continued developing a prototype study of the dependence of the NCS MEF on communications in five high-consequence scenarios defined by the OA Team: high-altitude nuclear burst; ground-based nuclear burst; solar superstorm; earthquake; and cyber attack. The study consists of conducting a series of analyses designed to support the NCS in its responsibilities to ensure continuity of communications for Federal departments and agencies in the event of a major disaster. Analysis results are intended to give the NCS a better understanding of communications infrastructure vulnerabilities and provide the basis for recommendations for infrastructure protection and support. The study also helps the NCS fulfill its duties associated with:

- The NSPD-51/HSPD-20, National Continuity Policy; and
- E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions.*

Operations Team

The Operations Team executes the NCS' ESF #2 role and coordinates the restoration and reconstitution of the communications infrastructure in concert with its government and industry partners. Additionally, the Operations Team is responsible for the day-to-day operation of the NCC, NCC Watch, the Communications Information Sharing and Analysis Center (COMM ISAC), and IT operational programs to include SHAred REsources High Frequency (SHARES-HF) Radio and Telecommunications Service Priority (TSP).

National Coordinating Center (NCC)

The NCC mission is "to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications service or facilities under all conditions, crises or emergencies." The NCC's strength lies in its long-standing relationships with its 24 Federal departments and agencies and 52-member COMM ISAC. As a government and industry body, the NCC plays a lead role in disaster response and recovery of NS/EP communications.

The primary vehicle within the NCC for monitoring and responding to emergent communications events is the NCC Watch. The NCC Watch provides 24x7 operations and maintains situational awareness on the health of the Nation's communications infrastructure. This includes managing the information sharing process, performing analysis, researching technical issues, and coordinating

and liaising with other Federal departments and agencies and the private sector. During a response, Government personnel communicate NS/EP requirements to industry and industry representatives provide the Government with expertise, resources, situational awareness, and status of the communications infrastructure.

Major NCC activities in 2009 include:

- 56th Presidential Inauguration;
- 2009 Presidential Address to Joint Session of Congress;
- 2009 Conficker Worm;
- 2009 Hurricane Preparedness Workshop;
- 2009 Situation Report (SITREP) Working Group;
- Eagle Horizon 2009 (EH09);
- NLE09; and
- Hurricane Felicia.

Communications Information Sharing and Analysis Center (ISAC)

Because the private sector owns and operates 90 percent of the Nation's critical infrastructure, the Federal Government must engage private industry in the government's NS/EP efforts. In accordance with Presidential Decision Directive 63 (PDD-63), *Protecting America's Critical Infrastructure*, which established the concept of the ISAC, the NCC was designated the ISAC for Communications on January 18, 2000. The NCC COMM ISAC's role is to facilitate the exchange of information between its government and industry representatives regarding vulnerability, threat, intrusion, and anomaly information affecting the communications infrastructure. The COMM ISAC represents the country's wireline and wireless service providers, equipment vendors, Internet service providers, satellite industry, and cable industry.

Major ISAC activities in 2009 include:

- 56th Presidential Inauguration;
- 2009 Conficker Worm;
- 2009 Hurricane Preparedness Workshop;
- 2009 SITREP Working Group;
- EH09
- NLE09; and
- Hurricane Felicia.

Operational Programs

SHAred RESources High Frequency (SHARES-HF) Radio Program

The SHARES-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 transmitting NS/EP information. It does so by bringing together existing high frequency radio resources of Federal and federally affiliated organizations, to include communications industry and critical infrastructure providers, when normal communications are disrupted or disabled.

The SHARES-HF Interoperability Working Group consists of more than 143 members representing 110 Federal organizations and key critical communications industries. The working group provides guidance and direction for the SHARES network and gives the Federal community a forum for addressing issues affecting HF radio. This body conducts four nationwide readiness exercises each calendar year to offer operational training to the more than 1,400 SHARES members. The overall exercise objectives are to

provide radio personnel training on operating procedures and various message formats, expand SHARES awareness within the Federal emergency response community, and improve the interoperability of new HF technologies.

Telecommunications Service Priority (TSP) Program

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

There are currently more than 218,000 active TSP assignments supporting NS/EP communications nationwide. During FY 2009, the NCS added, changed, or revoked more than 48,000 TSP codes. Additionally, the TSP user base increased by 184 new organizations, bringing the total number of organizations with active TSP codes to more than 1,200. More than 360 telecommunications carriers provide services with TSP assignments.

In addition to daily operations, the TSP Program Office supports presidentially-declared disasters, implementation of the National Response Plan, and ESF #2 and COOP activations. During FY 2009, the TSP Program Office assigned restoration and provisioning priorities for the following events:

- FY 2009 tropical storms and hurricanes;
- 2009 Presidential Inauguration;
- Northwest floods, Upper Midwest floods, Kentucky ice storm, Midwest tornados and floods;
- G-20 Summit;
- United National General Assembly 64;
- California Wildfires; and
- DHS Customs and Border Protection and Immigration and Customs Enforcement sensitive operations.

During FY 2009, the TSP Program Office hosted and facilitated a meeting of the TSP Oversight Committee (TSP OC). The purpose of the TSP OC is to identify, review, and recommend actions to correct or prevent systemic problems in the TSP System. Working with the TSP OC and associated working groups, the TSP Program Office continued to focus its efforts on resolving TSP operational issues and implementing recommendations to improve the efficiency and effectiveness of the TSP database. Several key issues discussed during the June 2009 TSP OC Meeting include the following:

- Recommendation from the *January 2007 NSTAC Report to the President on Emergency Communications and Interoperability* to explore enhancement of the TSP Program to accommodate requests from users of wireless telecommunications services at critical sites.
- Public utilities commissions' requests for vendor proprietary TSP data in their States.

Training and Exercise (T&E) Team

The T&E Team is responsible for ensuring that a cadre of skilled civilian and military reserve personnel are ready to provide emergency response support during crises and emergencies. During FY 2009, the T&E Team successfully planned, coordinated and performed the ESF #2 training and exercises and continued to sponsor the NCS Individual Augmentee Program (IMA). Details on these efforts appear in the following sections.

ESF #2 Training

The NCS is designated as a co-primary agency (along with FEMA) for implementing the ESF #2 Communications Annex of the NRF. ESF #2 supports the restoration of the public communications infrastructure and ensures the provision of Federal communications to support emergency response operations. In this role, the NCS ensures that our Nation's communications infrastructure can respond throughout any crisis or emergency condition. The ESF #2 missions are executed in response to any communications infrastructure crisis or emergency condition. In these situations, the National Emergency Communications Team supports the NCC and the Disaster Emergency Communications (DEC) Branch conducts field operations. The readiness level of these key ESF #2 components is sustained by ESF #2 Training Conferences and periodic distance training teleconferences.

From November 6–7, 2008, the NCS conducted an ESF #2 Winter Training Conference in McLean, Virginia, for more than 120 attendees. The Winter Training Conference objectives were to: review the year's disaster experiences; discuss the After Action Reports; and develop corrective

actions as required to advance the training and operational readiness of ESF #2 team members as part of the ongoing annual training cycle. The conference featured classroom presentations, panel discussions, and informal dialogue on topics related to the 2008 ESF #2 deployments, future activations, and the year's ESF #2 program developments.

The NCS held a workshop and tabletop exercise for DEC branch directors on November 5, 2008. This training session used a hurricane scenario as part of a Tabletop Exercise to discuss the roles and responsibilities of the DEC branch director (also referred to as a Federal emergency communications coordinator [FECC]). Lessons learned from the exercise resulted in revisions to the FECC job aid and the guidelines for management of the DEC Branch.

The NCS suspended sponsorship of the 2009 ESF #2 Spring Conference because of program funding limitations. However, to continue the training momentum that ESF #2 team members need to maintain readiness, the T&E Team, in conjunction with the ESF #2 Interagency Coordination Working Group (ICWG), decided to develop and present National and DEC branch team member training to ensure that all team members were prepared for deployment in support of ESF #2 operations before the 2009 Hurricane Season. The training would be conducted via traditional in-residence training and distance learning formats, some using a Webinar tool. During FY 2009, more than 15 training sessions and/or practical exercises were conducted to introduce various DEC Branch Team Job Aids and other emergency management topics such as:

- Team Deployment;
- ESF #12 (Energy);
- NCS Emergency Management Portal in the Homeland Security Information Network (HSIN);
- Organization of the DEC Branch;
- ESF #2 National Team Training;
- NCC Roles and Responsibilities;
- Federal Spectrum Management for Emergency Response Operations; and
- Project *Roll Call*.

ESF #2 Exercises

As a culmination of ESF #2 DEC Branch leadership training, the NCS sponsored a DEC leadership table top exercise on November 5, 2008, preceding the 2008 ESF #2 Winter Training Conference. This exercise validated ESF #2 Job Aids and SOPs, provided a practice environment for the new DEC Branch structure, and identified operational strengths and areas for improvement. This exercise identified corrections for documents (which were subsequently revised) and actions for further training.

The OMNCS participated in the annual EH09 COOP exercise directed by the White House on May 17, 2009. This non-scenario, internally-evaluated exercise focused on evaluating the OMNCS COOP. In coordination with the OMNCS, the FEMA National Continuity Programs Office incorporated a required continuity communications test element into Eagle Horizon for the first time. This element will be expanded in future EH exercises and will include improvements suggested in the EH09 After Action Report and Improvement Plan.

The OMNCS partnered closely with its Federal partners and the communications industry to plan and execute NCS responsibilities as a participant in NLE09 during June 28–30, 2009. The NCS demonstrated dedicated involvement in NLE09 by providing realistic, coordinated intelligence analyses, communications impact analyses, and regional operations to support the exercise play.

Currently, the NCS Training and Exercise Team is engaged in the national planning efforts for NLE 2010 (scheduled for May 2010 and featuring the effects of an improvised nuclear device detonation), NLE 2011 (scheduled for May 2011 and featuring an earthquake on the New Madrid Seismic Zone) and Cyber Storm III (scheduled for September 2010).

NCS Individual Mobilization Augmentee (IMA) Program

The NCS continued sponsorship of its IMA program, which provides a valuable resource of skilled Army Reserve personnel to augment communications response activities. This program offers the NCS a surge capability to deploy and react to a myriad of situations associated with ESF #2 operations. Some of these Army Reserve officers are communications professionals in their full-time civilian careers, and can apply their skills when responding to Federal emergencies. The IMAs may activate and deploy to support the NCS staff, or they may deploy to regional locations to help during disaster response and planning.

During FY 2009, NCS IMAs continued to support the ESF #2 Team during exercises and deployments. In response to the increased frequency and duration of duty deployments, the NCS IMA Unit increased its personnel strength to the current roster of 25 officers. Officers from the IMA Unit joined the NCS Regional Managers to represent ESF #2 in the following incidents and exercises: on-scene support of the 2009 Presidential Inauguration events; response to the 2009 Mid-West flooding; a regional exercise for a potential H1N1 influenza pandemic; a regional exercise for a potential New Madrid Seismic Zone earthquake; and the 2009 Texas Mobile Operations Exercise (MOBEX). The ESF #2 Winter Conference and distance training teleconferences were also important training events for the IMA Unit. These events provided opportunities for the military officers to train with their civilian team members who work with them during emergency operations.

A major training event during FY 2009 was the IMA Unit Training Weekend, which took place June 20–21, 2009, in Arlington, Virginia. To be fully functional in their assigned positions within the National team and DEC Branch, IMAs assigned to the NCS IMA Unit must attend an initial orientation that addresses: the organization and mission of the NCS; communications planning and operations in support of the NRF; NS/EP procedures; use of automated resources to manage and track NS/EP actions and prepare accurate, timely reports to summarize emergency operations; and the priority telecommunications programs that are provided to ensure the availability of communications services during an emergency. The purpose of this training event was to fulfill these training requirements and to prepare the IMAs for team assignments during the 2009 hurricane season (or any other potential incidents).

In addition, the officers participate in individual training sessions ('battle assemblies') and a 12-day annual training assignment to expand their knowledge and proficiency in emergency management by completing FEMA's on-line training courses, attending in-residence courses at the FEMA Emergency Management Institute, and participating in regional training events and meetings.

Plans and Resources Branch

The Plans and Resources Branch 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 Branch exercises authority and ensures accountability over all resources allocated to NCS programs.

The branch interfaces with the CS&C and DHS directorates on: financial and acquisition matters; DHS Planning, Programming, and Budgeting Execution (PPBE) System documentation and execution; and acquisition management. The branch 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 by developing business plans, performance plans, future year Homeland Security planning (FYHSP) documentation, advanced acquisition plans, and by providing 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-member departments and 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 branches 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/Government-Industry Planning and Management Branch

The Customer Service/GIP&M Branch is responsible for the most fundamental aspect of NCS' mission—coordination and partnership—which is crucial to the work of both the Technology and Programs Branch and the CIP Branch. The Customer Service/GIP&M Branch supports the mechanisms facilitating that coordination—within the Federal Government; among the Federal, State, local, and tribal governments; and between the Federal Government and industry. The following pages describe the mechanisms through which the NCS establishes and maintains its partnership with stakeholders throughout the NS/EP community.

National Communications System Committee of Principals/Council of Representatives

In 1963, President John F. Kennedy issued a Presidential Memorandum No. 252 to establish the NCS to provide better communications support to critical Government functions during emergencies. On April 3, 1984, President Ronald Reagan signed E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which superseded President Kennedy's original 1963 memorandum, and subsequently broadened the NCS' capabilities, expanding the NCS from its original 6 members to an interagency group of 24 Federal departments and agencies. E.O. 12472 also established the NCS COP, a Presidentially-designated interagency consortium through which all 24 NCS member departments and agencies provide advice and recommendations on NS/EP communications policy to the EOP.

Per E.O. 12472, the COP is designated as the forum in which NCS member departments and agencies review, evaluate, and present views on NCS programs or policies and other activities affecting the NS/EP communications environment. Each NCS member department and agency nominates and appoints a principal, at the assistant secretary or equivalent level, to serve as a member of the COP. Principals represent the positions of their respective parent organizations on policy, technical, and programmatic NS/EP communications issues and provide key subject matter expertise and written reports, comments, and recommendations to fellow COP members.

As William Belote (right) of the White House Office of Science and Technology Policy (OSTP) listens, NCS Deputy Manager and Director James Madon address issues on national security and emergency preparedness before the NCS COP meeting held June 10 in Arlington, Virginia. (Photo by Steve Barrett, NCS)

COP members are also charged with reporting on their organizations' NS/EP communications activities and providing recommendations to the Executive Office of the President, the Executive Agent of the NCS, and the Manager of the NCS. The NCS Manager presides over COP meetings, assisted by the NCS Deputy Manager.

NCS Manual 1-2-1, *Bylaws of the National Communications System Committee of Principals*, mandates that the COP meet at least twice per year. In practice, COP meetings occur on a quarterly cycle to provide members with an opportunity to engage in high-level discussions regarding policy development and collaborative activities in support of NS/EP communications.

During FY 2009, the COP met in October 2008 and January and June 2009 to discuss key NS/EP issues and challenges, such as Federal-level hurricane preparedness efforts and activities, domain name service vulnerabilities, NCS issuances, and continuity communications.

Exceptional work was accomplished by the COP's working groups, including the Priority Services Working Group (PSWG) and the CDEP WG. This increased level of engagement and activity subsequently generated a new level of visibility and prestige for the COP as a policy planning body.

Council of Representatives (COR)

The COP's permanent subordinate body, the Council of Representatives (COR), met in July and August 2009 to discuss how it can more effectively help the COP fulfill its NS/EP mission. COR members have valuable subject matter expertise in the NS/EP communications environment and often directly report to their COP Principals.

Bill Gunnels (left), the NCS COR member from the Defense Department, and Kim Godwin, the State Department representative to the COR, focus on a hurricane forecast presentation during a meeting of the NCS Committee of Principals held in Arlington, Virginia on June 10. (Photo by Steve Barrett, NCS)

During both the July and August 2009 meetings, the COR discussed the role of the COP as a senior-level, decision-making body and the COR as a working-level, implementing body. OMNCS aims to expand the COP and COR roles in the review and approval of NS/EP communications policy, response planning, and prospective programs. Specifically, OMNCS envisions that the COR will: conduct the initial examination of NS/EP communications initiatives or issues and report findings to the COP; provide oversight, guidance, and assistance to COP working groups; and vet issues that should be elevated for COP consideration and input. In addition, the COR has planned bimonthly meetings for members to discuss NS/EP issues or concerns, measure working group progress against missions and work plans, and conduct troubleshooting activities to ensure that work products meet the level of quality, expertise, and responsiveness appropriate for COP reports.

NCS COP Communications Dependency on Electric Power Working Group (CDEP WG)

In July 2007, the COP formed the CDEP WG to examine issues raised by, and relating to, the *NSTAC's Report on Telecommunications and Electric Power Interdependencies* (TEPI). The working group's mission was to examine issues raised in the NSTAC TEPI Report, and to work with the private sector to address the full set of NSTAC recommendations. Specifically, the CDEP WG set out to assess a broad range of concerns inherent in the Communications Sector's dependence on the reliable operation of the electric power sector.

During FY 2009, the COP's CDEP WG completed its charge by developing a final report and recommendations. This report consists of data collected during the COP's first-ever set of special events—the LTO Workshop and the Local Providers Workshop, during which members collaborated with key industry subject matter experts (SME) and members of academia to better inform their research. The Advanced Technology Group, which is within the NCS' Technology and Programs Branch, assisted in the CDEP WG's study and the facilitation of the CDEP WG's LTO Workshop.

The working group concluded that electric utilities are directed by State government officials on the priority for restoration of services while communications companies are driven by TSP agreements that are in place with their customers. Working group members also discovered that the two sectors typically work jointly to restore service at the State Emergency Operation Center level; however much of the coordination is performed on an ad hoc basis at the local level. Finally, access control and fuel availability issues must be resolved before an LTO occurs. In all, the CDEP WG developed a total of 39 recommendations for the DHS, NCS, COP, and the North American Electric Regulatory Commission to address. The NCS COP and NCS Manager approved the group's final report and will deliver it to the Secretary of Homeland Security and the President for their consideration.

