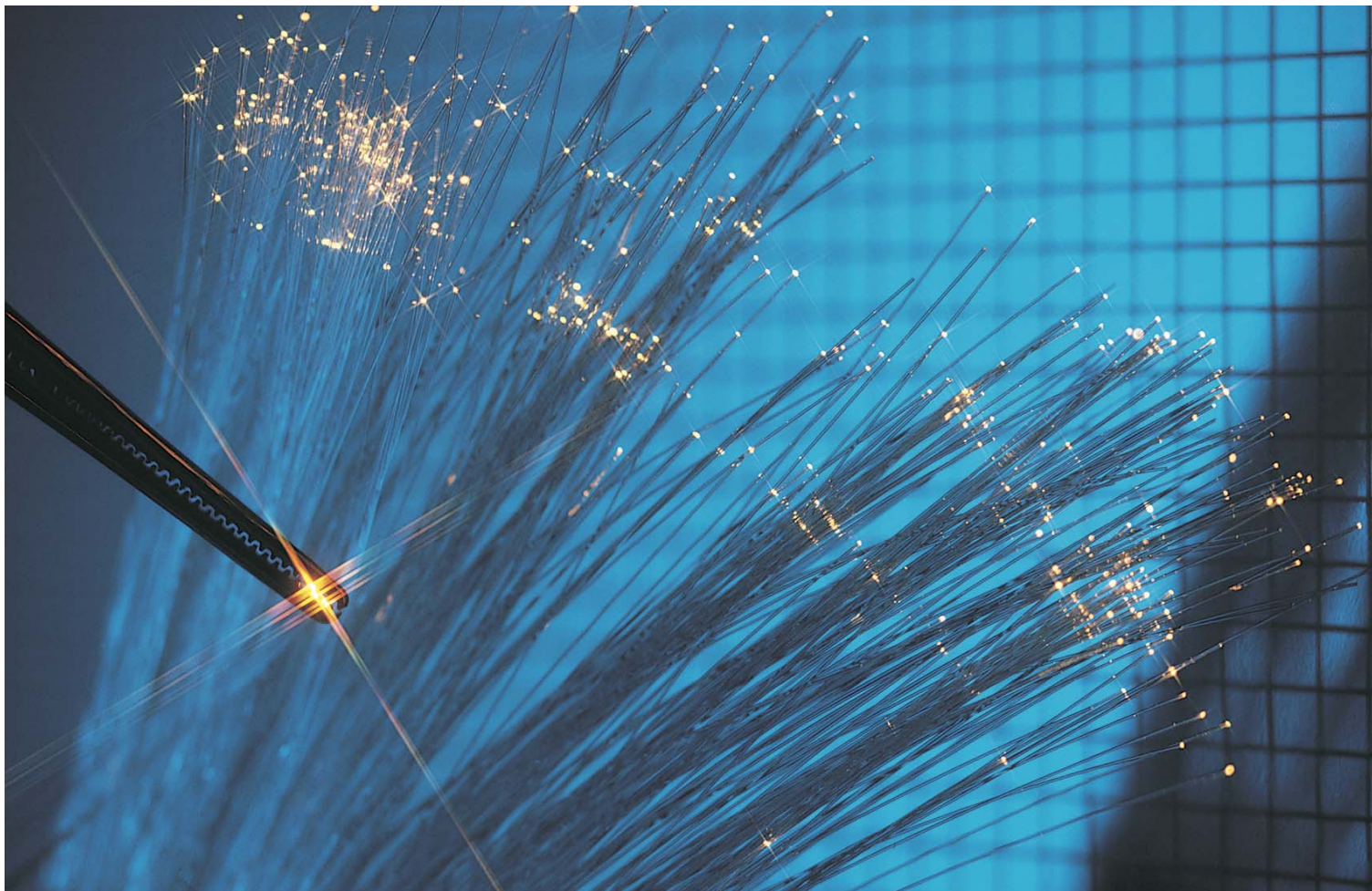


ANNUAL REPORT 2005



National
Communications
System





NATIONAL COMMUNICATIONS SYSTEM

Ensuring Essential
Communications for the
Homeland

Prepared by the Office of the Manager,
National Communications System

FOREWORD

The impact of Hurricane Katrina reminded the Nation of the critical role that telecommunications services play in response and recovery activities following catastrophic events. The value of the National Communications System's (NCS) emergency response programs was clearly highlighted in the aftermath of this devastating storm, which forced Government officials and first responders in the affected areas and across the Nation to mount one of the largest natural disaster recovery efforts in United States history. The mission of the NCS, as stated in Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, is to advise and assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in the planning for and provisioning of national security and emergency preparedness (NS/EP) communications under all circumstances. E.O. 12472 also orders the support and cooperation of 23 other Federal departments and agencies.

Hurricane Katrina also highlighted the NCS' role in Emergency Support Function #2 (ESF-2) as directed under the National Response Plan. The NCS—as the primary agency for ESF-2—coordinates Federal measures to ensure that NS/EP telecommunications are able to support the Federal, State, and local disaster response elements. Specifically, in the event of a Federal disaster, the NCS' National Coordinating Center (NCC), acts as a point of coordination and information sharing for communications infrastructure operators. Additionally, the NCC assists the Federal Government and industry partners in assessing damage, identifying and prioritizing communication requirements, monitoring the situation and response, developing status reports, and coordinating the provisioning and restoration of equipment and services.

The NCS coordinated the delivery of critical mobile communication vans and satellite phones, as well as wireless phones programmed for

Wireless Priority Service (WPS) to State and local government leaders and first responders, during Katrina response efforts. These efforts ensured the continuity of essential communications in areas where the local telecommunications companies were unable to respond due to widespread power outages, heavily damaged equipment and facilities, and destruction of the underlying telecommunications infrastructure itself. The NCS continued to provide much needed support immediately following Hurricane Rita, which caused further damage to the infrastructure across the Gulf Coast.

The NCS also experienced considerable leadership and organizational changes during Fiscal Year 2005. Judge Michael Chertoff was sworn in as the second Secretary of the Department of Homeland Security (DHS) on February 15, 2005; on April 11, 2005, I assumed the roles of Acting Undersecretary for Information Analysis and Infrastructure Protection, Assistant Secretary for Infrastructure Protection, and NCS Manager; and Dr. Peter Fonash was formally named the Deputy Manager of the NCS on April 21, 2005.

In July 2005, Secretary Chertoff announced his Six-Point Agenda for transforming the DHS organizational structure to better meet its various missions, reflecting conclusions drawn from the Second Stage Review—a study of the Department's programs, policies, operations, and structure. This review process led to transformational changes within the Department, one of which was the formal creation of a new Office of Cyber Security and Telecommunications to encompass both the NCS and the National Cyber Security Division.

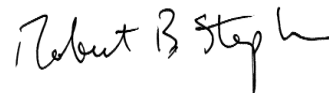
Furthermore, the NCS continued to lead by example through its proven operational programs and technologies; the organization's partnerships with industry and Government entities, including the President's National Security Telecommunications Advisory Committee (NSTAC), the NCS Committee of Principals (COP) and the Council of

Representatives (COR); and its knowledge of NS/EP policy to ensure the reliability and availability of NS/EP communications in a variety of activities over the course of the fiscal year. The NCS also leverages unique industry and Government partnerships through the NCC, the Communications Information Sharing and Analysis Center (ISAC), and the Network Security Information Exchanges (NSIE). These forums promote the sharing of information between NCC companies and the Government by providing a forum to discuss issues such as threats and vulnerabilities.

The NCS utilized its extensive knowledge of telecommunications policy by playing a central role in the Government's efforts to implement Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*. As the telecommunications sector specific agency, the Office of the Manager, NCS and its industry partners drafted the National Infrastructure Protection Plan's (NIPP) Telecommunications Sector Specific Plan. The NCS also serves as the lead agency for guiding the activities of the Telecommunications Government Coordinating Council (TGCC). Furthermore, in its capacity as the Sector Specific Agency (SSA) for telecommunications, the NCS has reached out to other SSAs to identify and address infrastructure interdependencies, and is also working closely within the sector to establish the Communications Sector Coordinating Council (CommSCC), the industry counterpart of the TGCC. The NCS, in support to DHS participation in the Committee on Foreign Investments in the United States, leveraged its knowledge on security issues related to foreign acquisitions and mergers in the communications field to evaluate telecommunications related foreign ownership issues, including undertaking an analysis of the vulnerabilities associated with foreign investment in various components of the satellite industry. In addition, the NCS worked to advance its

operational programs through the enhancement of its WPS program and the implementation of additional upgrades for Government Emergency Telecommunications Service (GETS) features throughout the public switched telephone network. These improvements will ensure reliable communication among senior leaders of industry and Government in times of crisis and network congestion. Furthermore, the NCS continued to evaluate the need for contingency communications among Federal agencies through resiliency efforts such as Route Diversity.

The devastation caused by Hurricane Katrina illustrates that the mission of the NCS remains as vital today as it has been over the past four decades. During the challenges that lay ahead, the NCS will remain committed to coordinating and ensuring essential communications for the Federal Government under all conditions. By continuing to strengthen our industry and Government partnerships, the NCS will continue to develop strategic solutions to ensure that NS/EP communications needs of all stakeholders are met.



Robert B. Stephan
Manager, NCS



NCS LEADERSHIP



Mr. Robert Stephan
Manager



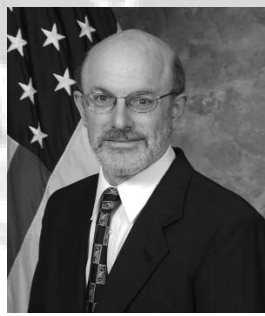
Dr. Peter A. Fonash
**Deputy Manager and
Director**



Col. Victoria Velez, USAF
Chief of Staff



Mr. Gary Amato
**Chief
Technology and
Programs Division**



Mr. Jeffrey Glick
**Chief
Critical Infrastructure
Protection Division**



Mr. James Bittner
**Chief
Plans and
Resources Division**



Mr. Thomas J. Falvey
**Chief
Customer Service
Division**

NCS COMMITTEE OF PRINCIPALS



Department of State
(DOS)
MR. BRUCE MORRISON



Department of the Treasury
(TREAS)
MS. VICKI WAIZENEGGER



Department of Defense
(DOD)
DR. LINTON WELLS



Department of Justice
(DOJ)
MS. KAREN BEARD



Department of the Interior
(DOI)
MR. W. HORD TIPTON



Department of Agriculture
(USDA)
MS. JANICE LILJA



Department of Commerce
(DOC)
MS. KAREN F. HOGAN



Department of Health
and Human Services
(HHS)
MR. ROBERT BLITZER



Department of
Transportation (DOT)
MR. EUGENE K. TAYLOR, JR.



Department of Energy
(DOE)
MR. HARRY HIXON



Department of Veterans
Affairs (VA)
MR. EDWARD F. MEAGHER



Department of Homeland
Security (DHS)
MR. STEVEN COOPER



Federal Emergency
Management Agency
(FEMA)
MR. BARRY WEST



The Joint Staff (JS)
LT. GEN. ROBERT SHEA,
USMC



General Services
Administration (GSA)
MS. SANDRA N. BATES



National Aeronautics
and Space
Administration
(NASA)
MR. ROBERT E. SPEARING



Nuclear Regulatory
Commission (NRC)
MR. RICHARD WESSMAN



National
Telecommunications
and Information
Administration (NTIA)
MR. FREDERICK R. WENTLAND



National Security Agency
(NSA)
MR. MORRIS HYMES



United States Postal
Service (USPS)
MR. PETER MYO KHIN



Federal Reserve Board
(FRB)
MR. KENNETH D. BUCKLEY



Federal Communications
Commission (FCC)
MR. JEFFREY M. GOLDTHROP

NCS COUNCIL OF REPRESENTATIVES



Department of State
(DOS)
Ms. KIMBERLY A. GODWIN



Department of the Treasury
(TREAS)
Ms. VICKI WAIZENEGGER



Department of Defense
(DOD)
COL. RANDALL CONWAY,
USA



Department of Justice
(DOJ)
Mr. GARY W. LAWS



Department of the Interior
(DOI)
Mr. TIMOTHY QUINN



Department of Agriculture
(USDA)
Mr. ROY ALLUMS



Department of Commerce
(DOC)
Mr. BENJAMIN CHISOLM



Department of Health and
Human Services (HHS)
Mr. ROBERT LAVENDER



Department of
Transportation (DOT)
Mr. MICHAEL DAMMEYER



Department of Energy
(DOE)
Mr. HARRY HIXON



Department of
Veterans Affairs (VA)
Mr. DAVID CHEPLICK



Department of
Homeland Security
(DHS)
Mr. JULIO MURPHY



Federal Emergency
Management Agency
(FEMA)
Mr. BARRY WEST



The Joint Staff (JS)
COL ROBERT GEARHART,
USMC



General Services
Administration (GSA)
Mr. THOMAS E. SELLERS



National Aeronautics and
Space Administration
(NASA)
Mr. JOHN C. RODGERS



Nuclear Regulatory
Commission (NRC)
Mr. THOMAS M. KARDARAS



National Telecommunications
and Information
Administration (NTIA)
Mr. WILLIAM A. BELOTE