Utility workers from Chattanooga, Tennessee, help their neighbors in Fulton, Kentucky recover from the January 26th ice storm by replacing numerous power poles. At the disaster's peak, more than 700,000 customers lost power. The lack of power inhibited these customers' ability to utilize everyday communications, such as landline telephones, in order to relay any need for help or supplies. (Photo by Dianna Gee/FEMA)

International Communications Working Group (ICWG)

During FY 2009, the COP's ICWG completed its charge to examine issues raised by the *NSTAC Report to the President on International Communications* and to address a series of the report's recommendations. The ICWG's mission centered on an assessment of the broad range of issues and requirements inherent to the establishment and global adoption of a framework to enhance the resiliency of the global communications infrastructure. ICWG members performed a gap analysis of the international communications efforts underway and identified existing joint-examination mechanisms in place for responding to all-hazard attacks. The ICWG also met with key industry representatives from the NSTAC International Task Force to clarify the intent of the NSTAC's recommendations. As a result of their investigations, ICWG members prepared a formal response on their findings to the NCS COP and the NCS Manager for review and approval. The ICWG concluded that existing entities should continue their present course to address the NSTAC recommendations without further ICWG involvement.

Priority Services Working Group

The COP established the PSWG in 2003 to assess and evaluate NCS priority service programs, including the GETS program, the WPS program, and the TSP program. In addition to evaluating these programs, the COP initially tasked the PSWG with examining priority service efforts, assessing cost issues, and analyzing the potential impact of future technologies on priority services programs.

During FY 2009, the PSWG discussed several key issues, including the need to: (1) conduct outreach to the tribal community regarding the benefits of enrolling in priority services programs; (2) engage in rule-making and revise certain outdated FCC Codes of Federal Regulation with respect to WPS and TSP; (3) develop proposed requirements for enrolling wireless carriers in the TSP Program; and (4) help the GETS/WPS Users Council facilitate routine testing of GETS cards and WPS devices by NCS member department and agencies.

In addition, the PSWG finalized its 2009 *Report on Telecommunications Service Priority* that discusses outstanding TSP issues, considers forward-looking matters, and identifies potential areas for future PSWG examination. This report supplements outstanding recommendations from the 2007 *Report on TSP*, and will be sent by OMNCS to the COP for review and approval.

NCS Issuances

As taken from NCS Directive 1-1, *NCS Issuance System*, the NCS Issuance System "governs the issuance of rules and guidance concerning the internal organization, policies, procedures, practices, management, and/or personnel of the NCS." As necessary, the COP continues to make recommendations to update existing NCS Issuances. The COP also reviews and provides comments on NCS Issuances in the development process.

NCS Issuances Review and Revisions Conducted during FY 2009

The following issuances are currently undergoing DHS internal review:

- Revisions to NCS Directive 3-11, *Government Emergency Telecommunications Service*; and
- NCS Directive 3-12, *Wireless Priority Service*.

The following issuances are currently in development:

- NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Access Networks*;
- NCS Manual 3-11-1, *Government Emergency Telecommunications Service Manual*; and
- NCS Manual 3-12-1, *Wireless Priority Service Manual*.

The OMNCS revised the following issuance as recommended by the NCS COP and submitted the suggested revisions to OSTP:

- NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* (October–November 2008).

The NCS COP reviewed and commented on the following issuance:

- NCS Directive 3-8, *Provisioning of Emergency Power in Support of National Security and Emergency Preparedness Telecommunications* (July 2009). OSTP asked the COP to determine if this directive's provisions were still valid. If so, members would then determine if NCS Directive 3-8 should be incorporated into NCS Directive 3-10. OMNCS will forward the final document to OSTP in the near future.

The OMNCS has received the following issuances and plans to submit them to the COP and COR for member review and comment:

- NCS Directive 3-1, *Telecommunications Service Priority (TSP) System for NS/EP*; and
- NCS Directive 3-13, *Communications Operations, Emergency Support Function #2-Communications, Mission Assignment Processing*
- NCS Directive 3-14, *Federal Reporting on National Security/Emergency Preparedness Telecommunications Impacts in Support of Emergency Support Function #2-Communications*

The President's National Security Telecommunications Advisory Committee (NSTAC)

E.O.12382, *President's National Security Telecommunications Advisory Committee*, signed by President Ronald Reagan in September 1982, established the NSTAC. The NSTAC consists of not more than 30 industry chief executives, each of whom is appointed by the President. Members represent major communications, network service provider, information technology, finance, and aerospace companies that provide advice to the President on NS/EP communications.

The NCS COR met on July 15 to re-invigorate their efforts as the working body of the NCS COP. The NCS plans to have the COR lead the Government NS/EP communications efforts, form working groups to address issues, and provide recommendations to the COP. (Photo by Steve Barrett, NCS)

The NSTAC held its annual meeting on May 21, 2009, in the Washington metropolitan area, to allow Principals an opportunity to confer with the President, receive feedback from Government stakeholders in both classified and unclassified settings, discuss and vote on NSTAC reports, and consider new issues for the upcoming work plan. During the 2009 NSTAC Meeting, the NSTAC Principals reviewed the activities of the past cycle, approved the *NSTAC Report to the President on Cybersecurity Collaboration* and the *NSTAC Report to the President on Identity Management Strategy*, and received briefings on DHS and FCC activities, cybersecurity, satellite security, and Government re-organization of executive national security functions. The NSTAC also met via conference call on November 6, 2008; February 10, 2009;

March 12, 2009; and August 11, 2009. Meeting topics included the *NSTAC Response to the Sixty Day Cyber Review Task Force*, IP-based NS/EP communications traffic, core assurance, identity issues, cybersecurity collaboration, NGNs, satellite security, legislative and regulatory issues, and the NSTAC work plan.

Industry Executive Subcommittee (IES)

During its monthly working sessions, the NSTAC's IES continued to identify communications issues critical to NS/EP activities for consideration by its subgroups. The NSTAC addressed a variety of issues, including: NS/EP IP-based traffic; cybersecurity collaboration; identity issues; core assurance; NGN; satellite security; 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 in subsequent sections.

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

- The Federal Advisory Committee Act;
- The Legislative and Regulatory Task Force (LRTF) 2008 Legislative and Regulatory Assessment;
- The Comprehensive National Cyber Initiative (CNCI);
- EMP attacks and solar storms;
- The Obama Administration and DHS NS/EP communications priorities; and
- The NCS COP's CDEP WG report, *Long-Term Outage Study*.

Physical Assurance of the Core Network

Following the 2008 NSTAC meeting, the NSTAC formed the Core Assurance Task Force (CATF) to: (1) examine infrastructure threats and issues concerning the physical aspects of core network security; (2) identify any existing deficiencies within core network physical security; and (3) provide recommendations on what, if any, additional mitigation measures the Government should take to help protect the network's core.

The CATF defined the elements of the core network, conducted a literature review of more than 50 Government publications, and studied the best practices related to core network security. The CATF also conducted interviews with a representative sample of the communications industry to gather additional data. Specifically, the CATF interviewed chief security officers from each of the working group facility sectors and the Government to help the CATF validate its findings, gather additional insights and concerns of the private sector, and identify additional ways for the Government to contribute to core network protection. Members also toured the Verizon Communications, Inc., facilities in New York City and discussed the impact of technological progression on physical security and related mitigation and protection measures with representatives from the New York and New Jersey State Offices of Homeland Security; the New York/New Jersey Port Authority; and the DHS Protective Security Advisor. The NSTAC completed the *NSTAC Report to the President on Physical Assurance of the Core* in November 2008, and the *Addendum to the NSTAC Report to the President on Physical Assurance of the Core* in February 2009. Both reports are designated For Official Use Only.

Cybersecurity Collaboration

In FY 2009, the NSTAC created the Cybersecurity Collaboration Task Force (CCTF) to examine the formation of a joint, public-private sector, 24x7 cybersecurity collaboration capability designed to detect, prevent, mitigate, and respond to cyber threats.

To support its examination, the CCTF solicited briefings and input from SMEs, including representatives from DHS, the DOD, Symantec Corporation, Verizon Communications, the National Cyber-Forensics Training Alliance, and the SANS Internet Storm Center. CCTF members also discussed the proposed cyber incident detection, prevention, mitigation, and response capability's desired end-state and challenges and opportunities associated with achieving this desired end-state. Using the information gathered during SME briefings and member discussion, the CCTF provided findings and recommendations to foster industry-Government cybersecurity collaboration by creating a Joint Collaboration Center (JCC). The NSTAC completed the *NSTAC Report to the President on Cybersecurity Collaboration* in May 2009. Secretary Napolitano subsequently approved the report and transmitted it to the EOP for consideration.

During its August 2009 Principals' Conference Call, the NSTAC directed the CCTF to continue its study of the operational and information sharing requirements needed to establish the JCC. The task force anticipates completing its examination during FY 2010.

Identity Management Strategy

The NSTAC created the Identity Issues Task Force (IdITF) to examine whether or not the Government could play a substantial role in identity management and if it could serve as a catalyst for broad implementation of identity management efforts.

During its examination, the task force gathered vital information through briefings from identity management SMEs. Members identified key identity management principles and actions needed for the Government to develop a national, comprehensive identity management vision and strategy. The IdITF assessed the current identity management environment, challenges, and incentives and developed recommendations on how best to achieve the desired end-state of a national, comprehensive identity management vision and strategy.

The NSTAC approved the *NSTAC Report to the President on Identity Management Strategy* in May 2009. Secretary Napolitano subsequently approved the report and transmitted it to the EOP for consideration.

Next Generation Networks

The NSTAC formed the Next Generation Networks Implementation Annex Working Group (NGN IAWG) in May 2008 to review the recommendations in the 2006 *NSTAC Report on Next Generation Networks*; review Government activities to date to address those recommendations; and provide guidance on how the recommendations can be further implemented in the short term.

The NGN IAWG developed a catalog of Government activities related to the 2006 Report recommendations and considered next steps for each recommendation. Following the review of Government activities, the NGN IAWG drafted a letter to the President, which highlights suggested next steps for Federal departments and agencies to further address the 2006 Report recommendations. The NSTAC approved the letter in November 2008.

Satellite Security

The NSTAC established the Satellite Task Force (STF) to review and update the 2004 NSTAC *Satellite Task Force Report* in response to an NSSO request to examine cyber and physical satellite security with an emphasis on ground network assets. The NSSO asked the NSTAC to identify existing threat countermeasures and mitigation strategies; identify any new satellite vulnerabilities since the release of the 2004 report; and assist the NSSO in advancing its satellite security partnerships.

To support its examination, the STF solicited member and external SME input and briefings from all segments of the commercial satellite industry to provide a full and complete evaluation of physical and cyber threats. The STF also reviewed the physical security threats to satellite network assets identified in the 2004 report. For each class of threat, the STF described the vulnerability, countermeasures, and mitigation strategies in place to withstand an attack. In addition, the STF distributed a questionnaire to Satellite Industry Association members to collect data on each industry segment's vulnerabilities, threats, and mitigation measures, and to validate its findings.

The NSTAC will complete its examination by November 2009.

National Security and Emergency Preparedness IP-Based Traffic

In 2007, the EOP requested that the NSTAC examine the risk, if any, to IP-based NS/EP communications traffic during times of network congestion. Specifically, the EOP solicited NSTAC's recommendations to determine the best way for IP NS/EP traffic to traverse the network when network congestion occurs. As a result, in January 2008, the Global Infrastructure Resiliency Task Force (GIRTF) began an investigation of traffic management and priority services for IP-based services. The NSTAC approved the *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic* in November 2008.

Legislative and Regulatory Issues

During FY 2009, the NSTAC's LRTF continued to monitor laws and regulations governing NS/EP communications.

The task force assessed the current legislative and regulatory environment in December 2008 to inform the NSTAC's Industry Executive Subcommittee (IES) of significant new or updated policies or regulations relevant to NS/EP communications. Specifically, the assessment examined: (1) nationwide broadband deployment; (2) broadband traffic management; (3) public safety spectrum; (4) 911 and Enhanced 911; (4) public alert and warning; (5) the FCC Public Safety and Homeland Security Bureau; (6) DHS OEC; (7) DHS administrative procedures, policies, and guidelines; (8) CNCI; (9) credentialing and

access to disaster sites; (10) protected critical infrastructure information; and (11) telecommunications and electric power interdependencies.

The task force examined several cybersecurity bills for their impact and relevance to NSTAC activities and NS/EP communications. Although Congress did not pass any of the examined legislation during FY 2009, members will continue to watch the bills throughout FY 2010 to determine whether or not any of the bills' provisions would adversely affect NS/EP communications and warrant further NSTAC examination or action. The LRTF also received briefings on OMNCS 2009 priorities and DHS CIP activities.

Research and Development

The NSTAC established the Research and Development Task Force (RDTF) to: (1) examine issues of concern from past Research and Development (R&D) Exchange (RDX) Workshops; (2) explore potential topics for and facilitate future RDX Workshops; and (3) explore R&D-related issues important to NS/EP communications. During FY 2009, the RDTF completed the September 2008 RDX Workshop Proceedings Document, which summarizes the discussions and events from the 2008 RDX Workshop. The document was distributed to participants and Government stakeholders as an aid for Government officials as they assess their agency's R&D budget priorities related to NS/EP communications.

NSTAC Outreach

The NSTAC Outreach Task Force (NOTF) fosters the exchange of information among key NSTAC stakeholders from both industry and Government on telecommunications-related NS/EP activities, on behalf of the NSTAC 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 2009 by:

- Sending a letter to President George Bush in November 2008 that provided industry feedback on NSTAC priority recommendations and asked the President to consider addressing these key issues during the remainder of his term;
- Providing briefings on NSTAC reports and recommendations, including the *NSTAC Report to the President on Cybersecurity Collaboration* and *NSTAC Report to the President on Identity Management Strategy*, to key EOP, DHS and DOD stakeholders;
- Completing the NSTAC Background Document and distributing it to EOP stakeholders to provide an overview of the NSTAC's history and the critical NS/EP communications issues the body has examined over its 27-year history; and
- Facilitating the NSTAC New Principals' Orientation on May 21, 2009, in conjunction with the 2009 NSTAC meeting.

Sector Specific Agency for Communications

The NCS is the Sector Specific Agency (SSA) for Communications under HSPD-7. Under the National Infrastructure Protection Program structure, there is a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC) that works to reduce risk across the Communications Sector. As the SSA for Communications and the Chair of the GCC, the NCS' responsibilities include:

- Coordinating steady state planning for the protection of critical infrastructure and key resources;
- Developing and implementing the Communications Sector-Specific Plan (CSSP) in partnership with industry;
- Collaborating with Federal, State, and local governments and industry;
- Identifying, prioritizing, and coordinating the protection of critical assets;
- Conducting risk and vulnerability assessments in partnership with industry;
- Chairing the Communications Government Coordinating Council (CGCC); and
- Performing the National Risk Assessment.

During the past year, the Communications Sector made significant progress toward completing actions and milestones for advancing the goals set forth in its CSSP. In February 2009, the Communications Sector collaborated with the energy sector to complete a cross-sector analysis of the Communications Sector's dependence on commercially available power sources. The CDEP WG study addressed the potential for, and the sector's ability to recover from, long-term outages, examining key cross-sector organizations, agreements, policies, and guidelines. The sector also completed communications infrastructure analyses in support of its Federal MEF during the fiscal year. These analyses examined the NCS' MEF dependence on communications in four high-consequence scenarios—high-altitude nuclear burst, ground-based nuclear burst, solar superstorm, and cyber attack. These high-consequence scenarios are critical in evaluating the resiliency of communications.

NCS Communications and External Affairs

The NCS—through coordination with the DHS' 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.

Under DHS management directives, all press releases on the NCS and NSTAC are coordinated through both the DHS CS&C external affairs director and the DHS National Protection and Programs Directorate (NPPD) Communications Director before being released by the Department. The NCS coordinates all inquiries with CS&C in conjunction with NPPD to ensure that the Department approves all requests for interviews and information about the NCS.

The 2009 Inauguration of President Obama allowed the NCS to highlight its NS/EP communications role as a liaison between the NCC and ESF #15—Public Affairs to promote the NCC before, during, and after the Inauguration. The NCS released information on emergency communications programs such as GETS and WPS—encouraging authorized users to test their service prior to inaugural events.

The NCS also filed daily reports on NS/EP communications activities through its DHS channels. FEMA, DHS, and the White House published these reports to promote success stories and inform the public of its NS/EP communications role. Additional news media and trade publications inquiries focused on: the NSTAC; the NCC and its COMM ISAC; the WPS, GETS, and TSP programs; the SHARES-HF Radio Program; and the NCS mission to work with industry in support of emergency communications.

In addition to fielding press inquiries, the NCS also produced a variety of on-line publications, reports, fact sheets, and brochures on NCS programs and the NSTAC. These publications included individual NSTAC reports approved by the committee and submitted to the White House for action. The NCS also published its FY 2008 report and it updated fact sheets and frequently asked questions on NCS programs. These publicly available publications provide NCS information to the media, communications companies, potential NSTAC membership applicants, and senior Government officials about NCS programs and activities.

The NCS Program Manager for Communications continues to serve on a variety of DHS public affairs and external affairs committees. NCS is 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 NPPD and the CS&C Branch dealing with external affairs activities.

Dr. Peter Fonash (left), serving as the Department of Homeland Security's Acting Deputy Assistant Secretary for Cybersecurity and Communications, presents a plaque to National Communications System Chief of Staff Allen F. Woodhouse commemorating the 25th anniversary of the National Coordinating Center for Communications. The ceremony was held on April 6. (Photo by Steve Barrett, NCS)

Outreach

The OMNCS continues to spearhead an outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences. NCS representatives participate in Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and CIP.

NCS outreach efforts are enhanced considerably by the six 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. These nine 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 of the NRF, and participate in local, regional, and national-level exercises designed to test emergency communications readiness.

The OMNCS also deploys its priority service communications booths and staff to conferences and conventions targeting emergency response communications and CIP audiences. Each year, the booth teams appear at nearly two dozen venues around the country, providing information on GETS, WPS, and TSP registration to potentially eligible customers attending these conferences.

Websites

The NCS website (*http://www.ncs.gov*) provides information on the NCS and NSTAC (*http://www.ncs.gov/nstac/nstac.html*), including history, programs, and activities. Online versions of NCS and NSTAC publications are also available on the website. In April 2009, a thorough review of the NCS website identified recommendations for branch chiefs about updating and expanding content for their respective programs. In addition, the OMNCS instituted a quarterly review process where randomly selected areas of the NCS website will be reviewed to ensure that the information remains current.

The NCS continues to work with DHS to maintain an NCS presence on the Department's public site (*http://www.dhs.gov*), and has its own intranet section on the Department's DHS Online internal communications site. In September 2009, the NCS began transitioning information on the current DHS Online page in the Department's efforts to upgrade its original intranet system. The Department plans to migrate to its new intranet platform in February 2010.

Footnotes

1 E.O. 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (and subsequently amended by E.O. 13286, Amendment of Executive Orders, and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, and E.O. 13407, Public Alert and Warning System).