National Security
Agency (NSA)
Ms. CAROL HIGGINS



United States Postal
Service (USPS)
Mr. WARREN SCHWARTZ

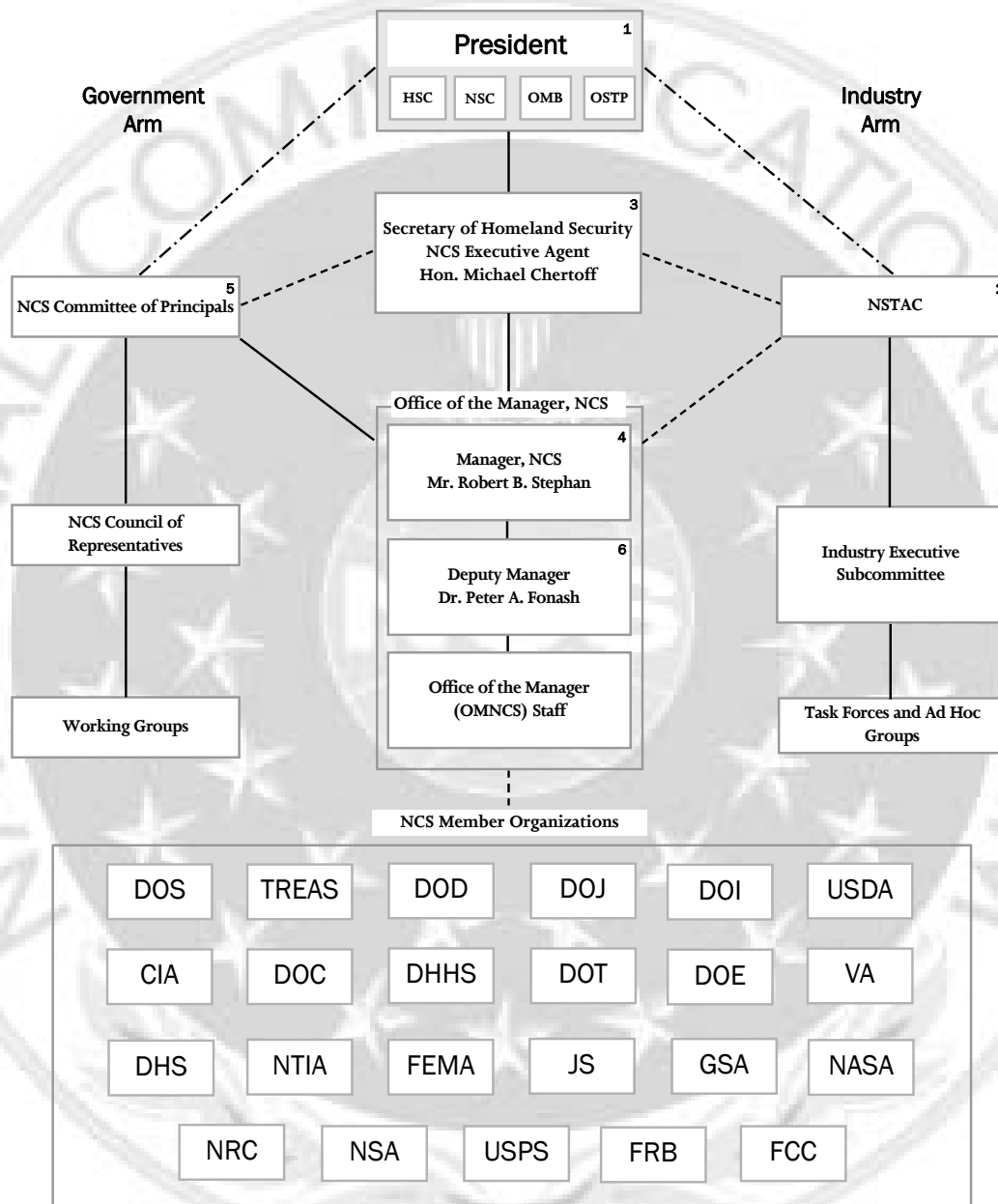


Federal Reserve Board
(FRB)
Ms. ANNE E. PAULIN



Federal Communications
Commission (FCC)
Mr. KENNETH P. MORAN

THE NCS STRUCTURE



1. Policy Direction and Direct Execution of War Powers Function
2. The President's National Security Telecommunications Advisory Committee created by Executive Order 12382
3. Executive Agent, NCS responsibilities assigned to Secretary of Homeland Security by E.O. 13286, February 28, 2003
4. Assistant Secretary for Infrastructure Protection, serves as Manager, NCS
5. The Key Telecommunications Officers of the NCS Member Organizations
6. First-line management position that is exclusively NCS

Legend

- Direction —————
- Coordination - - - - -
- Advice - . - . - .

TABLE OF CONTENTS

	Page Number		Page Number
I. INTRODUCTION/HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM			
Background	I-2	Department of Energy (DOE)	IV-23
NCS Environment: The Evolving Homeland Security Landscape	I-3	Department of Veterans Affairs (VA)	IV-24
<hr/> <hr/>			
II. EMERGENCY RESPONSE ACTIVITIES			
Hurricane Response 2004	II-3	Department of Homeland Security (DHS)	IV-25
Hurricane Response 2005	II-4	Central Intelligence Agency (CIA)	IV-28
London Terrorist Attacks	II-8	Federal Emergency Management Agency (FEMA)	IV-29
Preparedness Exercises	II-8	The Joint Staff (JS)	IV-30
<hr/> <hr/>			
III. NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS			
Technology and Programs Division	III-7	General Services Administration (GSA)	IV-31
Critical Infrastructure Protection Division	III-21	National Aeronautics and Space Administration (NASA)	IV-33
Plans and Resources Division	III-38	Nuclear Regulatory Commission (NRC)	IV-34
Customer Service Division	III-39	National Telecommunications and Information Administration (NTIA)	IV-35
<hr/> <hr/>			
IV. NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS			
Department of State (DOS)	IV-2	National Security Agency (NSA)	IV-37
Department of the Treasury (TREAS)	IV-7	U.S. Postal Service (USPS)	IV-41
Department of Defense (DOD)	IV-13	Federal Reserve Board (FRB)	IV-44
Department of Justice (DOJ)	IV-15	Federal Communications Commission (FCC)	IV-46
Department of the Interior (DOI)	IV-16	<hr/> <hr/>	
U.S. Department of Agriculture (USDA)	IV-17	A. NCS RELATED ACRONYMS	
Department of Commerce (DOC)	IV-19		
Department of Health and Human Services (HHS)	IV-20		
Department of Transportation (DOT)	IV-21		



I

INTRODUCTION:

THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

SECTION I

INTRODUCTION: THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

BACKGROUND

This report, prepared by the Office of the Manager, National Communications System (NCS), details national security and emergency preparedness (NS/EP) activities and telecommunications events, and highlights the agency's innovations, programs, and achievements during fiscal year (FY) 2005.

On August 21, 1963, President John F. Kennedy signed a Presidential Memorandum ordering the formation of the NCS in the wake of communications shortfalls in support of national security decision making during the 1962 Cuban Missile Crisis. During critical periods of the crisis, the United States (U.S.) Government encountered tremendous difficulty in establishing and maintaining communications with key parties. A study conducted by the National Security Council (NSC) in the wake of the crisis determined that a consolidated system to support critical Government communications functions should be created, resulting in the formation of the NCS. The original mission of the NCS was to:



“provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies, and international crises, including nuclear attack.”

Over the years, the role of telecommunications in supporting the Nation's NS/EP functions expanded. By the late 1970s, Government policy formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and recovery in the face of a nuclear attack from the Soviet Union. The expanded role of telecommunications was also evident in light of the growing complexity of Government, the rapid growth in telecommunications technologies and services, and the importance of telecommunications in responding to manmade and natural disasters.

On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which revitalized and expanded the NCS. The NCS mission, as defined by E.O. 12472, is to assist the President; the NSC; the Director, Office of

Science and Technology Policy; and the Director, Office of Management and Budget in the exercise of wartime and non-wartime emergency telecommunications responsibilities, and to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

Following the September 11, 2001, terrorist attacks, President George W. Bush issued E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, on October 8, 2001, and E.O. 13231, *Critical Infrastructure Protection*, on October 16, 2001.

E.O. 13228 established the White House Office of Homeland Security (OHS) and tasked it to coordinate protection efforts for critical public and privately owned information systems within the U.S. The OHS was also authorized to coordinate efforts to ensure the rapid restoration of telecommunications and critical information systems after disruption by a terrorist threat or attack. In addition, E.O. 13231 established the President's Critical Infrastructure Protection (CIP) Board and established the NCS Committee of Principals (COP) as a permanent standing committee. This E.O. also reiterated the reporting functions and responsibilities established in E.O. 12472.

On November 25, 2002, President Bush signed into law the *Homeland Security Act of 2002*, which established the Department of Homeland Security (DHS) and initiated a major reorganization of Government departments and agencies with homeland security missions. As part of the reorganization plan, the NCS and its NS/EP programs were designated for transfer to the new Department's Information Analysis and Infrastructure Protection (IAIP) Directorate.

On February 28, 2003, the President signed omnibus E.O. 13286, *Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, which transferred the NCS executive agent from the Department of Defense (DOD) to DHS. The NCS officially became a part of DHS on March 1, 2003.

NCS ENVIRONMENT — THE EVOLVING HOMELAND SECURITY LANDSCAPE

On August 29, 2005, Hurricane Katrina made landfall near New Orleans, Louisiana, causing massive damage and flooding in Louisiana, Mississippi, and Alabama. Among the catastrophic damage caused by Katrina, communications in the areas hardest hit were seriously affected, resulting in the largest national response to any natural disaster in U.S. history. During the response and recovery stages of the emergency, the NCS served as a hub between the private sector and the Government for communications, coordinating the arrival of mobile communications vans, and arranging for delivery of satellite phones, as well as wireless phones programmed for Wireless Priority Service for State and local Government officials and emergency responders. The NCS also coordinated delivery of equipment from telecommunications companies and arranged for the distribution of fuel for generators to keep the communications infrastructure operational.

The response and recovery efforts related to Hurricane Katrina brought to light several issues which will continue to alter the NS/EP communications landscape. Namely, the *Posse Comitatus Act* (18 USC 1385). The act limits the role of military in homeland defense and the function of the military in natural disaster response. Concerns arose that the Act impeded access to needed assets and that those resources had responsibilities that should be revisited and could be used in the future to augment the NCS' role during major catastrophes. Furthermore, during Hurricane Katrina, response and recovery were not only hampered by the flooding and debris left by the storm, but also by concern for the safety of recovery teams. Reports of looting and violence in New Orleans, which resulted in the mobilization of National Guard and Federal troops, created apprehension among the private industry officials who requested security escorts to parts of the cities where telecommunications facilities were in need of repair.

In addition, although DHS announced the completion of the National Response Plan (NRP) in January 2005, response and recovery efforts for Hurricane Katrina raised questions regarding the need for further clarification in the NRP as to when the Federal Government should intervene in emergency response efforts. The NRP replaces the initial National Response Plan, the Federal Response Plan, the U.S. Government Interagency Domestic Terrorism Concept of Operations Plan, and the Federal Radiological Emergency Response Plan. The development of the NRP was directed by Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, which directs the Secretary of Homeland Security to enhance the ability of the U.S. to prepare for and manage domestic incidents by establishing a single,

comprehensive, national approach. The issue of long-term loss of power and fuel for generators also came to the forefront in the aftermath of Katrina. While the NCS was able to coordinate the dissemination of generators and fuel, the need for plans and policies to assist with challenges in the provisioning of these assets is an issue that will be explored in the future. Specifically, the President's National Security Telecommunications Advisory Committee continues to address this interdependency through its Telecommunications and Electric Power Interdependency Task Force. The NCS and the National Coordinating Center, are also examining the use of resources during response and recovery efforts to ensure that all necessary resources are available to be utilized in a similar event, and also to identify any resources that the Federal Government could supply to assist the private industry in restoration.

In addition to the changes Hurricane Katrina wrought on the NS/EP environment, the NCS also experienced significant leadership and organizational change during FY 2005. Judge Michael Chertoff was sworn in as the second Secretary of DHS on February 15, 2005; Mr. Robert Stephan assumed the roles of Acting Undersecretary for IAIP, Assistant Secretary for Infrastructure Protection, and NCS Manager on April 11, 2005; and Dr. Peter A. Fonash was formally named the Deputy Manager of the NCS on April 21, 2005. In July 2005, Secretary Chertoff announced his Six-Point Agenda for transforming the DHS organizational structure to better suit its numerous missions, reflecting conclusions drawn from the Second Stage Review, an examination of the Department's programs, policies, operations, and structure. Under the realignment, the NCS will operate within the Office of Cyber Security and

Telecommunications, under the joint auspices of the new Assistant Secretary for Cyber Security and Telecommunications and the new Under Secretary for Preparedness. The new Assistant Secretary position was created in an effort to centralize the coordination of efforts to protect the communications infrastructure.

The proposed Office of Cyber Security and Telecommunications will have two primary responsibilities, cyber and telecommunications. The cyber security component will be responsible for collecting, analyzing, and coordinating access to information related to potential cyber terrorist threats, and will coordinate Department-wide activities on cyber threats. The telecommunications component will provide support to the communications infrastructure to meet mission-critical NS/EP communications needs for Federal, State, and local Governments, as well as private industry.

The combination of the communications and cyber sectors within the Office of Cyber Security and Telecommunications will allow the NCS to continue to interface with key stakeholders within its sector and among other sectors by addressing interdependencies that exist. The NCS has already developed a close partnership with the National Cyber Security Division in an effort to coordinate the operation of cyber-based programs. Also, as part of the National Infrastructure Protection Plan, the NCS is conducting outreach efforts to other sectors to identify and address infrastructure interdependencies.

While the landscape of NS/EP communications and preparedness continues to evolve, the NCS will continue to work through its existing and emerging partnerships to meet challenges associated with the changing policy, technology, and threat environments. The NCS remains committed to providing stakeholders and the Nation with proactive solutions to meet current and future homeland security communications demands.



II

EMERGENCY RESPONSE ACTIVITIES

SECTION II

EMERGENCY RESPONSE ACTIVITIES

The National Communications System (NCS) ensures that Federal, State, and local responders receive national security and emergency preparedness (NS/EP) communications support during national disasters. Over the past 42 years, the NCS has provided assistance to these responders following hurricanes, wild fires, ice storms, earthquakes, and various other national disasters, including the terrorist attacks of September 11, 2001.

The mission and day-to-day operations of the NCS ensure it is continually focused on maintaining communications in an emergency. The Emergency Support Function #2 (ESF-2) Annex to the National Response Plan ensures the provision of Federal communications support to Federal, State, local, tribal, and private sector response efforts during an incident. As stated in the ESF-2 Annex, the Office of Science and Technology Policy delegates the primary agency functional responsibility for ESF-2 to the NCS. When ESF-2 is activated, the NCS is responsible for coordinating emergency communications solutions and restoring permanent communications in the event of a natural disaster.