2 E.O. 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (and subsequently amended by E.O. 13286, Amendment of Executive Orders, and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, and E.O. 13407, Public Alert and Warning System).

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

4 Action by the Commission, April 9, 2008, by Commercial Mobile Alert Service First R&O [FCC 08-99].

4 NS/EP Telecommunications Support and Activities of Member Organizations

Department of State (DOS)

NS/EP Telecommunications Mission

Secure Voice Program

The Department of State continued its Operations and Maintenance phase of its Secure Terminal Equipment (STE) program in fiscal year (FY) 2009 and has begun the transition to the Next Generation secure Voice over Internet Protocol (VoIP) phone instrument, Viper. The Viper units are manufactured by General Dynamics and will replace the current 4,891 STE units deployed by State worldwide. The Secure Voice program completed a data call survey to all posts worldwide seeking their input on the current Secure Voice environment for their posts. The current failure rate of STE secure telephones worldwide is 72 percent. The Department's goal is to deploy a device that will allow them more capability in completing secure calls.

The program has acquired 270 Viper instruments for pilot deployments after successful laboratory testing was completed. The units have been deployed in support of special mission requirements in the Near East Asia (NEA) region and the Africa region. The successful Viper pilot was completed in September 2008 at embassies in Central America and the Caribbean. At this time the Department is performing a pilot test with the Public Switched Telephone Network (PSTN) version of the Viper phone. So far the testing has shown that the PSTN Viper will complete secure calls at a much higher success rate than the existing STE phones. The next step in deployment is bringing the Viper phone to 28 of the most critical need posts beginning in June 2009 with completion in August 2009.

To date, the program has acquired 2,320 Viper instruments. This satisfied the need for the pilot posts and the next stage of deployment. The Department will begin full implementation of the Viper at overseas posts this September with scheduled completion set for the end of 2010.

The program continues to sponsor the Secure Voice Products Community of Interest Group (SVP-COI) to address the technical and other factors associated with the legacy secure voice instruments. The SVP-COI will provide the Department a secure VoIP solution that addresses all operational requirements to protect National Security information. Secure Voice in general is a constantly changing environment covering everything from interoperability issues to configuration management and key issues, and affecting all regions of the world. The most immediate issue is VoIP integration into the secure voice environment. Commercial telephone companies are accelerating the re-direction of voice services on the public network to VoIP infrastructure.

The Department also continues to evaluate newly introduced Secure Voice technology such as the portable Secure Mobile Environment-Personal Electronic Device (SME-PED) just recently certified by the National Security Agency (NSA). The SME-PED units (in addition to cellular based secure phone

service) provide Personal Digital Assistant functions (such as e-mail and calendar). The Department is working closely with other Federal agencies on how best to address a SME-PED solution for the Department of State.

Anti-Virus Program

The Department's AntiVirus Program has detected and eradicated more than 545,000 viruses and broke the FY 2008 Spam all time high record of 277,192,748; to date (FY 2009) 471,137,249 Spam messages have been blocked. 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 33,348 home use anti-virus software CDs have been distributed. This proactive measure controls virus incidents from e-mails or documents prepared by employees at home. Currently, there are approximately 80,632 systems actively using SEP v.11 on OpenNet. ScanMail for Microsoft Exchange (SMEX) has been upgraded to version 8 from 3.x/6.2 due to end of life. Approximately 660 servers are running SMEX 8 across OpenNet and ClassNet. The AntiVirus Staff is also integrating new state-of-the-art perimeter security appliances and software (Fortinet) to replace the current legacy scanning technology (Trendmicro). This implementation spreads from HST to Beltsville Information Management Center (BIMC). The new integrated system provides a scalable solution to meet the continuing increase in demand for Department services. The AntiVirus Staff continues to research and analyze new applications and hardware to stay on the technology edge. This consolidated security approach in conjunction with the Secure AntiVirus Equipment Refresh (SAVER) will keep the Department's scanning technology up to date, while ensuring critical services are always available to the public as well as Department staff.

Communication Security (COMSEC) Modernization

The Department is continuing to modernize its national security encryption systems by using the NSA-certified Inline Network Encryption (INE) devices (KG-75s and KG-175s). These new devices replace aging serial based encryption systems with Internet Protocol (IP) based systems that will provide new higher capacity, robust network designs which leverage traditional Government-owned communications, 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 3.2 which is allowing the migration to the next generation INE (the KG-175D, also known as the TACLANE Micro). This encryption device supports Internet Protocol version 6 and also increases the performance and reliability of the Department's classified networks. This third generation INE device will also ensure compatibility with other government agencies and enhance the Department's ability to share critical information in near real time.

The Department has also implemented the NSA-mandated Electronic Key Management System (EKMS). The Department's primary communications hub, the BIMC, 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, NEA, East Asia and Pacific, and Western Hemisphere regions, and is being successfully utilized to encrypt their command and control data. The EKMS program has also successfully piloted the distribution of black electronic keymat over the existing Department of State network infrastructure. The black electronic keymat program is now moving into the full operational phase with deployments to critical overseas locations. This program allows for rapid secure electronic keymat to often dangerous locations in near-real-time, ensuring critical communications are maintained while not putting a diplomatic courier in potential harm's way.

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). PKI functionality has been installed on over 17,000 domestic and 19,000 overseas workstations. Projected completion for initial deployment is planned for the end of FY 2010. Working as partners, the Bureaus of Information Resource Management (IRM) and Diplomatic Security (DS) have issued more than 35,000 smartcard identifications (ID) to employees for building access and logon to the Department's Sensitive But Unclassified (SBU) system. The Department also uses PKI to secure access to its websites, certify mobile code and software patches, and authenticate

users to a growing number of applications. In addition, the PKI program actively supports the ePassport initiative spearheaded by the Bureau of Consular Affairs. This initiative, enabled through the Machine Readable Travel Document 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. As of May 2009, this system has digitally signed over 38 million U.S. passports.

The FPKIPA has cross-certified the Department's X.500 directory-based and Active Directory-based PKIs allowing each to connect to the Federal Bridge Certificate Authority (FBCA) at the high assurance level. Connection to the Bridge gives the Department's PKI user base of more than 33,000 the ability to securely exchange digitally signed and/or encrypted SBU information with more than ten Federal agencies, the State of Illinois, and several non-government entities and certificate providers. 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.

The Department continues its implementation of the Biometrics for 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 a 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 over 70 overseas locations. It is available for use at a total of 140 diplomatic facilities around the world. The BLADE overseas deployments in FY 2008 have been restricted due to current funding limitations but are expected to continue in FY 2009. The Personal Identity Verification (PIV) PKI authenticates and verifies all Department of State employees by digitally signing all new employee identification badges and issuing the mandatory PIV authentication certificate required under Homeland Security Presidential Directive 12, *Policies for a Common Identification Standard for Federal Employees and Contractors*. To date, over 58,000 PIV certificates have been issued.

Secure Video and Data Collaboration

The Department has established a Video Program Office (VPO) to coordinate all unclassified and classified video conferencing services. The Secure Video and Data Collaboration (SVDC) program has been incorporated into the larger VPO charter and continues to provide secret-high videoconferencing services to the Department of State and to interagency gateway services. The success of this growing program continues to prove itself through the increasing customer base, usage levels, and measurable cost savings. In FY 2008 the VPO supported an average of 200 multi-party classified and unclassified conferences a week. This is a considerable reduction of risk to personnel, incurred by limiting the need to travel, and is a particularly strong achievement of this program. The VPO is staffed 24x7, providing program management and customer support for conference scheduling, configuration, interagency coordination and technical assistance. The VPO 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, the VPO established technologies in its program that facilitate point-to-point conferencing abilities, allowing customers in multiple agencies to direct-dial and expedite videoconference establishment. The success of this program continues to grow, and 210 foreign SVDC installations are currently online. The VPO continues to expand and to improve the technologies and capabilities of this program. One effort that is ongoing is the testing of telework video conferencing capabilities. The VPO is determining the Department's requirements while evaluating several possible technical solutions.

Technical Security and Safeguards (TSS)

Responding to the new security vulnerabilities from the reality of the global information technology (IT) production, the Department employs dynamic Defensive Technical Counter-Intelligence methods to provide technical security and safeguards (TSS) for the Department's diplomatic posts and tenant agencies. These methods provide cost-effective, life-cycle risk management for technical integrity of IT equipment used inside the posts' Controlled Access Area and ensure the Department's IT security in a multi-faceted multi-cultural business environment. Coordination between the Department's Bureaus of IRM, DS, and Administration (A) 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 Global Information Technology Modernization (GITM) Program.

Domestic Radio Program

The Department's domestic radio program supports 24 Diplomatic Security Service (DSS) domestic field offices and the Washington, D.C., metropolitan area Washington Area Radio Network (WARN) system. The DSS 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 WARN system supports the Secretary of State and foreign dignitaries. The Department has recently completed an upgrade of all domestic Land Mobile Radio (LMR) systems to comply with the new National Telecommunications and Information Administration narrow-banding requirements. The radio program office is currently implementing a project plan for the migration of all domestic LMR 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, the Department owns and operates LMR and High Frequency radio systems for emergency and evacuation purposes at 260 overseas United States diplomatic posts. These systems are designed to support citizen services, security, and emergency activities of the individual diplomatic missions. The Department's radio program office is also implementing plans for the migration of all overseas LMR systems from DES to AES. In addition, the Department's radio program office is implementing a life-cycle management plan for the LMR systems utilizing a new contract with Kenwood.

Contingency Systems

In support of the Secretary of State's initiative on Transformational Diplomacy and to provide for communications in the event of catastrophic failures of the global telecommunications infrastructure, the Department has developed and is deploying two satellite based communications systems. The Remote Expeditionary Area Communications Hub is a small, portable, easily-to-use system geared towards the reporting officer operating in areas outside the local communications infrastructure, and currently offers remote Internet and voice access. The Mobile Information Programs Center, currently in development, offers all of the communications capabilities currently found in a Department communications center, including classified and unclassified Department voice and data services tailorable to the situation. These systems will operate anywhere in the world and have also been designed to be portable and easy to use.

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, consolidating all modernization efforts for classified and unclassified local area networks (LAN) worldwide (overseas and domestic) under a centralized program for execution. This program protects the Department's substantial investment in IT infrastructure by modernizing the LAN segment of the Department's networks on a four-year life cycle. GITM completed the initial four-year life-cycle refresh in FY 2007 and the next refresh cycle began in FY 2008. GITM modernizes existing LANs using emerging technologies to keep pace with new business requirements, not just replacement of existing equipment. In this way, equipment obsolescence is eliminated and the latest lines of business-driven requirements can be met. By providing reliable, secure, robust and scaleable LAN infrastructures, foreign affairs workers will have the necessary tools to enable communications, collaboration, knowledge management and the sharing of data and information in both classified and unclassified environments.

State Messaging and Archive Retrieval Toolset (SMART)

The State Messaging and Archive Retrieval Toolset (SMART) Program is delivering a new set of communication-tools to the Department of State. SMART replaces and enhances the current custom-developed cable systems that are difficult and expensive to support, and have a fairly high risk of failure. The current cable messaging and e-mail systems are being consolidated, from an end-user standpoint, into a single, easy to use system. Other tools being deployed under the SMART umbrella provide instant messaging, agency collaboration, and search tools for the archive and record management system.

This critical multi-year software integration and development project replaces old non-integrated systems by consolidating, centralizing, and modernizing messaging processes and systems in the Department. It will benefit the Department by enabling employees to search, manage, archive, and retrieve the information and knowledge contained in the millions of diplomatic messages that are sent each year. It also implements the Department's overarching e-Diplomacy knowledge management and inter-agency information sharing and collaboration strategies. Overall, SMART greatly improves information security, integrity, and privacy through the collection and storage of robust metadata about SMART messages that includes: message type; dissemination/address; retrieval/restrictive captions; precedence-command/control; classification-sensitivity; disposition; and integrity-clearance/approval.

IRM is the system integrator for developing and managing the system in useful segments through an incremental, multi-vendor approach. The SMART Program Management Office reports directly to the Chief Information Officer (CIO), to ensure that expertise within the Bureau transitions seamlessly from SMART product development and deployment to operations and maintenance. The Department employs a SMART Steering Committee to represent the business users of the Department, review progress on a regular basis, and make recommendations to the Undersecretary for Management at the major control gates and decision points. The Steering Committee is briefed monthly, the CIO is briefed weekly, and the Office of Management and Budget is updated approximately quarterly, and prior to all milestone decisions and funding related actions.

The SMART program is making excellent progress. Segmented software analysis, design, development and testing are on schedule, and the Segment 1 pilot system was successfully deployed at three pilot posts in the 1st quarter of FY 2008. SMART segments 2 and 3 were deployed to additional posts in the 1st and 2nd quarters of FY 2009; and SMART will move into production and full world-wide deployment in the 4th quarter of FY 2009.

Department of the Treasury (TREAS)

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 Chief Information Officer 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.

Treasury Government Security Operations Center

Building on the successful cybersecurity efforts in 2008, Treasury continues to place a great deal of focus and energy on defending its IT infrastructure against network threats. During fiscal year (FY) 2009, Treasury made significant changes organizationally and technically to more effectively defend the Treasury's network infrastructure and the Sensitive But Unclassified (SBU) data that traverses it. These efforts can be summarized as:

- Formally established and contracted for the Treasury Government Security Operations Center (GSOC), the Departmental cybersecurity operations analysis, response and reporting organization;
- Refined Trusted Internet Connection (TIC) security requirements, and established a concept of operations guide that will ensure all Treasury approved TICs provide

the required security data feeds of their Internet point of presence so a holistic operational situational awareness and response strategy may be achieved;

- Deployed numerous technical upgrades and capabilities within the GSOC to monitor for pervasive advanced persistent threats.

Treasury formally established the Treasury GSOC as the Department-wide cybersecurity monitoring, analysis, forensics response, and operational/Federal Information Security Management Act (FISMA) reporting organization, to ensure the Department is effective, coordinated, and timely in all cybersecurity incident response actions. Evolved from the TCS-Computer Security Incident Response Center, this 24x7x365 operation of 21 staff provides Treasury with the key cybersecurity subject matter expertise to properly defend its networks.

Under this new organizational structure, and with this evolved operational capability, Treasury has embraced compliance with the Office of Management and Budget (OMB) TIC initiative. Treasury plans to implement a heterogeneous architecture of "hard" Treasury owned TICs, as well as implementing approved TICs through "soft" managed TIC services where required. Treasury will implement its TIC compliance as it transitions from the Treasury Communications System to its new GSA Networx-based "TNet" architecture in late 2009. Treasury has published its security policy defining the minimum set of security controls and capabilities that all TICs must have, which is based on the minimum guidance set forth by OMB.

These operational analysis requirements have resulted in a multi-pronged effort to ensure the Treasury GSOC has appropriate resources to affect its mission. Treasury GSOC established a classified operations enclave with the Security Operations Center and an all-source Cyber Intelligence capability so that classified cyber incident information, threat data, and collaboration could be exchanged between lateral Federal, Department of Defense (DOD), and Department of Homeland Security (DHS) entities.

Treasury GSOC invested in a new modular and scalable Security Information Event Management architecture to include a more than 130 terabyte storage area network that will facilitate the collection and analysis of all TIC security log data. Treasury GSOC also launched numerous in-house developed tools such as EMIT (Email Inspection Tool). EMIT allows the GSOC analysts to inspect the entire Treasury Departments inbound mail stream for specialized targeted spear phishing attacks. As a result of the analytical products generated by these tools, GSOC analysts now regularly publishes Treasury Early Warning and Indicators (TEWI) reports via the United States Computer Emergency Readiness Team (US-CERT) GFIRST portal, 38 Federal and DOD agencies readily access and download these reports so they may use the information to better defend their own networks.

Voice/Video Program (formerly Digital Telecommunications Switching System – DTS)

During FY 2009, the Voice/Video 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 and sites in suburban Maryland and Northern Virginia, with physical interfaces to other telecommunications programs and services. The network provides voice, data, and video services via analog, Integrated Services Digital Network (ISDN) Basic Rate Interface, and ISDN Primary Rate Interface and Voice over Internet Protocol (VoIP) services to the DTS user community. Verizon is the incumbent contractor. The Voice/Video network is comprised of telecommunications infrastructure and SONET Ring topology connecting bureau sites to a Lucent Host 5ESS Central Office switch with software release 5E16.2. Optical Remote Modules, Remote Integrated Service Line Units, and NT-1 equipment are connected to the Host switch through a bi-directional self healing SONET ring, and standard copper wiring. Lucent and Tone Commander ISDN telephone sets and other peripheral equipment are owned and maintained under the current contract. In addition, an Avaya VoIP switch provides Internet Protocol service to six customer locations supporting ISDN and VoIP sets. The Voice/Video program also provides the following "bundled" services:

- Audio conferencing;
- Video conferencing;
- Automated Call Distribution;
- Interactive Voice Response Unit;
- Electronic Directory Services;
- Enhanced 9-1-1 (E911);

- Emergency Notification System;
- Network Security Monitoring System;
- Operations Manager – Network Surveillance System;
- Online provisioning capabilities;
- Online management reporting;
- Online billing;
- Service Level Agreements;
- Certification and Accreditation;
- Engineering and planning support;
- Dedicated 24x7 Treasury help desk;
- Unlimited software changes; and
- Technology refreshment.

Voice IT Security

The information transmitted and generated by Treasury's Voice/Video Program systems is considered SBU. Treasury developed the Voice/Video Security Program to meet all essential security requirements and technical guidance set forth in the following:

- Public Laws;
- OMB guidance;
- Government Accountability Office;
- National Institute of Standards and Technology (NIST) Special Publications
- Department of the Treasury Directives; and
- Voice-specific policies and procedures set forth in the Voice/Video DTS System Security Authorization Agreement and its appendices.

The Voice/Video System Security Plan (SSP) continuously defines the necessary actions for which Treasury is responsible and provides an overarching security framework and objectives. The Voice/Video System Security Authorization Agreement and its appendices describe security measures that are currently in place, or that the Program Management Office and Verizon plan to implement to ensure the confidentiality, integrity, and availability of voice and video services and to fulfill contract requirements (Government requirements such as FISMA, OMB A-130, and guidance from the 800 series of NIST Special Publications). Verizon's documentation complements the Voice/Video SSP by describing how Verizon implements Treasury's 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) 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 are capable of High Frequency (HF) Radio, secure voice, secure facsimile, and SIPRNet communications as well as unclassified voice, facsimile, and local area network operations. Secure video is also available.