The NCS works in coordination with all ESF-2 supporting agencies and private sector partners in emergency response events when ESF-2 is invoked.

Executive Order 12472 grants the NCS the authority to leverage its collective Government and communications sector knowledge, experience, and trusted relationships to support quick and effective emergency response within the NCS organizational structure. In this role, the NCS can draw on and deploy communications resources, particularly assets of its industry membership, to help ensure communications during a crisis.

During Fiscal Year (FY) 2005, the NCS utilized its extensive emergency response experience, as well as its successful priority services programs, to provide response and recovery support for the communications infrastructure during a number of incidents and activities. The NCS began and concluded FY 2005 by executing its ESF-2 responsibilities in support of the 2004 and 2005 hurricane seasons. The NCS' National Coordinating Center (NCC) maintained a high-alert posture and monitored, analyzed, and assessed approaching storms, including Hurricanes Charley, Frances, Ivan, and Jeanne in 2004 and Hurricanes Katrina and Rita in 2005. The NCC actively tracked and communicated pre- and post-landfall response activities in coordination with ESF-2 partners, field office components, and its telecommunications industry partners. The NCC also established information sharing channels with communications service

providers, mitigated potential facility damage, and helped to reduce anticipated recovery times.

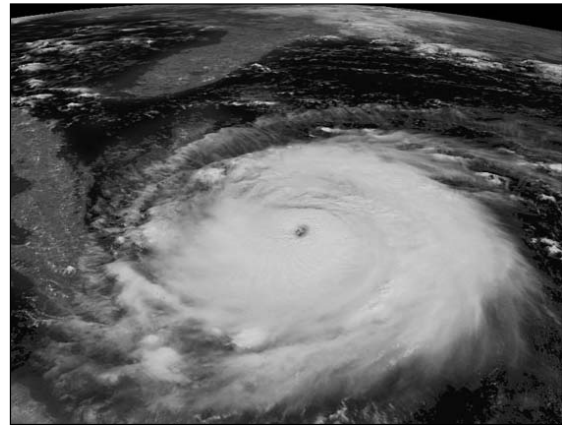
During FY 2005, the NCS continued to ensure that its NCC membership was aware of threats, vulnerabilities, switch outages, fiber cuts, power outages, and other incidents affecting the communications infrastructure. The NCC provided evaluation and analysis on multiple hardware and software vulnerabilities and exploits including Bagle, Skull B and Skull C Trojan, and Cabir Worm. In addition, the NCS analyzed communications issues brought to light by the London terrorist attacks and developed an emergency wireless protocol to coordinate requests for the disruption of cellular service. Finally, the NCS sought opportunities to test its preparedness and response capabilities in national-level exercises.

HURRICANE SEASON 2004

In August and September 2004, the Southeastern United States (U.S.) and the Gulf Coast were hit by a series of powerful, tropical storms and hurricanes. Hurricanes Charley, Frances, Ivan, and Jeanne hit Florida and parts of Alabama and Georgia in rapid succession. In addition, the effects of these successive storms impacted Puerto Rico, Mississippi, Tennessee, South Carolina, North Carolina, and Virginia. These storms and the associated flooding and high winds caused substantial property damage, power failures, and other utility problems. The storms caused repeated damage to the telecommunications infrastructure in some areas, leading to the interruption of services over the course of several weeks or even months. Hurricane emergencies requiring

the NCS to enact ESF-2 capabilities in 2005 include:

- Hurricane Charley struck the west coast of Florida during the late afternoon on August 13, 2004. The hurricane reached Category 4 strength, with winds of 145 mph when it made landfall at Port Charlotte, Florida.



- Hurricane Frances struck the east coast of Florida during the afternoon on September 4, 2004. The hurricane reached Category 3 strength with winds of 130 mph when recorded south of Melbourne, Florida. Frances was a slow-moving storm that produced major flooding in Florida and Georgia.
- Hurricane Ivan landed on the Gulf coast of Alabama in the early morning on September 16, 2004. The hurricane was rated as a Category 4 with winds of 135 mph when it struck southeast of Mobile, Alabama.
- Hurricane Jeanne struck the east coastline of Florida late at night on September 25, 2004. The hurricane

was rated as a Category 3 with winds of 130 mph when it hit at nearly the same point as Hurricane Frances, just south of Melbourne, Florida.

The procession of severe storms required activation of the full complement of NCC staffing resources. All three NCC Emergency Operations Teams were activated and a number of personnel supporting ESF-2 dispersed to the field. Industry representatives worked throughout the storms to provide status of communications and input on recovery operations, and highlight issues that could further impact recovery. The operations in support of the 2004 hurricane season marked a maturing of response activities across all levels. In particular, the operations chain functioned effectively with a greater focus on setting priorities, defining requirements, and solving problems originating in the field and escalating response levels as required through the chain from State to Federal representatives.

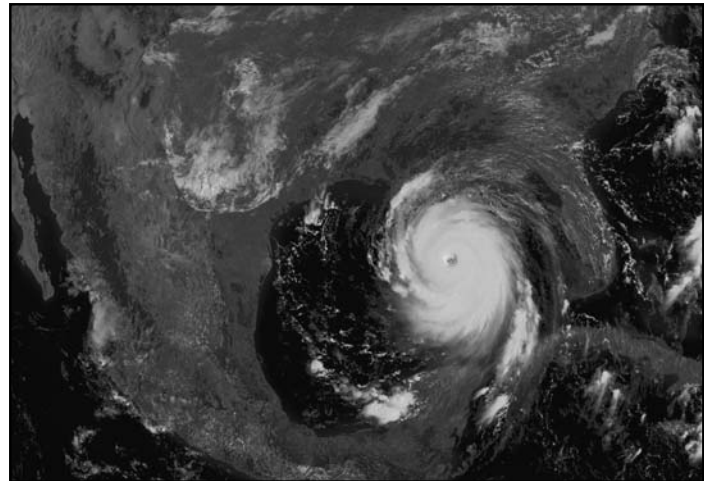
In addition to the NCS responsibilities in support of ESF-2, the NCC functioned as a central point of coordination and information sharing for communications infrastructure operators. While service providers relayed information through the NCC to the ESF-2 coordinators, the NCC platform also allowed for significant information sharing amongst service providers. The level and scope of information shared could not exist without the NCC as host and focus for industry exchange. NCC members imparted vital information about fuel resources, battery and remote power issues, customer impact, law enforcement, location access conditions, and provided a platform for the mutual aid function called into operation by service providers.

HURRICANE SEASON 2005

During August and September 2005, a series of powerful tropical storms and hurricanes struck the Southeastern U.S. and the Gulf Coast. Two storms—Hurricanes Katrina and Rita—resulted in significant problems for service providers and unprecedented damage to the communications infrastructure.

Hurricane Katrina

Hurricane Katrina first made landfall as a Category 1 hurricane on August 25, 2005, north of Miami, Florida, and then again on August 29, 2005, along the Central Gulf Coast near New Orleans, Louisiana, as a Category 4.



The storm surge breached the levee system that protected New Orleans from Lake Pontchartrain, subsequently flooding a majority of the city. This and other major damage to the coastal regions of Louisiana, Mississippi, and Alabama made Hurricane Katrina the most destructive and costly natural disaster in U.S. history. In addition, Hurricane Katrina caused a significant loss of life and displaced over one million people, resulting in a humanitarian crisis not seen in

the U.S. since the Great Depression. The Federal Government issued disaster declarations for parts of Louisiana, Mississippi, Alabama, and Florida, covering 90,000 square miles.

The NCS played a pivotal role in preparing for and responding to Hurricane Katrina by ensuring the provisioning and restoration of NS/EP communications services. Established NCS priority service programs proved extremely valuable during Hurricane Katrina. The NCS issued Telecommunications Service Priority (TSP) assignments, Government Emergency Telecommunications Service (GETS) cards, and Wireless Priority Service (WPS) procedures, and activated the Shared Resources (SHARES) High Frequency Radio Program. The NCS issued over 1,000 new GETS cards, while over 40,000 GETS calls were successfully completed during the recovery period. In addition, the NCS enabled over 4,000 cellular phones with the WPS capability and completed more than 1,500 TSP assignments. Restoration of these services supported key Federal, State, local and commercial activities; emergency response at all levels; hospitals; and the military.

The use of SHARES during Hurricane Katrina also proved to be an overwhelming success during the first few days of the response effort. The NCS coordinated participation by 431 SHARES stations, providing significant assistance in synchronizing efforts between Federal, State, and local Governments. During Hurricane Katrina, the SHARES program:

- Assisted local Governments and Federal entities with search and rescue missions for over 100 missing people in the affected area by

relaying critical information regarding those persons to the appropriate agencies;

- Communicated with the National Aeronautics and Space Administration's (NASA) Disaster Assistance and Rescue Teams and Communications Group, assisting them in their preparations for deployment to Stennis Space Center;
- Provided coordination of frequency assignments with the Department of Energy, the Federal Communications Commission (FCC), the Military Affiliate Radio System, the U.S. Navy, Federal Emergency Management Agency (FEMA), the Civil Air Patrol, the Amateur Radio Emergency Services /Radio Amateur Civil Emergency Service, and the States of Louisiana and Mississippi Emergency Operations Centers (EOC);
- Established contact with deployed Navy ships U.S. Ship (USS) Truman and USS Bataan, which were detailed to New Orleans to assist with the Katrina disaster; and
- Relayed health and welfare message traffic between volunteer agencies in Georgia and the American Red Cross National Headquarters in Washington, D.C.

In the aftermath of Hurricane Katrina, the NCS worked to ensure that all systems were in place for the ESF-2 elements to receive communications requests from affected areas.

Examples of actions taken by the NCS in support of its ESF-2 function include:

- Identified and dispatched satellite vans to various locations affected by the hurricane, including New Orleans City Hall, State Police headquarters in Baton Rouge, the Mobile Army Surgical Hospital at New Orleans Airport, and the National Guard facility in Jefferson Parish;
- Deployed communications satellite system platforms, satellite vans, and thousands of satellite and WPS-enabled phones to support recovery operations;
- Dispatched mobile capabilities, such as Cell on Light Trucks, to provide communications and offer cellular service to the Louisiana EOC;
- Delivered mobile communications trucks to the State EOC and to staging areas for Federal and industry responders;
- Initiated contacts with State EOCs to determine communication requirements;
- Identified requirements to supplement the destroyed Land Mobile Radio infrastructure in eight parishes in Louisiana;
- Worked with FEMA to initiate contract to provide replacement system; and
- Designed and installed a new E-911 system in Plaquemines Parish.

In addition, the NCS activated the National Response Coordinating Center ESF-2 desk at the FEMA Headquarters to provide around-the-clock support. The NCC utilized conference calls conducted twice daily with industry and Government representatives from communications companies (wireline, wireless, satellite) and numerous Federal entities both in the field and in Washington, D.C., including the NCS, General Services Administration, and FEMA to facilitate information sharing and coordinate response actions. In other support efforts, the NCC:

- Ensured continuous communication and collaboration between industry and Government, including the exchange of proprietary data to bolster situational awareness and operational response capabilities;
- Disseminated information regarding evacuee routes, curfews, health risks and other public concerns to assist service providers in their planning and restoration efforts;
- Facilitated the provisioning of the U.S. Marshals Service and Federal Bureau of Investigation (FBI) personnel to protect a critically important communications center in New Orleans. These law enforcement officers provided security for employees who felt threatened by individuals outside the facility allowing personnel to continue facility operations essential for response communications and coordination. The U.S. Marshals and FBI escorted employees and fuel trucks to and from the facility as well as providing facility security;

<ul style="list-style-type: none"> • Provided the local carrier with detailed satellite images, which the carrier had been unable to access without the NCC’s assistance. These images enabled the carrier to prioritize its restoration efforts by providing information on which areas were still under water; • Arranged the installation of a 106-foot portable Emergency Response Tower to Jefferson Parish to replace the destroyed 400 foot permanent tower that supported first responders in the area; • Successfully coordinated offers for assistance of communications resources and assets (such as satellite phones) from local, national, and international sources; • Maintained full time liaison with the Department of Defense’s (DOD) U.S. Northern Command for coordinating communication support to effected areas; • Provided commercial emergency mobile assets and organized military assets to support local authorities following Hurricane Rita; and • Provided status reports to the Department of Homeland Security (DHS) and the White House. 	<p>southwestern Louisiana and southeastern Texas, and reopened some of the levee breaches caused by Hurricane Katrina in late August. Rita hampered restoration efforts related to Hurricane Katrina by causing flooding and other obstructions in southwest Louisiana and southeast Texas. In addition, Rita knocked out power to over two million customers and caused at least 100 deaths. The Federal Government issued disaster declarations for parts of Louisiana and Texas. Examples of NCC actions include:</p> <ul style="list-style-type: none"> • Provided continuous communication and collaboration, including the exchange of proprietary data to bolster situational awareness and operational response; • Shared information regarding pre-landfall assessments, Government response activities, and damage assessments; • Facilitated local access coordination on behalf of the telecommunications infrastructure providers; • Coordinated deployment of cellular capabilities to Cameron Parish to replace damaged communications; and • Coordinated fuel delivery for broadcasters in the region to facilitate continued broadcast of information, updates, and instructions to citizens.
<p>Hurricane Rita</p> <p>On September 24, 2005, Hurricane Rita made landfall between Texas and Louisiana as a Category 3 hurricane. The storm caused extensive damage in the coastal areas of</p>	<p>In the aftermath of Hurricane Rita, the NCS issued 256 additional GETS cards, equipped 1,140 phones with WPS, and registered 80 new lines for TSP.</p>

LONDON TERRORIST ATTACKS

On July 7, 2005, terrorists unleashed a coordinated attack on London's public transportation system during the morning rush hour, bombing three Underground stations and one double-decker bus. The attacks killed 56 people, including the four suspected bombers, and injured 700 others. The incident was the deadliest single act of terrorism in the United Kingdom since the 1988 bombing of PanAm Flight 103, and the deadliest bombing in London since World War II. While London emergency services personnel responded to the incident, the NCS contacted British officials to offer support.