The issuance of Government Emergency Telecommunications Services (GETS) cards continued to increase in FY 2008. 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 Office COOP team members as well as Treasury Bureaus. The acquisition of a new, expanded Treasury 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 2009 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 completing installation and implementation testing of a Treasury high frequency radio network in support of NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, requirements for emergency back-up communications;
  - HF radios have been procured and installed at Treasury Headquarters, EMC and the Treasury Headquarters COOP site. HF radios are being installed at all Bureau COOP sites and selected Bureau headquarters locations; and
  - 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 Top Secret level.
- Additional GETS Cards are pre-positioned at all Treasury alternate operating facilities and EMCs so that cards can be transferred to Treasury staff to respond to immediate crises;
- Secure cell phones for senior staff (Secretary Successors) of the Treasury;
- WPS phones for senior staff of Treasury Bureaus;
- WPS phones for entire COOP team by end of FY 2008;
- Secure and non-secure video teleconferencing capability for the primary and alternate Treasury Headquarters COOP site;
- Full installation and monthly testing of unclassified voice, facsimile, e-mail, and secure voice, secure facsimile and secure e-mail for its primary COOP site and EMC;
- Acquisition of fixed-station satellite communications for the primary Treasury COOP site;
- Full installation, testing, and use of the Event Tracking System (E-Team) in Treasury's EMC and Bureau locations.

Support for the Federal Public Key Infrastructure Development

The Department of Treasury continues to provide first-class technical, operational, and leadership support in the development and use of an interoperable government-wide Public Key Infrastructure (PKI) to permit secure electronic transactions across Treasury, National Aeronautics Space Administration (NASA), Social Security Administration (SSA), DHS, 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 all Bureaus. Treasury's PKI infrastructure is a critical component in the General Service Administration's (GSA) Personal Identity Verification (PIV) Managed Service Offering (MSO), as required by Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. Significant progress was made in FY 2009 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.

Treasury continues to work with other agencies through the Federal PKI Shared Service Provider (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 has developed a successful partnership with NASA, SSA, and DHS through the SSP program. Treasury is actively seeking future business engagements with other agencies, and will continue its efforts to do so over the next fiscal year.

Treasury is continuing its business relationship with the Federal Bridge Certification Authority that supports conducting "trusted" business with member agencies through a common PKI architecture and policy. 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 is expanding its current resources to meet forecasted demand and logical/physical access requirements, such as those brought about by the Department's involvement in the Federal identity and access management program, E-Authentication Federation, and PIV, as described above. Treasury's critical Certification Authority hosts have undergone significant recalibration over the past year; this effort will continue over the coming months to meet PIV integration objectives. Also, the triennial Independent Audit of the Treasury PKI infrastructure, hosted by the Bureau of Public Debt, was completed earlier this fiscal year to meet Federal PKI Policy Authority requirements.

Also, Treasury is continuing 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.

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 communications 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 2009, 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 (including 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 (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's 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 2009 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 Assurance Program continued to make great strides in keeping its systems, as well as Bureau systems, compliant with certification and accreditation policies and procedures.

Treasury's GSOC provided cybersecurity monitoring for the Department's wide area 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.

Treasury's Voice/Video Program continued to provide secure access to Treasury's complex voice telecommunications infrastructure in the Washington, D.C., metropolitan area.

The Treasury Office of Emergency Preparedness saw an increase in GETS cards in FY 2009 as it supported COOP requirements and made plans for a more capable local EMC.

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 WPO assisted Treasury Bureaus in upgrading their LMR equipment and assisted in the procurement of equipment to secure the transmission of sensitive law enforcement-related information (including 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.

Department of Defense (DOD) and Joint Staff (JS)

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) executes the following national security and emergency preparedness (NS/EP) telecommunications responsibilities:

- Provide, operate, and maintain the telecommunications services and facilities to support the President and the Secretary of Defense and to execute the responsibilities by E.O. 12333, *U.S. Intelligence Activities*, December 4, 1981.
- Ensure that the Director, National Security Agency (NSA), provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications.
- Execute the functions listed in Sections 3(d) and 3(i) 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 (DISA) 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

National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive (HSPD) 20, *National Continuity Policy*

DOD, in coordination with the Department of Homeland Security (DHS), is tasked to provide secure, integrated Continuity of Government (COG) communications capabilities. The policy 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. In August 2008, the Principal Deputy Assistant Secretary of Defense (PDASD), HD&ASA and the Office of the Assistant Secretary of Defense (OASD) NII/DOD CIO jointly informed the Assistant to the President for Homeland Security and Counterterrorism/National Continuity Coordinator that DOD will provide an initial operating capability consisting of an integrated secure voice, video, and data capability that leverages the best attributes of current operational Category I communications systems. This capability will emphasize the Defense Red Switch Network (DRSN), the Crisis Management System (CMS), the Distributed Continuity Integrated Network-Top Secret (DCIN-TS) and the Joint Worldwide Intelligence Communications System (JWICS). DOD, DHS, and the Office of Science and Technology Policy have conducted initial coordination throughout the interagency community for the draft *Federal Executive Branch Continuity of Government Communications Implementation Strategy*. The goal of this strategy is to establish the vision, objectives, and execution plan for the future state of COG Communications; outline the mission, vision, key objectives; outline critical assumptions and challenges; provide reference documentation; and delineate interagency roles and responsibilities.

Defense Red Switch Network

The DSRN is DOD's global senior level secure voice telephone and secure voice conferencing system. It provides rapid, high quality secure and non-secure voice communications services to special command and control (C2) users. The DRSN provides its customers access to the strategic and tactical

communities (ground networks, airborne, and seaborne platforms), DOD, Federal, U.S. public switched networks, and some Allied equipment and networks from a single, multifunction, user-programmable instrument. The user terminal can be configured as a single line or multi-line device capable of processing secure or non-secure voice. There are over 64 switches in the network supporting all the Combatant Commanders (COCOMs), many subordinate commands, the National Military Command Center, Secretary of Defense (SECDEF), White House Communications Agency, Department of State, Federal Bureau of Investigation, and DHS. The network is also critical to supporting complex multi-participant emergency voice conferences and serves as a gateway/interface to other secure voice systems. This voice conferencing represents a key capability that provides rapid setup, extensive monitoring and management capabilities using Command Center consoles, and the ability to connect large numbers of conferences. It also allows the conference to be extended across gateways to tactical, wireless, Internet Protocol (IP)-based or other secure voice systems and at multiple security levels.

The DRSN is in the process of a tech refresh effort in conjunction with the services and agencies that own the switches, to replace end of life models with the new DSS-2A model, to ensure continued viability and sustainability of the network. DISA is also operating, as an adjunct to the DRSN, a Voice over Secure IP (VoSIP) secure voice service using the Secret Internet Protocol Router Network (SIPRNet) as transport. VoSIP provides a SECRET only secure voice capability to those user communities that do not have requirements for the MLS, Conferencing and gateway capabilities that are unique to the DRSN.

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 DISA on behalf of the National Security Council (NSC), extends the President and the White House Situation Room point of presence to approximately 150 fixed and deployed locations worldwide. CMS 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 IP backbone. The core CMS applications are the Secure Video Teleconferencing System, the Crisis Management Network (CMN), the Executive IP Phone System which incorporates the National Operational Intelligence Watch Officers Network, 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.

In addition to the 150 sites, there are now more than 170 portable devices in the field including 50 "one case" next generation models. Fifty plus desktop units bring the video conferences directly to the participants' fingertips. Extending that reach are more than a half dozen interfaces to other voice and video networks. Overseas site expansion in particular progresses at a rapid pace. Recently CMS completed a total replacement of the CMN or high speed facsimile network at over 40 sites. The Executive IP Phone System now numbers over 300 instruments spread over the extensive IP network. Finally, CMS has expanded its presence on a variety of executive level aircraft and is planning an enhanced ground infrastructure to accommodate service demand.

In the contingency world CMS provides a number of entry points for remote users particularly those who will "dial-in" through a variety of media. Four newly deployed digital gateways along with several planned facilities accommodate the growing number of contingency sites requiring dial-in capability. These gateways, along with the 11 analog gateways, can support large numbers of fixed and remote participants in a single call. Additional users can be placed in a virtual waiting room and invited to join conferences as required. Looking to the future, CMS is poised to dramatically expand the Executive IP Phone System and add interfaces to other voice networks. CMS will also offer expanded collaboration in a presentation mode as well as a high definition capability.

Distributed Continuity Integrated Network-Top Secret (DCIN-TS)

DCIN-TS (GOLD) enterprise is a DOD secure data, voice and video, internet-protocol-based crisis management and business continuity system currently used by Senior Leaders and staff throughout the DOD and the interagency community for day-to-day information exchange, real-time collaboration, and decision-making.

Joint Worldwide Intelligence Communications System (JWICS)

JWICS is a 24-hours-a-day network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide. It provides Department of Defense Intelligence Information System (DODIIS) users a SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics.

Critical Infrastructure Protection

DOD Directive 3020.40 assigns responsibilities to DOD components for the identification, prioritization and where appropriate, protection of DOD and non-DOD networked assets essential to protect, 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 HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*.

A key accomplishment this past year, in terms of breadth of participation and time committed by government and private sector DIB partners, has been the review and revision of the Goals, Objectives, Implementing Actions, and Metrics in the DIB Sector Specific Plan (SSP), meant to guide the Critical Infrastructure Key Resources (CI/KR) protection efforts throughout the sector. These revisions were codified in the *2009 Sector Annual Report* and will be incorporated in the on-going rewrite of the CI/KR objectives and procedures.

DIB private sector partners, through the DIB Sector Coordinating Council, have formed a Defense Security Information Exchanges patterned after the extant National Security Information Exchange (NSIE). In 1991, the NSIEs were formed at the joint request of the National Communications System (NCS) and the President's National Security Telecommunications Advisory Committee.

Mission Assurance and National Security Systems (NSS)

National security depends on a global information infrastructure that is reliable and resilient. The DOD and NCS are working in partnership through the Committee on National Security Systems (CNSS) with Federal Departments and Agencies and with the private sector our Allies to ensure resilience of our networks for the NS/EP community. DOD established a task force to reduce the risk of degraded or failed missions by analyzing dependencies and cascading effects of information and communication technologies supporting Primary Mission Essential Functions (PMEF). It identified key capability and resource gaps for network resiliency. Findings from the DOD task force's efforts were incorporated into Cyber Storm II, a DHS-sponsored, national-level cyber exercise held in March 2008, and Global Lightning '09, a DOD-sponsored exercise held in November 2008 to promote realistic modeling, exercises, and simulations. These exercises enhanced network resilience, continuity of operations planning, and protection of critical information infrastructures for NSS.

The Committee on National Security Systems works closely with the Intelligence Community (IC), DOD, and the National Institute of Standards and Technology (NIST) to enhance the security of NSS by moving toward a common set of policies and instructions for the entire Federal Government. The goal is to blend applicable documents and best practices of these three communities into a single process for the approval and authorization to operate an NSS, as well as to establish a more holistic and strategic common risk management framework for assessing risk and building trust by using common standards. The result will be one set of documents for the entire Federal Government to use with respect to risk management and CNA.

In support of this effort, the CNSS issued CNSS Policy (CNSSP) No. 22, *Risk Management Policy for National Security Systems*, which establishes the requirements for enterprise risk management within the National Security Community. The CNSS is currently working on several documents with NIST to assist in the development and implementation of the Risk Management Program outlined in CNSSP No. 22. Instructions include information on categorizing information and information systems, a security controls catalog, a guide to assessing security controls, and assessing risk.

The CNSS prepared an Annual Report to the President that captures the progress made against the 2008 priorities and recommendations in the 2007/2008 CNSS Report, *An Agenda for Safeguarding National Security Systems*, in the five focus areas: 1) assured information sharing; 2) managing risk; 3) identity assurance; 4) network resilience for mission assurance; and 5) building and sustaining a superior information assurance workforce. These efforts are consistent with NSPD 54/HSPD 23, and the Comprehensive National Cybersecurity Initiative.

In addition, the CNSS issued CNSSP No.25, *National Information Assurance Policy for Public Key Infrastructure (PKI) in National Security Systems*, for the implementation of a PKI for the SECRET environment. This policy facilitates identity authentication, technical non-repudiation, data integrity, and communications privacy on these networks among trusted participating entities. The CNSS is also developing the first ever common Information Assurance (IA) lexicon for the DOD, IC, and Civil communities (update to CNSSI 4009). Having a nationally recognized common lexicon will improve communications between the communities and ensure that policies, instructions, and other guidance are using consistent terms, as well as enhance reciprocity.

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 Global Information Grid (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 Leadership Command Capability (NLCC) Executive Management Board (EMB)

The NLCC EMB serves as the principal oversight committee for the Defense and National Leadership Command Capabilities (DNLCC). It serves as the principal forum in coordination with other Department and interagency forums for decision-making, information sharing, coordination, and resolution of issues regarding interagency communication and senior leadership capabilities and programs. The NLCC EMB also provides a forum for discussion of issues associated with non-DOD assets supporting defense and national senior leaders. The EMB has the authority and responsibility to provide policy, validate and approve requirements, management and oversight of the planning, funding, implementation, operation and maintenance of DOD elements, equipment, and other assets supporting senior leaders.

Senior Leader C3 Systems – Airborne (SLC3S-A)

This Air Force sponsored system provides the capability for the President of the United States and Vice President of the United States, Secretary of State, Director National Intelligence, Secretary of Homeland Security, SECDEF, Chairman of the Joint Chiefs of Staff, and the COCOMs to perform national security and emergency response roles while airborne, world-wide. Senior Leadership and their designated staffs are provided access to live television, secure and non-secure voice, data, and video teleconferencing (VTC) capabilities to maintain situational awareness, collaborate, and reach-back to home station information sources. The system includes infrastructure/networks on aircraft, air-to-ground satellite communications (SATCOM) and line-of-sight systems, and teleports with dedicated high speed terrestrial connectivity to Air-to-GIG gateways (A2G2s) that extend services from home stations and other locations to the aircraft. Robust IA protections are implemented at a number of points in the system including the A2G2s. The SLC3S-A Global Network Operations Center (GNOC) provides oversight to the system and acts as the central focal point for troubleshooting and resolving any issue to maintain maximum availability of services to Senior Leadership. SLC3S-A uses systems such as Boeing Broadband Service Network, INMARSAT, Ultra High Frequency (UHF) Military Satellite Communications (MILSATCOM), Very High Frequency/Frequency Modulation(VHF/FM), High Frequency (HF), NORTHSTAR, and Iridium for air-to-ground connectivity. SLC3S-A supports the VC-25A, E-4B, C-32A, C-40B, C-37A, C-20B/H, E-6B, and tactical platforms when fitted with DV comfort pallet (C-17, KC-10, C-141, C-130). Several immediate improvements were recently implemented:

- Permanently installed the Crisis Management System on the C-32As and C-40Bs to enable Senior Leader secure VTC capability with the White House.
- Began the replacement of the STU-IIIs with the STE-RI.
- Upgraded the VC-25A switching system with an interim digital capability to include testing and fabrication of a digital NORTHSTAR capability.
- Upgraded the GNOC location, its information assurance capability. and circuits to provide diversity and redundancy.

National Military Command System (NMCS) Transformation

The Joint Staff, in conjunction with the Services, COCOMs, and DISA, has developed and approved a new Concept of Operations (CONOPS) for the NMCS. This CONOPS aligns the NMCS with the July 2008 DOD Directive on Defense and National Leadership Command Capabilities that

emphasizes information integration and sharing. This CONOPS is being incorporated into the CJCS Instruction on the NMCS.

National Guard Bureau's Joint CONUS Communications Support Environment (JCCSE)

JCCSE enables reliable and timely flow of key information to support State and Federal military activities required for Homeland Defense (HD)/Civil Support (CS) missions. JCCSE is currently made up of three primary initiatives: 1) The Joint Command, Control, Communications & Computers (C4) Coordination Center (JCCC); 2) the Joint Incident Site Communications Capability (JISCC); and 3) the Joint Information Exchange Environment (JIEE). JCCSE identifies the JCCC as one of the key organizational components that provides planning, coordination, and monitoring of NG Joint C4 capabilities in support of nationwide HD/CS mission requirements. The JCCC provides SA and builds the C4 common operating picture from the incident site thru the National Guard Bureau to the COCOMS and mission partners.

JISCC is the deployable communications capability, as prescribed by the JCCSE, that is specifically tailored to support unique HD/CS mission requirements. JISCC is a C-130 transportable, transit case-based system organized into five modules:

- **SATCOM Reach-back Communications Module.** Ku-band (Ka upgradeable) deployable SATCOM terminal and backup reach-back capability.
- **Incident Site Communications Module.** 20-25 handheld radios and a signal repeater to extend range for intra-team communications.
- **Interoperable Communications Module.** Audio gateway and radios that facilitate radio interoperability with first responders (police, fire, medical), other Government agencies (such as FEMA), and non-Governmental agencies (for example, the Red Cross)
- **On-scene Command Post Integration Module.** Extension of the desktop to the incident scene; voice or IP telephones, computers, video teleconferencing, & multi-function printer.
- **Support Equipment Module.** Generators, power distribution, environmental control unit (ECU), tent, and transport trailer.

The Joint Information Exchange Environment (JIEE) supports National Guard operations and mission coordination by sharing and processing domestic event information and associated Requests for Information (RFI) and Requests for Assistance (RFA) among the 54 States and Territories, and the National Guard Bureau. JIEE also supports National Guard SA and the building of the National Guard Common Operational Picture enabled by standard geospatial information services. JIEE is compliant with the National Information Exchange Model (NIEM) Common Alerting Protocol (CAP) to support information sharing with FEMA and civilian agencies. JIEE is being developed in accordance with JCCSE and Federal strategic objectives to enable a trusted DOD Joint and Interagency strategic operations information (SOIS) sharing environment.

Pandemic Influenza (PI) Preparation

The OSD CIO established a Pandemic Influenza Preparation Working Group (PIPWG) in May 2009 to address OSD Information Technology posture for handling a PI outbreak. The working group is chaired by OSD CIO and OSD Policy. At a high level, the following accomplishments have been completed:

- Assessment of OSD IT capabilities for remote access (unclassified and classified). Currently OSD has 3,500 laptops distributed with remote access client software, approximately 3,000 blackberries, and approximately 800 wireless air cards. There must be further proliferation of Secure Mobile Environment-Personal Electronic Devices and TALON cards throughout DOD for classified computing.
- Review of alternatives for Virtual Government Furnished Equipment (Non-GFE with bootable CD-ROM issued by the government to ensure security protocols are utilized). The OSD CIO office along with NII met with Air Force Research Lab representative from Wright Patterson AFB. They are working with the OSD CIO office on a solution (Lightweight Portable Security [LPS]) bootable CD-ROM solution that will work with the OSD CIO Citrix infrastructure. OSD CIO has received the prototype and plans to test solution. OASD(NII)/DOD CIO also has NSA evaluating the product for use.