Because of the suspected use of cellular phones in the London terrorist attacks, officials in New York and New Jersey shut down cellular service in several area tunnels. Due to difficulties with the shutdown process, the DHS Acting Under Secretary for Information Analysis and Infrastructure Protection tasked the NCS to develop a coordinated decision-making process for disabling and restoring cellular communications services in times of emergency. The NCS worked with State and local authorities, cellular carriers, and corporate vendors to develop an emergency

wireless shutdown protocol to facilitate coordination of requests for cellular service suppression in defined area(s) with the cellular service providers as a result of a specific threat, and to ensure swift response and restoration once the threat was determined to no longer exist.

PREPAREDNESS EXERCISES

During FY 2005, the NCS participated in several exercises/activities aimed at testing and evaluating its preparedness and emergency response capabilities. The most noteworthy of these exercises were Top Officials 3 (TOPOFF 3) and Pinnacle.

In April 2005, the NCS participated in TOPOFF 3, a congressionally mandated international counterterrorism exercise series designed to test the Nation's preparedness to respond to and recover from a terrorist incident. TOPOFF 3 included a full-scale exercise, which allowed the NCS to test its emergency response plans in a real-time, realistic environment. The DHS Office of State and Local Government Coordination and Preparedness sponsored the TOPOFF Exercise series. Among issues addressed during the exercise were approaches to public communications in times of high public anxiety and confusion.

In June 2005, the NCS participated in the national-level exercise Pinnacle. The event consisted of a full-scale, scenario-based, interagency Continuity of Operations (COOP) exercise that provided a framework for each department and agency across the Federal Government to conduct its own internal COOP exercise focused on the specific purpose/objective of the organization.

III

NS/EP

**TELECOMMUNICATIONS
SUPPORT, ACTIVITIES, AND
PROGRAMS**

SECTION III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS) and the national security and emergency preparedness (NS/EP) community during fiscal year (FY) 2005.

National Communications System Leadership Changes

President George W. Bush appointed Mr. Robert B. Stephan as the Department of Homeland Security's (DHS) Assistant Secretary for Infrastructure Protection (ASIP) on April 11, 2005. In assuming that position, Mr. Stephan also became the Manager of the National Communications System (NCS). Mr. Stephan replaced Mr. Robert P. Liscouski, who submitted his resignation in early 2005.

Dr. Peter A. Fonash, who had been the Acting NCS Deputy Manager since the resignation of Mr. Brenton C. Greene in June 2004, became the NCS Deputy Manager on April 21, 2005. Mr. Gary Amato, formerly the NCS Deputy Division Chief for Technology and Programs, became Chief of the NCS Technology and Programs Division in January 2005.

INTERNATIONAL

The NCS, during FY 2005, began consolidation of its international engagement and coordination activities by relocating the Department of State (DOS) detailee to the Director's staff. The move will promote improved coordination of international strategic and policy goals within NCS and stakeholder agencies. The change aided greatly with ASIP Stephan's focus on international engagement as part of the National Infrastructure Protection Plan (NIPP), as well as a renewed effort with Canada and Mexico embodied in the Security & Prosperity Partnership (SPP). The DOS detailee works closely with the Critical Infrastructure Protection (CIP) (N3) and Technology & Programs (N2) Divisions both of which retain responsibilities for international engagement to advance NCS goals. Additionally, DHS relies upon the DOS detailee for coordination of Homeland Security Telephone Links. These core capabilities are highlighted and enhanced in both the bilateral and multilateral engagements of the NCS.

FY 2005 ACCOMPLISHMENTS

**North Atlantic Treaty Organization
Civil Communications Planning
Committee**

OMNCS represents the United States (U.S.) on the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), its telecommunications working group, and other subsidiary bodies. On behalf of the NCS, the DOS detailee heads the U.S. CCPC delegation at all NATO meetings with the U.S. telecommunications industry representative, as well as representatives of the U.S. Postal Service (USPS). The DOS detailee continuously works with the U.S. Representative to NATO's Senior Civil Emergency Planning Committee, as well as colleagues and counterparts in the State Department and other agencies.

During FY 2005, the CCPC met twice in plenary session, once at NATO headquarters in Brussels, Belgium, and once in Poiana Brasov, Romania. Its telecommunications working group (WG-T) and the postal working group (WG-P) have each met on four occasions. A number of small reporting groups — ad-hoc working groups and Groups of Rapporteurs — completed or continued work on papers from the 2003-2004 Work Program. Work is now underway on the 2005-2006 Work Program by similar groups within the committee.

The U.S. successfully persuaded members to conduct more of the work using electronic means as an adjunct to separate face-to-face discussions. Additionally, the U.S. found agreement with members to schedule and conduct reporting group meetings to coincide with Plenary, WG-T, or WG-P schedules and locations.

Major NATO FY 2005 activities and accomplishments include:

- Coordination with key allies to encourage a more focused work program for the CCPC. The work program supports the NATO defined roles for Civil Emergency Planning (CEP). As directed by the North Atlantic Council, direct linkage to the following main subjects were made in the work program: Support military planning and operations, support for national authorities in civil emergencies including protection of the civil population against chemical, biological, radiological, and nuclear (CBRN) incidents, cooperation with partner nations, and NATO Crisis Management Arrangements.
- The U.S. volunteered to head Task 2.1 of the 2005/2006 Work Program, which will examine member nations' response to terrorism. Additionally, the U.S. has offered to lend its expertise to several other initiatives in the 2005/2006 work program.
- Papers from reporting groups the U.S. participated in were completed on electromagnetic pulse (EMP), Information Society, and Impact of CBRN/weapons of mass destruction on CEP. Nearing completion are papers on Local Loop and International Telecommunications Organizations. The Local Loop paper is of particular note, as a success with the focus of the product directed to CEP planners. Several documents reflecting the full range of the Work Program are now in various stages of development and/or discussion.

- A joint Experts Training seminar was conducted during November 2004 that included the Manager of the National Coordinating Center (NCC), and three USPS experts. The tabletop exercise provided insight on the problems faced when dealing with multiple sectors and critical infrastructure interdependencies. The U.S. designated the Manager of the NCC the Electronic Communications Liaison Officer to be contacted by NATO for technical assistance with international telecommunications issues during times of emergency, crisis, and war. The NCS also attended a NATO seminar in Zurich discussing the interdependencies of the so-called “Magic Triangle” of Communications, Power, and Transportation.
- The U.S. also participated in team visits of NATO experts to Partner nations in Croatia and the Slovak Republic. Both telecommunications industry and USPS experts were represented in the multinational teams.

International Engagement

Policy

This year, under DOS lead, a U.S. multi-agency working group is revising U.S. International CIP strategy. The NCS, along with other directorates in Infrastructure Protection, participated in a number of meetings to start work on the new documents. Generally, the focus will move from outreach efforts to building effective working relationships with allies and other nations that help the U.S. address its Homeland Security goals.

Under the guidance of ASIP Stephan, the NCS defined its international engagement policy as part of the update to the NIPP.