- Through the Pentagon Area CIO Council, OSD CIO is also working with ITA (Pentagon Common IT provider) to assess ITA's capabilities and capacity per Service/Agency on remote access capability (unclassified and classified).

Department of Justice (DOJ)

NS/EP Telecommunications Mission

Led by the Attorney General, the broad mission of the Department of Justice (DOJ) is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide Federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior and to ensure fair and impartial administration of justice for all Americans.

DOJ is composed of some 40 separate component organizations including:

- The United States Attorneys (USA), who prosecute offenders and represent the United States Government in court;
- The major investigative agencies: the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATFE)—which deter and investigate crimes, and arrest criminal suspects;
- The United States Marshals Service, which protects the Federal judiciary, apprehends fugitives, and detains persons in Federal custody;
- The Federal Bureau of Prisons, which confines convicted offenders;
- The litigating divisions, which represent the interests of the American people and enforce federal criminal and civil law;
- Other major departmental components including: the Justice Management Division (JMD); the Executive Office for Immigration Review; the United States Trustees; the Office of Justice Programs; the Office of Community Oriented Policing Services; the Office of the Federal Detention Trustee; the National Security Division; the National Drug Intelligence Center; the Community Relations Service; the Office of the Inspector General; the Office on Violence Against Women; and the United States Parole Commission.

Headquartered in Washington, D.C., the Department conducts much of its work in offices located throughout the country and overseas.

The national security and emergency preparedness (NS/EP) telecommunications mission for the DOJ is to assure the availability of telecommunications services in support of these essential law-enforcement functions.

Current/Ongoing NS/EP Telecommunications Activities

The Department centralizes its NS/EP telecommunications services in the Office of the Chief Information Officer (CIO) under the JMD for all DOJ component agencies, except the FBI which operates its own telecommunications services.

The Deputy CIO's E-Government Services Staff operates and manages the Justice Unified Telecommunications Network (JUTNet), DOJ's enterprise wide area network. The Deputy CIO's Operations Services Staff operates and manages the Department's enterprise datacenters where secure interagency messaging is provided via the Defense Message System (SIPRNET), Justice Automated Message System, and Joint Worldwide Intelligence Communications System. The Deputy CIO, IT Security Services, operates and manages the Justice Security Operations Center (JSOC), DOJ's enterprise network monitoring and security incident management capability. The Deputy CIO, Law Enforcement Wireless Communications, manages and operates the Department's enterprise land mobile radio platforms.

The Department is an active participant in the Government Emergency Telecommunications Service program, the Wireless Priority Service program, and the Telecommunications Service Priority (TSP) program.

DOJ continues its strong support of the National Communications System's goals and objectives through active participation in such forums as the Committee of Principals, the Council of Representatives, and the TSP Oversight Committee.

Significant Activities – Enterprise

- The Department continues to rely upon JUTNet, one of the largest MPLS-based networks in operation, to provide secure, reliable wide area network services to over 2000 locations throughout the United States and its territories.
- Satellite and mobile wireless-based connections were added to the portfolio of JUTNet services to enhance disaster recovery capabilities, improve network reach to remote areas and support tactical operations.
- DOJ component agencies continue to develop innovative approaches to establish and sustain mission-critical voice and data services during continuity of operations scenarios including the ATFE developed 'fly-away' kits and the USA deployed a mobile operations center vehicle.
- The Department established the JSOC to provide comprehensive monitoring of the Department's enterprise networks and to enable rapid response to cybersecurity incidents.
- The Department completed implementation planning and pilot testing for its Trusted Internet Connection; full-scale deployment will be completed by end of Calendar Year (CY) 2009.
- The Department re-invigorated efforts to upgrade its legacy land mobile radio platforms and completed plans to begin deploying the Integrated Wireless Network solution in the Mid-Atlantic and Midwest region in CY 2010.
- The Department completed an enterprise voice services strategy which will leverage JUTNet's highly secure and reliable network infrastructure to provide advanced, cost-effective voice services; source selection will be completed by end of CY 2009 with deployment beginning in the National Capital Area in CY 2010.

Department of Interior (DOI)

NS/EP Telecommunications Mission

The Department's mission is to efficiently manage the Nation's natural resources. The Department of the Interior (DOI) and the U.S. Department of Agriculture (USDA) 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 Federal, State, local, 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 Federal Technology Service (FTS) 2001 contract. Selection of a successor service provider under the GSA's Networx contract will be accomplished in early Fall 2009 with transition immediately following. DOI has already begun transition activities for its voice FTS2001 successor service provider.

DOI has completed consolidation of its bureau backbone data communications networks to a single Department-wide Multi Protocol Label Switched-based architecture with enhanced network security functionality. The enhanced security functionality includes threat management, vulnerability management, and assurance. In fiscal year 2009 DOI added enterprise incident management and risk management capabilities according to National Institute of Standards and Technology guidance.

DOI has also consolidated Internet service provider access from 33 points of presence to 5 throughout the Department and has applied for self-service provider status under the Office of Management and Budget (OMB) Trusted Internet Connection Program. DOI additionally has incorporated National Communications System functionality at each of its five consolidated gateways.

The transition of DOI's wideband LMR systems to the National Telecommunications and Information Administration (NTIA) mandated narrowband operation is a continuing high priority for the National Park Service and the Bureau of Indian Affairs. Spectrum Relocation in the 1.710 GHz band has additionally given a high priority. Geological Survey and the Bureau of Reclamation have made tremendous strides and are at or near completion on their three projects. National Park Service is working directly with NTIA and OMB to ensure successful completion of its two multi-state projects.

DOI has established a National Radio and Spectrum Program Management Officer and is implementing Joint Program Operations in the Denver Federal Center with the U.S. Fish and Wildlife Service, the Bureau of Indian Affairs, the U.S. Bureau of Reclamation, and the U.S. Department of Agriculture's Forest Service. DOI awarded in November 2008 its second multi-vendor, multi-year contract to supply Project 25 (P25) standard narrowband radios and supporting infrastructure to support DOI, USDA and Department of Justice, providing lower-cost standardized interoperable P25 radios. This contract additionally has a recurring 6 month technical refresh cycle to provide DOI's radio users the most current radio technology available.

DOI participates 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 high frequency backup radio links are used to augment DOI emergency relocation site communications. Critical circuits on the DOI network and Bureau segments have received Telecommunications Service Priority designation.

DOI Significant Accomplishments

In 2007 DOI signed separate memorandums of understanding with the States of Montana and Wyoming for interoperability partnerships in their statewide P25 compliant LMR systems. In 2008, DOI entered into a similar memorandum of understanding with the States of Nebraska and Wisconsin. Also in 2008, DOI and NTIA successfully certified through the Interdepartmental Radio Advisory Committee's Spectrum Planning Subcommittee the use of DOI's frequencies inside the state wide system for Montana. This marks as a cornerstone for proportional sharing agreements between Federal and State government communications providers. DOI continued this work through 2009 by renegotiating the partnership with the State of South Dakota to provide opportunities for all Federal agencies operating in the State. The Department additionally was able to steer through the NTIA amendments to the NTIA Manual codifying the Federal/Non-Federal sharing of radio systems.

In 2008, DOI and Customs and Border Protection (CBP) entered into an agreement to share common encryption keys for securing communications between DOI and CBP southwest border law enforcement officers. DOI has fully implemented key sharing for all DOI LE personnel along the border, has awarded a contract to develop a comprehensive regionalization study of DOI systems operating across the border, and has piloted Radio over Internet Protocol at selected sites with the National Park Service. These projects all tie together to formulate a comprehensive Radio and Wireless Architecture baseline for integration in the Department's Enterprise Architecture framework.

DOI has established a joint DOI, Department of Homeland Security, and National Institute of Standards and Technology funded Telecommunications Service Center (TSC). The TSC provides a laboratory component level and holistic testing capability for determining manufacturer's radio equipment compliance with P25 standards and ability to work in support of incident command scenarios and systems. The LMR industry is very supportive of this effort, with multiple vendors providing baseline user, infrastructure, dispatch, and encryption equipment for testing. Currently DOI has tested all mobile and portable equipment available for procurement through its $500 million Blanket Purchase Agreement.

United States Department of Agriculture (USDA)

NS/EP Telecommunications Mission

The United States Department of Agriculture (USDA) national security and emergency preparedness (NS/EP) communications program enables assigned personnel to perform primary mission essential functions during a Federally declared disaster or emergency event. The program also supports the National Response Framework Emergency Support Function #2 for communications.

Current/Ongoing NS/EP Telecommunications Activities

The USDA Forest Service, National Interagency Fire Center (NIFC), has prepositioned Land Mobile Radio systems in London, Kentucky, for hurricane support. The cache of approximately 500 Very High Frequency and Ultra High Frequency radios acquired by the Federal Emergency Management Agency (FEMA), are maintained at the state of 'Ready for Use' in NIFC facilities. NIFC also supports the states and other departments and agencies that request radio support.

The USDA has prepositioned Government Emergency Telecommunications Service (GETS) calling cards in those Regional offices located in typical Hurricane paths across the Southern and Eastern United States. USDA typically deploys stockpiles of GETS calling cards prior to landfall when necessary, returning the cards to stock when the emergency has subsided.

In addition to NIFC radio personnel, USDA has trained telecommunications technical support specialists on stand-by for deployment to address critical infrastructure outages. Volunteers are geographically dispersed across the United States to support a wide range of disaster events.

The USDA has a robust priority services program, which enlists the support of 85 staff members representing each bureau and staff office. The Department manages an average of 1,500 GETS cards, close to 300 Wireless Priority Service assignments, and over 100 Telecommunication Service Priority circuits.

USDA continues to strengthen its Continuity of Operations Communications capabilities by routinely testing equipment and services in compliance with National Communications System Directive 3-10, *Minimum Continuity Communications Requirements*.

Significant Accomplishments

The USDA, working in conjunction with the Department of Homeland Security Office of Emergency Communications and Fire and Law Enforcement agencies from throughout the country, established a Type III All-Hazard Communications Unit Leader course and is working on a Type III All-Hazard Communications Technician course. USDA's radio cache supplied radios/communications equipment and spectrum support to wildland fire incidents in seven Geographic Areas.

Department of Commerce (DOC)

NS/EP Telecommunications Missions

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 conducts the constitutionally mandated decennial census, which is the basis of representative democracy.

Agencies operating within the DOC 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 (NTIA), Patent and Trademark Office, National Institute of Standards and Technology (NIST), 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's (NCS) Committee of Principals and Council of Representatives, the National Cyber Response Coordination Group, the Critical Infrastructure Protection Policy Coordination Committee, the Committee on National Security Systems, 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 objectives:

- The DOC is involved in homeland security initiatives and efforts to enhance preparedness with the necessary information technology equipment, software, and hardware upgrades. The DOC Headquarters is located in the Herbert C. Hoover Building (HCHB) located in Washington, DC 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 liquid crystal display 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.
- 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.

- NOAA's Hybrid Single-Particle Langranqian Integrated Trajectory System (HYSPLIT) supports emergency planners and first responders in detecting and tracking chemical and biological weapons in the atmosphere. At the local/regional level, field forecasters regularly respond to requests for dispersion forecasts from State and local emergency managers. At the national level, the model is often applied to needs from the aviation industry and air quality regulators. Internationally, NOAA responds through its participation with the World Meteorological Organization and the International Atomic Energy Agency by providing dispersion model forecasts in the event of a large scale nuclear incident. This is important because the accidental or intentional release of chemical, biological or nuclear agents can have significant health, safety, homeland and national security, economic, and ecological implications. The HYSPLIT model is a tool that helps explain how, where, and when chemicals and materials are atmospherically transported, dispersed, and deposited. Having this understanding is essential for responding appropriately and preventing disaster. For instance, accurate predictions of the path of a chemical release help emergency managers evacuate the affected people and predictions of volcanic ash plume locations allow aircraft to avoid dangerous areas.

- In response to the World Trade Center (WTC) tragedy, NIST conducted a three year building and fire safety investigation to study the factors contributing to the probable cause (or causes) of post impact collapse on WTC towers. To advance emergency planning, the study was expanded to include research in areas of prevention of progressive collapse, fire resistance design and retrofit of structures, and fire resistive coating for structural steel. As a result, the New York City Police Department has produced a report titled, *How to Prevent and Mitigate the Effects of a Terrorist Attack on a Building*, and stated that many of its guidelines incorporated recommendations and best practices from the NIST study.

The DOC serves as a lead government agency implementing alternative communications technology with an emphasis on the Internet and electronic-commerce, as well as methods for protecting government networks. The DOC continues to promote and support the use of NCS services and programs, especially in light of recent hurricane disasters and post-9/11 security programs.

Department of Health and Human Services (HHS)

NS/EP Telecommunications Mission

The national security and emergency preparedness (NS/EP) mission of the Department of Health and Human Services (DHHS) is to lead the Nation in preventing, responding to and reducing the adverse health effects of public health emergencies and disasters. This includes assisting internal and external stakeholders in public health in obtaining sponsorship for various priority telecommunications programs, and assisting divisions of DHHS with NS/EP requirements such as National Communications System (NCS) 3-10, *Minimum Requirements for Continuity Communications*. The Office of Preparedness and Emergency Operations is further responsible for ensuring that the Department has the systems and logistical support in place to coordinate the Department's operational response to manmade or natural public health and medical threats and emergencies.

Current/Ongoing NS/EP Telecommunications Activities

Current emphasis continues to be on enhancing disaster communications during all-hazards events. Some of the areas include:

- Continuing to increase awareness of priority telecommunications programs within the healthcare sector. This is especially important in a pandemic environment where social distancing will place additional burdens on the telecommunications infrastructure.
- Government Emergency Telecommunications Service (GETS)/Wireless Priority Service. Ensure each of our over 100 National Disaster Medical System teams have GETS cards for their command staff, and are trained in their use.
- 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 (FCC) to publicize available systems and best practices. Many additional health care facilities now have priority telecommunications programs such as Telecommunication Service Priority due in large part to the shared effort between DHHS and FCC.
- Enhancing interoperability by continuing to work with the Department of Homeland Security and the Federal Emergency Management Agency in frequency coordination, equipment purchase and training. By using a common "code plug" of frequencies DHHS teams can interoperate or share equipment with other responders.
- Increasing the supply and portability of Satellite Internet systems. This included re-engineering our current kits to include a larger quantity of spares and supplies such as fiber optic cable.
- Continuing implementation and testing of NCS Directive 3-10 for all systems involved with continuity.

Department of Transportation (DOT)

NS/EP Telecommunications Mission

The Department's mission as outlined in the Department of Transportation (DOT) Strategic Plan, asserts that the Department will "serve the United States by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people."

This core mission of the Department is constant. We remain flexible to the ever-expanding global economic environment.

Current/Ongoing NS/EP Telecommunications Activities

The Department is an extremely active participant in the National Communications System's (NCS) Committee of Principals and Council of Representatives, the President's National Security Telecommunications and Advisory Committee, and 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 Department and the resulting benefits realized.

Government Emergency Telecommunications Service/Wireless Priority Service (GETS/WPS)

DOT has insured that all essential personnel have not only received GETS cards and WPS on their government furnished cell phones, but that the services are tested on a regular basis.

Continuity of Operations (COOP)

DOT is a willing participant in all of the Exercises mandated by the National Exercise Program and seeks out intra-agency partners to test communications capabilities. The DOT National Continuity Programs Office is continually testing and training to ensure that the Department has a viable, functional, and interoperable communications system.

These frequent tests ensure that DOT senior leadership can communicate swiftly, securely and efficiently with both the Executive Branch and the DOT Operating Administrations (OA) under all circumstances.

The DOT continues to conduct internal communications tests quarterly along with the OAs to assess the viability of their communications systems (including, secure/non-secure voice, fax, and data systems). The Department, along with many other departments and agencies, participates in regularly scheduled inter-agency communications tests to assess the departments and agencies' abilities to communicate with each other using an array of communications media.

On a quarterly basis, the external communications test results from each department and agency are reported to the White House. DOT demonstrates the ability to communicate during each internal and external communications test cycle.

DOT initiated a resiliency program to provide greater options for COOP. When activated, this program allows the Secretary and a primary successor to operate simultaneously from different continuity locations. Robust and interoperable communications, in both unclassified and classified environments, are keys to the success of the resiliency program.

Cybersecurity

The DOT launched its new Cyber Security Management Center (CSMC). The DOT CSMC had been in the planning stages for two years and was designed to consolidate all cybersecurity incident response activities within the Department. This has been a successful venture for the Department and the CSMC has gained positive recognition in the Federal cybersecurity community. The DOT has also participated in several Federally sponsored exercises, the most noteworthy being Cyber Storm Exercises. As in all Cyber Storm exercises, the transportation sector was a primary focus of this exercise.

Department of Energy (DOE)

NS/EP Telecommunications Mission

The U.S. Department of Energy (DOE) utilizes a number of the national security and emergency preparedness telecommunications activities in support of DOE missions to advance the National, economic, and energy security of the United States. These activities include the ability to respond to natural disasters as well as adversarial situations.

Department of Energy Headquarters

The Department presently has 1,472 Government Emergency Telecommunications System cards and 299 Wireless Priority Service accounts, and continues to ensure the Telecommunications Service Priority requirements are kept up to date. DOE is presently in the process of designing and engineering the High Frequency-Automatic Link Establishment and the stationary Satellite Phone System, the last items necessary to meet the requirements included in National Communications Systems Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, at the Headquarters and the primary Alternate Operating Facility. The Devolution Alternate Facility will be delayed due to the requirement for a Sensitive Information Compartmented Facility.

DOE participated in exercise EAGLE HORIZON 09 (EH09), a Federal Emergency Management Agency-sponsored interagency continuity exercise held June 17, 2009. This was the first exercise for the new Secretary of Energy and his Chief of Staff to observe and participate. During the tabletop exercise, the Continuity Emergency Management Team fine-tuned some of the functions and discussed how to improve other aspects of the team.

Savannah River Site (SRS)

SRS has completed the emergent frequency changes for the National Nuclear Security Administration, Office of Secure Transportation to the South Carolina Relay Station satellite earth station, as required by the satellite service provider.

SRS has established the South Carolina Palmetto 800 account and acquired programming information and access to the system for Aiken County Emergency Medical Services. This provides mutual aid support between the county and the site.

SRS has completed the installation of two replacement Air Craft radios for the Operations Center. The radios are used by the security forces to communicate with aircraft over flying the site.

Los Alamos National Laboratory (LANL)

The LANL trunked radio backbone is utilized by the Protective Force, the Emergency Management Office, Hazardous Materials (HAZMAT), Los Alamos Police and Fire Departments, and various crafts and support services. There are currently 296 talk groups and 3,526 portable, mobile, and base station radios. Seventeen consoles, geographically dispersed, provide dispatch capability.

Through conventional interface cards, operators communicate and have patching capability with Federal, State, and local law enforcement personnel as well as county and tribal emergency responders. Identical backbone equipment is located at two separate sites and connected to the trunked radio switch through fiber optic cables and microwave. The Fire Department and Emergency Management vehicles are equipped with Global Positioning System/Automatic Vehicle Location receivers.

Department of Veterans Affairs (VA)

NS/EP Telecommunications Mission

Deployable Communications

The Department of Veterans Affairs (VA), through the Office of Information Technology, has created the Office for Business Continuity, which is tasked to design a comprehensive emergency communications architecture for VA. Currently it includes a diverse set of technologies and services to support emergency preparedness and response activities, as well as day-to-day operations. The VA's main emergency communications system is the Very Small Aperture Terminal (VSAT) satellite system, which provides voice, video, and data network service in a single package. This is a rapid deployable system that can be deployed to an affected area during a disaster in a matter of hours. To extend its effectiveness, VSAT assets 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. In addition to these systems, the VA has recently acquired what we call Mobile Vet Centers. These vehicles are equipped with VSAT terminals and proper OIT equipment to help perform VA Primary Mission.

Centralization of Systems

VA has made great progress towards the centralization of its information technology resources. The Department has stood up various highly redundant data centers throughout the country that produce a more consistent implementation of VA's healthcare and benefits systems and so far have resulted 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 4 years. Additionally, 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 24x7 audio and video teleconferencing services for business meetings, program planning sessions, distance learning, interviews and hearings. VANTS customers include VA employees, emergency personnel, State officials, hospitals, universities, and other Federal Government agencies, including DOD. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 kilobits per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 1,512 audio ports for voice teleconferencing.

VA has joined the National Telecommunications and Information Administration in proving the viability of a Government-wide, classified data exchange to update the Government Master File of Radio Frequency Authorizations in real time over the public switched telephone network.

VA coordinates with the 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 MXUs 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.

Department of Homeland Security (DHS)

NS/EP Telecommunications Mission

DHS Wireless Services

The Wireless Services Branch (WS) under the Department of Homeland Security (DHS) Office of the Chief Information Officer (CIO) supports the national security and emergency preparedness (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 Office of Emergency Communications (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.

The following accomplishments are a result of collaboration between DHS WS and OEC during fiscal year (FY) 2009:

- Secure and protect numerous spectrum assignments supporting Federal Protection details for events (Presidential Inauguration), emergency response events and disasters (California fires), and daily mission-critical operations (securing the border);
- Continue working with the Components through the DHS Wireless Working Group to coordinate tactical wireless needs, resources, and activities across the Department;
- Develop a Department-wide strategy to improve the efficiency, effectiveness, and interoperability of DHS tactical wireless investments through coordination and resource (infrastructure, spectrum) sharing. This strategy includes the establishment of a new joint wireless program office to provide Departmental strategic planning, oversight, and coordination for tactical wireless investments;
- Provide guidance and coordination support to Customs and Border Protection (CBP) and Immigration and Customs Enforcement to ensure alignment of American Recovery and Reinvestment Act (ARRA) tactical wireless investments with Departmental strategies and policies. As part of this support, WS presented the DHS cross-cutting tactical wireless strategy to the ARRA tactical wireless mini-Acquisition Review Board;
- Collect and consolidate the Department's tactical wireless budget requirements for FY 2011-FY 2015 in accordance with DHS Deputy Secretary guidance;
- Provide continued programmatic, acquisition, and engineering support to the DHS Components to restore critical wireless capabilities lost due to the congressionally mandated transition of all Federal systems off the 1710-1755 megahertz frequency band. As part of this support, WS has begun developing a funding request package to Office of Management and Budget (OMB) for approximately $100M to complete the transition;
- Coordinate with Components on the development of the Wireless Management Directive 4100 revision (MD 4100.2); and
- Develop an Interagency Agreement with the DHS OEC to provide technical operations support for the development of wireless digital audio and video surveillance equipment standards supporting Federal law enforcement and investigative operations.

Homeland Secure Data Network (HSDN)

By the end of FY 2009, the DHS deployment of the Homeland Secure Data Network (HSDN) reached 138 government sites, providing a unified system and program that enables the sharing of SECRET-classified level data between DHS 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. HSDN is the single program within DHS that enables agencies to collaborate and communicate effectively at a

SECRET-classified level among Federal and State government and supporting entities. With HSDN capabilities, DHS can collect, disseminate, and exchange both tactical and strategic intelligence information throughout DHS and DHS partners.

HSDN has continued supporting DHS and its homeland security partners mission requirements by identifying applicable advancing information and applied technologies that are capable of improving data collection, analysis, and dissemination of SECRET-classified information. In FY 2009, HSDN:

- Maintained periodic HSDN program self-assessments and evaluations through the DHS-established Operational Analysis periodic review and reporting process, for identifying areas for improvements in costs and operational efficiencies and effectiveness;
- Continued support to the mission requirements of DHS and its homeland security partners by identifying applicable advancing information and applied technologies that are capable of improving data gathering, fusion, analysis, intelligence gathering, and dissemination at a SECRET-classified level;
- Completed a security assessment of HSDN by the National Security Agency Blue Team. The final report states that HSDN was in a "very good" security posture and is a "well managed network;"
- Achieved and maintained a Green rating on the OMB Federal IT Dashboard;
- Completed recertification for 43 FY 2005 HSDN sites and 13 FY 2006 HSDN sites;
- Achieved Authority to Operate for the HSDN Core 3-year required recertification;
- Deployed 26 new HSDN sites to the network to include 7 other Government agency sites, for a total of 138 sites;
- Transitioned the HSDN Data Center equipment (26 populated racks of equipment) from Fairlakes facility to DHS Data Center 2;
- Initiated deployment of the Secure Mobile Environment Portable Electronic Device to provide classified wireless communications for voice and data for the support of tactical, strategic and Homeland Security environments;
- Designed and began a pilot for a new Enterprise Portal. The Enterprise Portal is an enterprise class, web-based, and real-time collaboration application to allow organizations within DHS to collaborate and share information. The Enterprise Portal will provide support for Communities of Interest: Wikis, blogs, message boards, Web Meetings, Instant Messaging, Document libraries and Static Web pages;
- Implemented ISSE Guard pilot for CBP, which is a controlled interface that enables the bidirectional flow of data between two or more security domains accredited for operation at different classification levels;
- Deployed the ISSE Guard pilot, Chiliad Discovery/Alert™. Chiliad Discovery/Alert™ is a comprehensive, revolutionary software platform that allows for on-the-fly analysis and extraction, real-time knowledge fusion, dynamic navigation, and instant alerts across extended enterprises;
- Hosted Secret Risk Management System and Secret Trusted Agent on HSDN for use by DHS components conducting Certification and Accreditation activities on collateral classified systems;
- Provided the DHS Executive Communications Team with SECRET-level data and video teleconferencing access in support of senior level staff while between DHS locations and in remote locations with no fixed DHS network access; and
- Supported DHS National Level Exercise 2009 with on-site personnel.

Office of Emergency Communications

The DHS OEC was established by Public Law 109-295, the "Post-Katrina Emergency Management Reform Act of 2006." Director Chris Essid leads OEC, which supports and promotes the ability of emergency responders and government officials to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters. In addition, OEC works to ensure, accelerate, and attain interoperable and operable emergency communications nationwide.

Stakeholder partnerships across jurisdictions and agencies are essential for improving emergency communications nationwide. The following accomplishments are a result of collaboration and accountability among OEC and State, local, and tribal governments; emergency first responders; and the private sector:

- Supported the implementation of the National Emergency Communications Plan (NECP), the Nation's first strategic plan targeted at improving emergency response communications. More than 80 percent of the 55 milestones set to be completed within the first 12 months of the Plan were completed on schedule;
- Conducted Statewide Communications Interoperability Plan (SCIP) Implementation Workshops in 51 States and territories;
- Released a guide on Establishing Governance to Achieve Statewide Communications Interoperability;
- Provided more than 150 technical assistance training sessions in all 56 States and territories, focusing on risk and impact and aligning with SCIP and NECP implementation efforts;
- Strengthened existing partnerships and engaged new audiences in States and localities nationwide through a variety of stakeholder engagements;
- Developed SAFECOM grant guidance and the Interoperable Emergency Communications Grant Program guidance for FY 2009;
- Trained more than 1300 Type III Communications Unit Leaders;
- Participated in the signing, in Mexico, of the bilateral telecommunications agreement created by the United States-Mexico High-Level Consultative Commission on Telecommunications;
- Facilitated the establishment of interoperable communications capabilities for the 2010 Olympics Coordination Center in the State of Washington; and
- Hosted the first National Conference on Emergency Communications, April 2009, Chicago, Illinois.

Office of the Director of National Intelligence (ODNI)

NS/EP Telecommunications Mission

The national security and emergency preparedness telecommunications mission of the Office of the Director of National Intelligence (ODNI) is to ensure the secure flow of all-source foreign intelligence information to the President, and other selected national policy makers. To this end, ODNI ensures that Intelligence Community organizations together provide secure, rapid, and reliable 24x7 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
- Capable of world-wide quick reaction in support of crisis and special operational requirements.

Telecommunications Staff Organization

The DNI Chief Information Officer (CIO), as the Intelligence Community (IC) CIO, manages activities relating to Information Technology (IT) infrastructure and enterprise architecture requirements of the IC, including: messaging; telecommunications; and information services capabilities.

Current/Ongoing NS/EP Telecommunications Activities

Active participation in the National Communications System (NCS) activities of the Committee of Principals, Council of Representatives, and underlying working groups.

Active participation as a member of the Joint Telecommunications Resources Board.

Continuing to work with ODNI Continuity Programs to assure proliferate Government Emergency Telecommunications Services, the Wireless Priority Service, the Telecommunications Service Priority, and other NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, requirements in accordance with the ODNI's Implementation plan for achieving compliance with NCS 3-10.

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

ODNI Significant Accomplishments

- Continuing implementation of the Intelligence Community Login capability, providing the architecture for personnel from IC agencies to access their home organization's IT infrastructures from remote locations.
- Assisted numerous departments and agencies with developing plans for compliance with the requirements for Top Secret/Sensitive Compartmented Information connectivity now required by NCS Directive 3-10.

Federal Emergency Management Agency (FEMA)

NS/EP Telecommunications Mission

The mission of the Federal Emergency Management Agency (FEMA) is to reduce the loss of life and property, and protect the Nation's critical infrastructure and constitutional forms of government from man-made and natural hazards through a comprehensive program of mitigation, planning, response, and recovery. 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 systematically evaluates and adopts new technologies, and provides recurring technical exercises and guidance for Federal, State, and local governments to ensure the preservation and continuation of our form of government under the Constitution.

Current/Ongoing NS/EP Telecommunications Activities

FEMA provides critical infrastructure support to communities, counties, 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, as well as other Federal partners to promote interoperability. 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;
- 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;
- Ensures the location of key government officials during all emergency and non-emergency conditions; and
- Coordinates the assignment and use of all Federal radio frequencies at an incident site to include high frequency, 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.

FEMA National Continuity Programs Directorate (NCP) Readiness – Significant Achievements

To enhance communications interoperability, FEMA continues to develop and foster inter agency partnership with other Federal agencies, as well as State and local governments, through recurring communications exercises. FEMA regularly participates in the Department of Defense (DOD) Interoperability Communications Exercise (DICE) and Joint User Interoperability Communications Exercise to test and evaluate agency-wide telecommunications capabilities. However, FEMA understands that true interoperability can only occur when advanced technical resources are bolstered by reliable operational procedures. To this end, FEMA continues to lead a number of operations-driven exercises, such as Eagle Horizon and Determined Accord, to evaluate not only

interagency communications but the implementation and operational procedures that facilitate and enable interoperable communications.

FEMA operates and maintains the FEMA National Radio System (FNARS) to provide the President and other Federal officials with resilient and assured voice and limited data capability to the FEMA regions, State Emergency Operations Centers, key alert and warning facilities, and other locations to help meet information sharing requirements at any time, across the full threat spectrum. FNARS is currently undergoing a major modernization to replace outdated and logistically unsupportable equipment.

FEMA operates and maintains the Internet Protocol Locator (IPL) which ensures that key government officials can be located during all emergency and non-emergency conditions. The IPL system is currently under lifecycle replacements.

The Readiness Reporting System (RRS) is a continuity monitoring system designed to measure and report both the individual and aggregate abilities of Federal departments and agencies to continue their Priority Mission Essential Functions in support of the required National Essential Functions. The RRS is used to conduct assessments and track capabilities at all times under all conditions, including natural disasters, manmade incidents, terrorism, and war. FEMA has been charged with developing, operating, and maintaining the RRS system to measure continuity capabilities of the Federal Executive Branch departments and agencies

FEMA's Disaster Operations Role

FEMA's commitment to the nation's need for rapid, reliable, interoperable communications continues to serve as a driving force in FEMA's vision for supporting Federal, State, local, and tribal agencies in accomplishing their mission. Many of the elements necessary to achieve this vision are being set in motion. This involves defining the Agency's national strategy for rapid response, internal agency assessments, strategic policy reviews, acquisition system enhancements, refinement of our requirements-based approach to procurement, and joint interagency doctrine development. The groundwork is clearly established to address and resolve current and future operability and interoperability issues while providing new capabilities to the nation's disaster responders.

FEMA leads and coordinates the Federal Government's disaster response, continuity efforts, and restoration of information technologies and communications essential for an effective response. Through FEMA's Disaster Operations Directorate (DOD), communications activities are accomplished that are necessary to unify all communicators around one common effort—the delivery of information to emergency responders. This common vision within FEMA establishes an interconnected system of communications capabilities across all levels of government that provides mission critical information and situational awareness vital to decision making. Strategic, operational, and tactical infrastructures must converge to provide seamless connectivity throughout the designated disaster area, from the incident site to national-level command and control facilities.

One of FEMA's near term goals in its support of NS/EP communications is to build a robust emergency communications program that delivers the information needed for operational and tactical command and control during disaster response operations.

Disaster Operations Directorate Key Communications-Related Accomplishments for 2008-2009

- Supported the response to North Dakota flood, Kentucky ice storm, and other disasters by deploying Mobile Emergency Response Support to facilitate air-to-ground communications, augment communications in remote areas, and support live-video feeds;
- Established all 10 mandated Regional Emergency Communications Coordination Working Groups (RECCWG) that consist of Federal, State, and local representatives, and other non-government agencies to address interoperable emergency communication concerns;
- Developed 27 State, 15 Emergency Support Function, and 4 regional emergency communications plans that allow FEMA to be better prepared to preposition and deploy communications resources during catastrophic incidents;
- Developed 11 pre-scripted Mission Assignments with the Federal Communications Commission, National Communications System, United States Coast Guard), DOD, and United States Forest Service to facilitate rapid response for communications requirements;

- Provided communications planning and coordination with other Federal agencies during the 2008 Democratic National Convention, 2008 Republican National Convention, and 2009 Presidential Inauguration;
- Developed a National Response Network Strategy for enabling interoperable emergency communications through the use of Internet Protocol-based networks;
- Hired 10 Regional Disaster Emergency Communications Coordinators to improve emergency and interoperable communications within and between States and FEMA Regions;
- Developed a National Charter for the RECCWGs to define the RECCWG mission, responsibilities, membership, meeting schedule, and general procedures;
- Participated in multiple emergency communications exercises to include DICE, Vigilant Accord, and Eagle Horizon;
- Upgraded all Mini-Emergency Operations Vehicles to include enhancements for voice, video, and data communications capabilities;
- Upgraded all Incident Response Vehicles to include streaming air-to-ground video capability;
- Acquired transportable communications towers with interchangeable Land Mobile Radio and microwave line of sight capabilities with greater operational range.

Central Intelligence Agency (CIA)

NS/EP Telecommunications Mission

The national security and emergency preparedness (NS/EP) telecommunications mission of the Central Intelligence Agency (CIA) is to ensure the secure flow of all-source foreign intelligence information to the President, Director of National Intelligence, and other selected national policy makers. To this end, CIA provides secure, rapid, and reliable 24x7 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;
- Supportive of crisis and special operational requirements through world-wide quick reaction.

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 NS/EP Telecommunications Activities

- Active participation in the efforts of the National Communications System's Committee of Principals and Council of Representatives.
- Continued support of the Government Emergency Telecommunications Services, Wireless Priority Service, and Telecommunications Service Priority programs.
- Continued to transition CIA legacy secure telephone units to the new Secure Terminal Equipment.
- Continued to increase CIA participation in the continuity community communications and Information Technology (IT) infrastructure testing over the past year through the addition of new capabilities and facilities and improving our test results.
- Continued to improve CIA Continuity of Operations/ Disaster Recovery (DR) posture by making several improvements in our DR architecture. Significant effort has been channeled into virtualization of our IT storage to reduce environmental loads in data centers while increasing performance and high availability for critical mission essential functions (MEF). Another main focus has been on efforts to eliminate or mitigate single points of failure, especially in the transport layer.
- Continued to enhance telecommunications services between the CIA, other U.S. Government organizations, and the U.S. military services.

CIA Significant Accomplishments

- Established a new agency-wide regulation requiring that all critical mission essential systems and applications be identified at the earliest phases of planning, and that disaster recovery planning be incorporated throughout the project lifecycle.
- CIA Primary Mission Essential Functions (PMEF) were officially approved this year. CIA completed working with internal business leads and IT support to identify mission critical systems and applications that support CIA PMEFs and MEFs, along with their associated Recovery Time Objective and Recovery Point Objective specifications.

General Services Administration (GSA)

NS/EP Telecommunications Mission

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

GSA consists of two integral components—The Public Building Service and the Federal Acquisition Service (FAS). Within the FAS, the Office of Integrated Technology Services (ITS) provides telecommunications and network services to Federal departments and agencies. ITS works with agency customers to understand their requirements, simplify the acquisition process, and provide assistance throughout implementation, enabling agencies to focus on their respective missions and avoid dealing with acquisition complexities.

The GSA mission support functions for national security and emergency preparedness (NS/EP) are detailed in the 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, Section 706, War Emergency Powers;
- National Response Framework;
- National Security Presidential Directive-51/Homeland Security Presidential Directive-20, *National Continuity Policy;*
- National Continuity Implementation Plan; and
- National Communications System Directive 3-10, *Minimum Continuity Communications Requirements.*

Current/Ongoing NS/EP Telecommunications Activities

FAS-ITS assists agencies in developing solutions using its portfolio of information technology (IT) and Network Services contracts to satisfy mission needs of 135 Federal agencies both domestically and around the world.

GSA's Networx Universal and Networx Enterprise contracts are 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 the SatCom-II contract, GSA Schedule 70 acquisitions, GSA Government-wide Acquisition Contracts and other integrated technology resources, ITS is a one-stop shopping facility for virtually any IT requirement.

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

GSA Telecommunications Specialists are appointed in each geographic region to serve as the National Communications System (NCS) Regional Manager (NCSRM). The NCSRM conducts planning for Emergency Support Function (ESF) #2 disaster communications response. Responsibilities include regional emergency disaster response planning efforts and training and participation in Federal Emergency Management Agency (FEMA)-led exercise activities. Additionally, the NCSRM fosters working relationships with the telecommunications industry within the respective region, ensuring a mutually coordinated government/telecommunications industry emergency response effort. During the pre-deployment phase, the NCSRM coordinates and assesses potential emergency telecommunications requirements throughout the assigned region. Upon FEMA activation of ESF#2, the NCSRM assists with critical communications restoration efforts. During catastrophic events, the NCSRM provides ongoing situational awareness and may be requested to assume the role of the Federal Emergency Communications Coordinator (FECC) to deconflict competing demands for service and prioritize restoration efforts. During disaster response efforts, the

NCSRM/FECC provides status, information, and recommendations for the restoration of critical telecommunications requirements within the affected area to the National Coordinating Center (NCC) and the Federal Coordinating Officer.

GSA/FAS Significant Accomplishments

- GSA supported FEMA and the NCS regional disaster response and training efforts during the 2009 calendar year.
- GSA deployed emergency telecommunications support personnel for the restoration of critical NS/EP communications capabilities in the regions impacted by hurricanes Dolly, Gustav, and Ike.
- GSA regional personnel closely monitored the rapidly spreading wildfires in southern California and during the North Dakota floods and prepared for deployment as necessary.
- GSA provided extensive support communications and logistics services in support of Presidential transition.
- GSA continued FAS-ITS participation in the National Defense Executive Reserve—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 may be called upon to augment the FAS-ITS staff or other Federal departments and agencies when organizations must rapidly mobilize to respond to national security emergencies.
- GSA continues to promote the Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP) and Wireless Priority Service (WPS) programs to its communications customers and to manage the issuance of GETS and WPS capabilities internal to GSA.
- FAS-ITS is a contributing member and participates in activities of the Committee on National Security Systems, the Joint Telecommunications Resources Board, Continuity of Operations (COOP)/Continuity of Government exercises, the Continuity Communications Working Group, the Communications Government Coordinating Committee, the Information Technology Government Coordinating Committee, the NCC, the NCS Committee of Principals (COP) and Council of Representatives, the NCS COP Priority Service Working Group, the NCS COP Communications Dependency on Electric Power Working Group, and the TSP Oversight Committee.

Other Significant Activities

On a continuing basis, FAS-ITS modifies IT and Network Services contracts to ensure that they meet NS/EP requirements for interoperability, survivability, and other anticipated needs that may arise during emergency situations. FAS-ITS also provides readily accessible acquisition services to FEMA, the NCS, and Federal, State, local, and tribal governments in order to facilitate rapid recovery efforts.

FAS-ITS continues to provide industry components and Federal departments and agencies with current information regarding available products and services, including disaster support, contingency planning, and COOP services. GSA capabilities are further promoted through participation in a number of multi-agency committees, working groups, and the GSA website (*http://www.gsa.gov*).

National Aeronautics and Science 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 successfully accomplishing national-level programs approved by the White House. This includes Telecommunications Service Priority (TSP), Wireless Priority Service, and the National Telecommunications Management Structure.

NASA also continues to 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

The NASA Integrated Services Network (NISN) supports both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency and with 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's 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 customer satellites.

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

NASA's 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;
- Participated in TSP;
- Participated in the Title Globe exercises; and
- Participated in the Eagle Horizon 2009 exercises.

Nuclear Regulatory Commission (NRC)

NS/EP Telecommunications Mission

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

The Commission's national security and emergency preparedness (NS/EP) telecommunications provide for highly reliable connectivity between the NRC emergency operations center and 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 communicating relevant information during accidents or events at NRC-licensed facilities.

Current/Ongoing NS/EP Telecommunications Activities

The NRC supports National Communications System (NCS) NS/EP programs and remains active in the NCS Committee of Principals and Council of Representatives activities. The systems and programs used in support of NS/EP telecommunications 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, 51 NRC-licensed nuclear facilities use ETS with Telecommunications Service Priority through FTS 2001 and 23 facilities use private corporate systems. Satellite phones are used by headquarters and regional staff and resident 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 with continuity responsibilities. 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, Secure Video Teleconferencing is used in the Headquarters Operations Center and at all the NRC Regional Incident Response Centers. Monthly tests of all communications assets are conducted from the Headquarters Operations Center and its backup location. NRC staff test GETS, satellite phones, and WPS quarterly.

NRC Significant Accomplishments

- NRC completed installation and implementation of a web-based incident management tool to coordinate with other Federal and State agencies.
- Secure Iridium satellite phones were purchased and fielded to support continuity of operations management and in accordance with NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* requirements.

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 the Federal Government's 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 U.S. spectrum policy for the 21st century. A key goal of OSM is to fully automate the spectrum management business processes to improve effectiveness and efficiency in all Federal spectrum use, including NS/EP applications. Specific examples of activities in this regard include the following:

- Development of the initial release of the Federal Spectrum Management System (FSMS);
- 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;
- Planning the scope of future FSMS releases; and
- 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 both NS/EP and normal conditions.

In addition, NTIA is continuing to:

- Serve as a principal member of the JTRB and its senior staff working group;
- 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;
- Support 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 (COR) activities and endeavors, including the NCS COP Priority Services Working Group and Communications Dependency on Electrical Power Working Group;
- Participate in the NCS SHared RESources High Frequency Interoperability Working Group activities.

Significant Accomplishments

- Fully supported the Office of the Manager, NCS (OMNCS) relative to the National Response Framework Emergency Support Function 2-Communications (ESF #2). NTIA participated in the OMNCS biweekly ESF #2 training activities.

- Coordinated and assisted in developing the spectrum management portions of the OMNCS ESF # 2-Standard Operating Procedures (ESF# 2-SOP), the Federal Emergency Management Agency Joint Field Office-Standard Operating Procedures (JFO-SOP) and the 2009 Federal Interagency Hurricane Concept Plan.

- Continued development of the Federal Strategic Spectrum Plan.

- In coordination with the National Highway Traffic Safety Administration (NHTSA): 1) provided over $40 Million to 30 U.S. States and territories to help 911 call centers across the country improve the ability to locate people calling from wireless and Internet-connected telephones; 2) delivered to Congress, a national plan for migrating to a national Internet Protocol-enabled emergency network capable of receiving and responding to all citizen-activated emergency communications and improving information sharing among all emergency response entities.

- 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.

- Through the NTIA Emergency Response Group (ERG), participated in Exercise Eagle Horizon 2009 (EH09) from the primary NTIA alternate facility. The following objectives were developed for EH09, based on the multiple threat scenarios in accordance with National Security Presidential Directive 51/Homeland Security Presidential Directive 20, the National Continuity Policy Implementation Plan, and the Federal Continuity Directives: 1) exercise the Federal Executive Branch Continuity alert, notification, and deployment procedures; 2) implement interagency continuity communications; 3) exercise department and agency Continuity implementation and operational procedures; 4) review and update the viable elements of the department and agency continuity capability; and 5) assess the department and agency ability to identify and prioritize essential functions and conduct operations from pre-planned alternate locations. Twenty-four members of the NTIA ERG relocated to the alternate relocation site.

- Participated in the monthly Exercise Title Globe 2009 communications drills.

National Security Agency (NSA)

NS/EP Telecommunications Mission

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

Information Technology and Information Assurance

Within NSA, several organizations share responsibility in supporting NS/EP related activities: National Information Assurance Research Laboratory (NIARL), Information Assurance (IA) Worldwide Enterprise, and the Technology Directorate (TD).

- The NIARL conducts and sponsors research in the technologies and techniques needed to secure U.S. national security systems, including cryptography, high-confidence software and systems, authentication, high speed security solutions, secure wireless multimedia, secure operating systems, secure 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 DOD's emerging Global Information Grid (GIG); developing and evaluating secure information systems and its sub-components; developing and evaluating tamper protection products; and providing trusted microelectronics products.

- The TD plans and operates the telecommunications systems and networks that link NSA elements worldwide, and also provides connectivity to other Government services.

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, the Department of Homeland Security, and other entities with IA responsibilities. Information assurance should be an integral part of any continuity plan and/or recovery in the event of a national crisis or emergency.

Current/Ongoing NS/EP Telecommunications Activities

NSA Commercial Solutions for NS/EP Telecommunications

- The National Cryptographic Solutions Management Office (NCSMO) is tasked with leading the effort to transform and modernize cryptographic capabilities for the 21st century. The NCSMO coordinates and oversees cryptographic transformation by supporting the replacement of 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 GlG architecture.

- The NCSMO conducted an end-to-end cryptographic capability and risk analysis of the National Communications System (NCS) requirements and architecture identified in NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*. Analysis of the results identified capability gaps and risk areas for senior leader consideration and will be incorporated into a national strategy and roadmap for cryptographic solutions.

- A major focus of the NSA has been the development of the Secure Mobile Environment Portable Electronic Device (SME PED). SME PED, now in production, provides transformational capability allowing secure mobile voice and Internet Protocol (IP) based services critical to sustaining interoperability with State and

Local governments and first responders. SME PED has been approved to operate on all Defense Information Systems Networks (DISN) and has reached full operational capability.

- 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 Encryptor Interoperability Specification (HAIPE IS) features a variety of management, cryptographic and networking enhancements. This version specifies use of additional updated commercial standards and adds functionality to reduce the amount of bandwidth required for operation.

- High-level security design requirements to guide vendors in developing non-Cryptographic Controlled Items, IPsec, and HAIPE compliant products were defined. The requirements and specifications define the future of encryptor development efforts.

- Devices compliant with HAIPE IS version 3.0 were certified and are available for purchase.

Key Management Infrastructure (KMI) for NS/EP Telecommunications Systems

- NSA is implementing Key Management Infrastructure (KMI) modernization to support Cryptographic Modernization objectives and the GIG IA strategy. The development of KMI for DOD is a critical foundation element for ensuring an adequate security posture for national security systems by providing transparent cryptographic capabilities consistent with operational imperatives and mission environments. KMI is an infrastructure that will generate, distribute, and manage key products for the cryptographic inventory used to protect national security information. The KMI is vital to achieving an effective IA posture for the Defense Information Infrastructure and the broader national security community. The KMI will improve on existing information protection using technology transfer to ensure responsive Critical Design Reviews (CDR) as well as the System CDR. It successfully demonstrated the Over the Network Keying emulator being developed to assist End Cryptographic Unit developers who are planning to connect to the KMI. Coding has begun and the team has successfully compiled and executed two incremental systems builds during 2009.

Enterprise Security Management (ESM) Supporting NS/EP Telecommunications Systems

- ESM, along with Enterprise Services Vulnerability Management and Cyber Network Defense, support mission management and the successful employment of information systems within the enterprise. ESM is identified by Information Assurance Directorate Senior Leadership as a key strategic initiative. ESM will evolve to an integrated and comprehensive set of enterprise security services and capabilities, including:

  1. Identity Management
  2. Attribute Management
  3. Credential Management
  4. Privilege Management
  5. IA Metadata Management
  6. Policy Management
  7. IA Configuration Management
  8. Audit Management
  9. Cryptographic Key Management
  10. Authentication

- The first steps in the evolution include a Privilege Management Pilot (PMP) to be launched in the operational space of an identified Combatant Command customer in fiscal year (FY) 2009. A second PMP will address federation in FY 2010. Initiatives supporting IA Configuration Management and IA Audit Log Management commenced mid-FY 2009.

- The NSA has also taken the lead on defining several ESM essential standards. Those standards include IA metadata, identity attribute, and configuration for technical security operations enabling vulnerability management, measurement and policy compliance evaluation and identification of anomalous or malicious network activity.

Security Assessment 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, and TEMPEST services. Technical advice and assistance in support of assessments and evaluations within annual exercises have also been provided.

Vulnerability Analysis and Operational Assessments Supporting NS/EP Telecommunications Systems

- The NSA provides vulnerability analysis and operational assistance to the national security community regarding computer network defense. These activities are accomplished through community coordination, policy and analysis 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 promote strong and actionable countermeasures and recovery. These assessments provide a unique look at U.S. Government systems, operations, personnel, and current technology, which enable 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.

Senior Information Assurance Officer (SIAO) Supporting NS/EP Telecommunications Systems

- As a component of the 24x7 NSA Threat Operations Center – IAD has a 24x7 presence in the form of a SIAO on the watch floor. The SIAO functions on behalf of the IAD Director after-hours and has the ability to call in any personnel as needed to respond to national security needs.

COMSEC Utility Program (CUP) Supporting NS/EP Telecommunications Systems

- NSA operates the CUP to ensure it is able to meet emergency cryptographic needs for the national security community. The CUP maintains a pool of cryptographic devices that it can distribute immediately in response to a national security crisis, ensuring continuity of secure communications and the ability to establish new secure communications links when necessary.

Federal Reserve Board (FRB)

NS/EP Telecommunications Mission

The Federal Reserve Board's (FRB) national security and emergency preparedness (NS/EP) responsibilities relate to the maintenance of the national economic posture, and in particular: the operation and liquidity of banks; the maintenance of national monetary, credit, and financial systems; and the maintenance and restoration of stable and orderly markets. The FRB considers essential services and systems related to the national economic posture to include: critical funds transfer systems (wholesale/large-value payment systems); securities and derivatives clearing and settlement systems; supporting communications systems and service providers; and key financial market trading systems and exchanges.

Telecommunications Staff Organization

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

Current/Ongoing NS/EP Telecommunications Activities

The FRB supports National Communications System (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 and the Wireless Priority Service for Federal Reserve Banks, depository institutions it regulates, 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 – 2009

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 (e.g., 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.

There are 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.

In Fiscal Year 2009, the Federal Reserve is participating in the Cyber Fire, Cyber Financial Industry and Regulators exercise, which is sponsored through a public-private sector partnership with the Financial Services Sector Coordinating Council, the FS-ISAC, and multiple financial regulators. The exercise is an opportunity for the public and private sector to test their crisis management and incident response protocols and will result in a better understanding of the gaps in the financial sector's overall crisis management capabilities and reveal opportunities for improvement in security and resiliency.

Pandemic Flu Preparations

The FRB has developed contingency plans to continue the operation of the NS/EP priority telecommunications programs in the event of a pandemic flu outbreak. The plan incorporates the training and equipping of staff located in disparate regions of the country. In early 2009, The Federal Reserve exercised some of these practices to address the H1N1 outbreak in the United States.

Federal Communications Commission (FCC)

NS/EP Telecommunications 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, State, local, and tribal 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 their use.
- Providing expert technical advice to policymakers on wireless and wireline matters, broadcasters, satellite systems, land mobile radio systems, cable service providers and 911 call centers.

Current/Ongoing NS/EP Telecommunications Activities

- The FCC held three Summits and two Speaker Series Events during fiscal year 2009:[1]
  - Lessons Learned: 2008 Hurricane Season (December 11, 2008)
  - Pandemic Preparedness: Enhancing Communications Response for Health Care and First Responders (September 18, 2008)
  - Deployment and Operational Guidelines for Next Generation 911/E 911 Systems (February 25, 2009)
  - National Emergency Communications Plan, Chris Essid, Office of Emergency Communications, Department of Homeland Security (DHS) (October 22, 2008)
  - U.S. Department of Transportation's Role in Next Generation 911, Laurie Flaherty, Office of Emergency Medical Services, National Highway Traffic Safety Administration, Department of Transportation (October 22, 2008)
- Hits on the FCC's suite of public safety Web pages average nearly 120,000 per year. Content available includes a public safety clearinghouse, a searchable repository of over 250 emergency plans, guidelines, and reference materials.
- In September 2008, the FCC activated the Disaster Information Reporting System (DIRS) to provide communications situational awareness during Hurricanes Gustav and Ike. System improvements to DIRS have been identified and implemented, including a new reporting timeline to improve data accuracy and a vigorous outreach effort to broadcasters that resulted in 384 new accounts (and more than 1,000 total entities in DIRS).

- Project Roll Call also was activated successfully for Hurricanes Gustav and Ike.

- The FCC continues to meet with the Federal Emergency Management Agency (FEMA) to discuss the implementation of Next Generation Emergency Alert System in the context of FEMA's Integrated Public Alert and Warning System.

- On September 25, 2008, the FCC adopted a *Third Further Notice of Proposed Rulemaking* that proposes specific steps for achieving a broadband public safety network in the 700 Megahertz (MHz) band with nationwide interoperability.

- On January 13, 2009, the FCC submitted a cross border interoperability report to Congress and an updated report on the status of treaty negotiations with Canada and Mexico regarding the coordination of the re-banding of 800 MHz radios.

- On July 22, 2009, the FCC released its first annual *Report to Congress On State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*.

- On October 21, 2008, the FCC adopted rules to give interconnected Voice over Internet Protocol providers rights of access to any and all capabilities necessary to provide 911 and E911 service from entities that own or control those capabilities.

- In June 2009, an FCC outreach team went to Houston, Baton Rouge, Biloxi, Mobile, and Tallahassee where it conducted 26 meetings with over 250 State, county, and local public safety officials to discuss and learn about emergency response communications issues.

- In June of 2009, a FEMA-sponsored, FCC-organized training was held at the U.S. Naval Base Coronado focused on training FCC and FEMA personnel on the Project Roll Call spectrum monitoring equipment.

- In August of 2009, the FCC conducted a thirty-day review of its ability to respond to a major public emergency. A public release of the report is pending.

- The FCC is drafting a report to Congress in coordination with Canadian officials and DHS to facilitate expedited licensing and provide states with guidance regarding cross border interoperability. This report is due by December 4, 2009.

Footnote

1 See http://www.fcc.gov/pshs/summits

United States Postal Service (USPS)

NS/EP Telecommunications Mission

The U.S. Postal Service (USPS) 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. The USPS:

- Delivers 212 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;
- Handles more than 46 percent 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;
- The USPS is the second largest employer in the United States with nearly 656,000 career employees;
- The USPS does not receive tax dollars for operations, it is a self supporting agency, using revenue from the sale of postage and products to pay expenses;
- The USPS operates the largest civilian vehicle fleet in the world with more than 221,000 vehicles driving more than 1.2 billion miles each year and using 121 million gallons of fuel;
- The USPS provides services at:
  - More than 27,800 vending machines;
  - Nearly 33,000 commercial retail outlets;
  - Nearly 17,000 banking and credit union Automated Teller Machines;
  - 2,500 Automated Postal Centers®.
- Has annual operating revenue of nearly $75 billion;
- The USPS has the one of the largest e-mail systems, delivering more than 13 million emails a day with an average delivery time of less than five minutes;
- The USPS intranet is the largest in the world connecting more than 28,000 locations to critical business systems 24 hours a day, 365 days a year.

Benefits

Information Technology (IT) is dedicated to helping the USPS improve service and operations through technology. In the telecommunications area, IT has equipped key personnel with the tools necessary to continue operations in the event of national/local emergencies or disasters. IT has employed National Communications System (NCS) 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 USPS Large Private Branch Exchange (PBX) Telephone Systems throughout the country. IT has also refreshed many Key Telephone Systems at smaller USPS facilities throughout the country.

The USPS has not been assigned any specific NS/EP telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs, engineers and develops 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 and upgrades to the USPS Data Network in fiscal year (FY) 2006, the USPS 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 USPS 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 (VoIP) environment. Presently these systems are operating with conventional Digital Primary Rate Interface trunks for commercial and within network calling.

Internet Protocol (IP) Soft Phone Capabilities

The USPS is currently piloting Internet Protocol (IP) Soft Phone for Windows PC, teleworkers and road warriors have the flexibility to establish a virtual office anywhere and at any time. For employees who travel or who work from home, using the IP Soft Phone starts by connecting their Windows-based PC to the USPS network using a broadband connection. The employee's communication profile, including their extension, programmed line/feature keys and preferences settings, is then immediately available using the IP Soft Phone for Windows PC, no matter where they are located in the world. In addition, multiple employees can share the same PC when traveling, with access to their personalized settings when using the Soft Phone. Once connected to the corporate network, employees are able to address their voice communication needs as if they were at their corporate office. The IP Soft Phone for Windows PC and the employee's Nortel desktop IP Phone can ring concurrently, upon receipt of an incoming call or show as off-hook status when making an outbound call. This enhances employee flexibility and personal productivity while working from away from their office.

Key Telephone Systems

The USPS standard Key System is an Avaya. These systems are sized depending on the amount of handsets 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 through conventional telephone lines from the Local Exchange Carriers.

USPS has experimented with VoIP in a Key System environment. Due to funding issues in FY 2009 USPS has ceased the VoIP deployment as a Key System replacement technology.

PBX Security

All PBXs in the USPS have been configured to limit the amount of access local personnel have to make changes to the system. The PBXs are locked down to prohibit trunk-to-trunk transfers that can open the systems up to hackers. The PBXs are also monitored for unusual calling patterns that would indicate fraudulent or criminal activity.

All PBXs 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 PBXs so that proactive plans may be issued to advise employees and business partners of any outages or malfunctions.

NCS Directive 3-10

The USPS has several of the communications requirements as identified in NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, and has a budget and program plan that will enable USPS to move forward in implementing NCS Directive 3-10.

Wide Area Network Upgrades

Since the beginning of this fiscal year USPS has upgraded the telecommunications service at numerous 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.

All USPS facilities now have connections into the corporate data network in order to have email capabilities. They also have the abilities to provide data through intranet web-based informational faceplates. All functions from customer support to employee services are found through the USPS data network.

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-up and installing a managed Virtual Private

Network (VPN) firewall router at each location—thus protecting USPS computer assets from any malicious Internet activity

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 Statistics

- 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 five broadband providers into just two providers, thus simplifying troubleshooting and problem resolution.

Centralized Cellular Services Management

The USPS has centralized cellular services management in order to reduce costs, enhance reliability, improve accountability, and increase device security. This effort has resulted in $8 million in savings by eliminating unused devices and placing devices into a negotiated national minute pooling plan with the major cellular providers throughout the country. The average monthly recurring cost of cellular services has dropped by 30 percent during FY 2009. Providing Blackberry devices and Broadband Cellular technology to key employees within the management structure has allowed the online managers to react promptly to changes in the environment and staffing to meet critical goals and objectives. It also allows for the user to have access to data and to communicate with parties internally and externally for mission vital applications.

Local Dial Tone Management

The USPS has centralized local dial tone services at all facilities. This has increased accountability and has driven down costs on these services. An accurate inventory of all telephone lines and their costs per month is now available to management for review.

Contracts have been awarded geographically to assure the lowest cost possible for these services. This action has reduced USPS telephone line costs by 25 percent compared to FY 2008.

Spectrum Management Activities

The USPS manages its radio spectrum under the procedural guidelines and regulations from the National Telecommunications and Information Administration. The spectrum is managed centrally by the Spectrum Management Office (SMO), a unit of the Information Technology Group.

In FY 2009, the USPS began a program to increase spectrum technology efficiency by deploying spectrum efficient devices (SED) throughout the infrastructure. The SED employs IP Code Division Multiple Access technology that allows for the reduced requirement for spectrum while maintaining the same level of channelization configurations. This technology allows for communications to traverse the wide area network throughout the network in order for communications to be intra-facility in real time.

The transmissions are digital and can be encrypted to enhance security and privacy of communications. The devices are all compliant with military specifications and are fully software programmable.

Channel configurations are based on a commonality of services for maintenance, operations, safety, administration and law enforcement.

The SMO provides resolution for interference issues within the spectrum, both licensed and un-licensed. The expansion of part 15 devices within the processing facilities increases the need to mitigate interference within the processing centers and administrative offices.

GETS and WPS NCS Activities

The USPS has deployed GETS and WPS access to key personnel throughout the organization. Centralized management is through Information Technology. Access is tested monthly to maintain competency in using the service.

NCS-Related Acronyms

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

A

ACH	Automated Clearing House
AES	Advance Encryption Standard
AFT	Assured File Transfer
ANSI	American National Standards Institute
ARP	Allocation-Retention-Priority
ARRA	American Recovery and Reinvestment Act
ART	Analysis Response Team
ASD	Assistant Secretary of Defense
ATFE	Alcohol, Tobacco, Firearms and Explosives
ATG	Advanced Technology Group
ATIS	Alliance for Telecommunication Industry Solutions

B

BCEP	Business Continuity and Emergency Preparedness
BCIS	Bureau of Citizenship and Immigration Services
BLADE	Biometrics for Logical Access Development and Execution Program
BIMC	Beltsville Information Management Center

C

C4	Command, Control, Communications, and Computer Systems Directorate
C&A	Certification and Accreditation
CA	Certification Authority
CATF	Core Assurance Task Force
CBP	Customs and Border Protection
CCA	Continuity Communications Architecture
CCMG	COOP Communications Managers Group
CCTF	Cybersecurity Collaboration Task Force
CDEP	Communications Dependency on Electric Power
CDEP WG	Communications Dependency on Electric Power Working Group
CDMA	Code Division Multiple Access
CDR	Critical Design Reviews
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
CLONES	Central Location On-line Entry System
CLS	Continuous Linked Settlement
CMAS	Cellular Mobile Alert Service
CMN	Crisis Management Network
CMRS	Commercial Mobile Radio Service
CMS	Crisis Management System
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CNAT	Communications Network Analysis Tool
CNCI	Comprehensive National Cyber Initiative
CNSS	Committee on National Security Systems
CNSSP	Committee on National Security Systems Policy
COCOM	Combatant Commanders
COG	Continuity of Government
COMM ISAC	Communications Information Sharing and Analysis Center
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
COTS	Commercial Off-The-Shelf
CP	Contingency Planning
CS	Civil Support
CS&C	Cybersecurity and Communications
CSCC	Communications Sector Coordinating Council
CSMC	Cyber Security Management Center
CSSP	Communications Sector-Specific Plan
CUP	COMSEC Utility Program
CWIN	Critical Warning Infrastructure Network
CY	Calendar Year

D

DCIN-TS	Distributed Continuity Integrated Network-Top Secret
DEC	Disaster Emergency Communications
DES	Data Encryption Standard

DHS	Department of Homeland Security
DHHS	Department of Health and Human Services
DIB	Defense Industrial Base
DICE	Department of Defense Interoperability Communications Exercise
DIRS	Disaster Information Reporting System
DISA	Defense Information Systems Agency
DNLCC	Defense and National Leadership Command Capabilities
DOC	Department of Commerce
DOD	Department of Defense
DOD	Disaster Operations Directorate (Section IV-FEMA)
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DR	Disaster Recovery
DRH	Directed Retry Handover
DRSN	Defense Red Switch Network
DS	Diplomatic Security
DSS	Diplomatic Security Service
DTS	Digital Telecommunications Switching System

E

E911	Enhanced 9-1-1
EBS	Emergency Broadcast System
EKMS	Electronic Key Management System
EH09	Eagle Horizon 2009
EMC	Emergency Management Centers
EMIT	Email Inspection Tool
EMP	Electromagnetic Pulse
E.O.	Executive Order
EOC	Emergency Operations Center
EOP	Executive Office of the President
EPS	Evolved Packet System
ERG	Emergency Response Group
ESF #2	Emergency Support Function 2-Communications
ESM	Enterprise Security Management
ETS	Emergency Telecommunications System

F

FAS	Federal Acquisition Service
FBCA	Federal Bridge Certificate Authority
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FECC	Federal Emergency Communications Coordinator
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
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
FY	Fiscal Year
FY HSP	Future Year Homeland Security Planning

G

GAO	Government Accountability Office
GCC	Government Coordinating Council
GCS	Global Communications Service
GETS	Government Emergency Telecommunications Service
GIG	Global Information Grid
GIP&M	Government-Industry Planning and Management Branch
GIRTF	Global Infrastructure Resiliency Task Force
GIS	Geographical Information System
GITM	Global IT Modernization
GMI	Global MSF Interoperability
GNOC	Global Network Operations Center
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act
GSA	General Services Administration
GSM	Global System for Mobile Communications
GSOC	Government Security Operations Center

H

HAIPE IS	High Assurance Internet Protocol Encryptor Interoperability Specification
HCHB	Herbert C. Hoover Building
HD	Homeland Defense
HD&ASA	Homeland Defense and Americas' Security Affairs
HF	High Frequency

HHS	U.S. Department of Health and Human Services
HPC	High Probability of Completion
HPM	High Power Microwave
H.R.	House of Representatives Resolution
HSDN	Homeland Security Data Network
HSPD	Homeland Security Presidential Directive
HYSPLIT	Hybrid Single-Particle Langranqian Integrated Trajectory System

I

IA	Information Assurance
IAT	Internal Analysis Tool
IC	Intelligence Community
ICWG	International Communications Working Group
ID	Identification
IdITF	Identity Issues Task Force
IEEE	Institute of Electrical and Electronics Engineers
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMA	Individual Mobilization Augmentee
IMS	IP Multimedia Subsystem
IMT	Infrastructure Mapping Tool
INE	Inline Network Encryption
IOS	Interoperability Specification
IP	Internet Protocol
IPL	Internet Protocol Locator
IR	Industry Requirements
IRAC	Interdepartment Radio Advisory Committee
IRM	Bureau of Information Resource Management
IRS-CI	Internal Revenue Service-Criminal Investigation
ISDN	Integrated Services Digital Network
ISP	Internet Service Providers
IT	Information Technology
ITS	Integrated Technology Services
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
IWN	Integrated Wireless Network

J

JCC	Joint Collaboration Center
JCCC	Joint Command, Control, Communications & Computers Coordination Center
JCCSE	Joint CONUS Communications Support Environment
JFO	Joint Field Office
JIEE	Joint Information Exchange Environment
JISCC	Joint Incident Site Communications Capability
JMD	Justice Management Division
JSOC	Justice Security Operations Center
JTF-GNO	Joint Task Force-Global Network Operations
JTRB	Joint Telecommunications Resource Board
JUTNet	Justice Unified Telecommunications Network
JWICS	Joint Worldwide Intelligence Communications System

K

Kbps	Kilobit per second
KMI	Key Management Infrastructure

L

LAN	Local Area Network
LANL	Los Alamos National Laboratory
LMR	Land Mobile Radio
LRTF	Legislative and Regulatory Task Force
LTE	Long-Term Evolution
LTO	Long-Term Outage

M

MACC	Multi-Agency Communications Center
MAD	Missions Assurance Division
MEF	Mission Essential Functions
MERS	Mobile Emergency Response Support
MHD	Magneto hydro dynamics
MHz	Megahertz
MMS	Multimedia Message Service
MOBEX	Mobile Operations Exercise
MPS	Multi-media Priority Service
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
NAT	Network Discovery Tool
NCC	National Coordinating Center
NCP	National Continuity Policy
NCS	National Communications System
NCSD	National Cyber Security Division
NCSMO	National Cryptographic Solutions Management Office
NCSRM	National Communications System Regional Manager
NCUA	National Credit Union Administration
NDAC	Network Design and Analysis Capability
NEA	Near East Asia
NECP	National Emergency Communications Plan
NEF	National Essential Functions
NEN	Near Earth Network
NGN	Next Generation Network
NGN IAWG	NGN Implementation Annex Working Group
NIARL	National Information Assurance Research Laboratory
NIFC	National Interagency Fire Center
NII	Networks and Information Integration
NIIF	Network Interconnection Interoperability Forum
NIST	National Institute of Standards and Technology
NLE	National Level Exercise
NOAA	National Oceanic and Atmospheric Administration
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
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSPD	National Security Presidential Directive
NSS	National Security Systems
NSSE	National Special Security Event
NSSO	National Security Space Office
NSTAC	The President's National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration

O

OA	Operating Administrations (Section IV)
OA	Operational Analysis
OASD	Office of the Assistant Secretary of Defense
OCC	Office of Comptroller of Currency
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OEC	Office of Emergency Communications
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OSD	Office of the Secretary of Defense
OSM	Office of Spectrum Management
OSTP	Office of Science and Technology Policy
OTS	Office of Thrift Supervision

P

P25	Project 25
PAS	Priority Access Service
PBX	Private Branch Exchange
PCC	Policy and Charging Control
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMEF	Priority Mission Essential Functions
PMP	Privilege Management Pilot
PN	Public Network
PNT	Positioning Navigation and Timing
PPBE	Planning, Programming, and Budgeting Execution System
POP	Point of Presence
PSN	Public Switched Networks
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
RCC-WG	Regional Communications Coordinator Working Group

RDD TTX	Radiological Dispersion Device Table Top Exercise
RDM	Route Diversity Methodology
RDTF	Research and Development Task Force
RDX	Research and Development Exchange
RECCWG	Regional Emergency Communication Coordination Working Group
RFC	Request for Comments
RFI	Request for Information
RFP	Request for Proposal
RPH	Resource Priority Header
RRAP	Regional Resilience Assessment Program
RRS	Readiness Reporting System
RSVP	Resource Reservation Protocol

S

SATCOM	Satellite Communications
SAVER	Secure AntiVirus Equipment Refresh
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SCIP	Statewide Communications Interoperability Plan
SEC	Security and Exchange Commission
SECDEF	Secretary of Defense
SED	Spectrum Efficient Devices
SHARES	Shared Resources
SHARES-HF	Shared Resources High Frequency Radio Program
SLA	Service Level Agreements
SMART	State Messaging Archive Retrieval Toolset
SME	Subject Matter Experts
SME-PED	Secure Mobile Environment-Portable Electronic Device
SOC	Security Operations Center
SOP	Standard Operating Procedures
SA	Situational Awareness
SIAO	Senior Information Assurance Officer
SIPRNet	Secret Internet Protocol Router Network
SITREP	Situation Report
SMEX	ScanMail for Microsoft Exchange
SMO	Spectrum Management Office
SMS	Short Message Service
SP	Special Publication
SPWG	Service Provider Working Group
SRS	Savannah River Site
SSA	Social Security Administration (Section IV)
SSA	Sector Specific Agency (Section III)
SSP	Sector Specific Plan (Section III)
SSP	System Security Plans (Section IV)
SSP	Shared Service Provider (Section IV-TREAS)
STE	Secure Terminal Equipment
STF	Satellite Task Force
SVDC	Secure Video and Data Collaboration
SVP-COI	Secure Voice Products Community of Interest
SVTC	Secure Video Teleconferencing

T

T&E	Training and Exercise
TADAC	Technology Assessment and Data Analysis Cell
TAN	Technology Assessment Network
TCA	Transformational Communications Architecture
TCS	Treasury Communications System
TD	Technology Directorate
TEDE	Telecommunications Electromagnetic Disruptive Effects
TEPI	Telecommunications and Electric Power Interdependencies
TEWI	Treasury Early Warning and Indicators
TIA	Telecommunications Industry Association
TIC	Trusted Internet Connection
TSC	Telecommunications Service Center
TSP	Telecommunications Service Priority
TSP OC	TSP Oversight Committee
TSS	Technical Security and Safeguards

U

US-CERT	U.S. Computer Emergency Readiness Team
USGS	U.S. Geological Survey
UMTS	Universal Mobile Telecommunications System
USA	United States Attorneys
USACE	US Army Corps of Engineers
USDA	U.S. Department of Agriculture
USPS	U.S. Postal Service
USSS	United States Secret Service

V

VA	Department of Veterans Affairs
VANTS	VA Nationwide Teleconferencing System
VHF/FM	Very High Frequency/Frequency Modulation
VoIP	Voice over Internet Protocol

VoSIP	Voice over Secure Internet Protocol
VPN	Virtual Private Network
VPO	Video Program Office
VSAT	Very Small Aperture Terminal

W

WARN	Warning, Alert, and Response Network Act
WiMax	Worldwide Interoperability for Microwave Access
WPO	Wireless Program Office
WPS	Wireless Priority Service
WS	Wireless Services Branch
WTC	World Trade Center

X

XTE	eXperimental Testbed Environment

National Communications System
Department of Homeland Security

245 Murray Lane
Mailstop 0615
Washington, DC 20598-0615

www.ncs.gov
ncsweb1@dhs.gov

National
Communications
System