Among the many groups the NCS participates in, the NCS also participates in the DOS led U.S. Government (USG) working group on next generation networks (NGN). The unique relationship the NCS/NCC has with the Telecom Information Sharing and Analysis Center (ISAC) lent itself well to soliciting input from the U.S. telecommunications industry via the President’s National Security Telecommunications Advisory Committee’s (NSTAC) NGN Task Force (NGNTF) in preparation for discussions in Geneva under the International Telecommunications Union’s Study Group on NGN. Additionally, the NCS and the National Cyber Security Division (NCSD) have worked throughout the year to find and exploit opportunities to work together on issues of common concern or interest.

Bilateral and/or Multi-lateral Relations

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

- SPP — This new framework for U.S., Canada, and Mexico addresses mutual cross-border CIP and CEP. The NCS, as lead for U.S. telecommunications, is playing a significant role in coordinating activities under Goal 9 of the Security portion of the Partnership. Additionally, the NCS is working with several other organizations and agencies on cross-cutting issues in both portions of the SPP. To date OMNCS staff have met twice with Canadian counterparts and re-engaged Mexico with a teleconference.

<ul style="list-style-type: none"> • Canada — <ul style="list-style-type: none"> • Katrina relief and support. The long-standing relationship between U.S. and Canadian telecom sectors, allowed for real-time communication and assessment with our Canadian colleagues. Canada quickly ensured continuous participation in the daily teleconferences and rallied “men & material” support to stage for on site assistance if and when needed. • Civil Emergency Planning Telecommunications Advisory Group (CEPTAG). The U.S./Canada CIP bilateral agreements established the CEPTAG working group. It also provides the foundation for work on the SPP. The U.S.-Canada working group continues to enjoy a strong and effective relationship as a broad range of issues including SPP, NATO, and the trilateral relationship of U.S./Canada/UK. • The weekly Video Teleconferences between the NCC and Canadian CIP/CEP officials continued throughout the year. In addition, regular liaison visits by Canadian operations personnel to the NCC continued this year. • Bell Canada, a Canadian telecommunications company and member of the Canadian 	<ul style="list-style-type: none"> Telecommunications Cyber Protection (CTCP) working group, participated in the NCS’ National Security Information Exchange (NSIE), a best-practice/information sharing forum. • As a result of U.S./Canada information sharing on ISAC best practices, Industry Canada established the CTCP, a Canadian Telecommunications information sharing organization with like objectives. • With the help and expertise of the NCS, Industry Canada worked with a Canadian wireless service provider to implement Wireless Priority Service (WPS) to facilitate the completion of critical calls during emergencies for personnel with public safety and emergency preparedness responsibilities throughout Canada. • Mexico — Monthly teleconferences conducted under the auspices of the Bi-National Accord, continued until early in the calendar year when Mexican cabinet level reassignments resulted in a break of communication. Contact was recently established with the newly designated Mexican Telecommunications liaison enabling re-engagement, with broad discussion on the many aspects of the relationship.
--	---

- United Kingdom — Following the London bombings on July, 7, 2005, the U.K. dispatched a representative to discuss and explore possibilities for enhanced communications between our governments during times of crisis. The NCS has since met twice with the U.K. to further explore the proposal. The proposal now includes a tri-lateral arrangement between the U.S., U.K., and Canada.
- Israel — At the request of Israel, DHS Office of International Affairs formed a working group for CIP. The inaugural meeting took place in DHS headquarters with NCS and NCSD providing a joint presentation and proposals. The NCS proposed the establishment of a hotline between the DHS Secretary and his counterpart, which was well received.
- Netherlands — The NCS hosted a visit of a delegation from the Netherlands composed of high-level Government officials. The Netherlands had an interest in the activities of the NCC and received briefings on NCC capabilities.
- Russia — The Manager of the NCS participated in the U.S.-Russia Technical Talks held at the U.S. DOS in October 2004. In his capacity as Chairman of the Standing Subcommittee on Upgrades, the Manager has the responsibility for U.S. oversight of improvements to and modifications of the various “hotline” programs between the two nations. The Manager negotiated

preliminary plans and procedures for the installation and activation of a Homeland Security Telephone Link (HSTL) between Secretary Ridge and his Russian counterpart. Further, the Manager of NCS participated in the U.S.-Russia Technical Talks in Moscow in April 2005. Representing DHS, the Director led the proposal to establish a hotline between the DHS Secretary and Russia. After an in-depth discussion, the Manager brought back issues for evaluation and decision.

Hotlines

Homeland Security Communications Links (HSCL/HSTL, aka Hotline) lines provide the Secretary the capability to discuss issues concerning common counter-terrorism initiatives with his foreign colleagues in a rapid, reliable, and secure manner during times of emergency. Additionally, the hotlines provide the Secretary with the ability to contact his counterparts on a recurring basis during periods of non-emergency to discuss sensitive matters relating to the welfare and protection of nations.

The initiative to establish hotlines between the Secretary and key counterparts in other countries was undertaken in late 2003 with six countries designated to be the first — U.K., Mexico, Canada, Russia, Israel, Japan and NATO. To date, HSTLs have been established with Canada, Mexico, and the U.K. A link with Russia is being actively pursued.

OMNCS also discussed the status of hotlines and the Senior Leadership Communications program of which the HSCL's are a part, with the recently installed head of the Defense

Information Systems Agency (DISA). DISA provides technical, operational, and maintenance support for the hotlines.

FY 2006 and Beyond

NATO

The U.S. will continue to maintain representation in the CCPC, to ensure that U.S. interests and goals are addressed in the body. Planning includes attendance in normally scheduled Plenary (2) and Working Group (4) meetings throughout the year. The aforementioned analysis of nations' response to terrorism is due calendar year (CY) 2006. The U.S. has already participated in one team visit to Latvia. Additional team visits for this CY are anticipated.

Bilateral and Multi-lateral Meeting

The NCS will continue to foster those relationships noted in accomplishments in FY 2004 and 2005 that have proven to produce meaningful, reciprocal discussion and agreement. This will be particularly so for the SPP with Canada and Mexico. Relationships with key allies, the U.K., and Japan will also be of critical focus. Below is the latest list of bilateral and multi-lateral meetings the NCS may be invited to participate in:

- Joint Contact Group: A high level U.S./U.K. forum to explore a variety of security issues.
- Exercise Cyber Storm: This DHS-sponsored interagency exercise originally slated for November 2005 has been postponed to February 2006. Representatives from Federal, State, local, and allied governments will participate as well as industry.
- Japan: A CIP Bilateral meeting has been scheduled for early December 2005. On the agenda is a

proposal for the establishment of a hotline.

Hotlines

In addition to continued negotiation to establish a hotline with Russia, the NCS will seek to establish hotlines in Israel, Japan, NATO, Australia, and New Zealand.

TECHNOLOGY AND PROGRAMS DIVISION

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

Division objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs and evaluating emerging technologies to alleviate impediments to interoperability. The NCS shares this information with industry and international standards organization bodies to ensure that NS/EP requirements are incorporated into any recommendations those entities may be formulating.

The following pages highlight the major projects undertaken by the Technology and Programs Division during FY 2005.

PRIORITY TELECOMMUNICATIONS SERVICES

Government Emergency Telecommunications Service

Background

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

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient, reliable, and robust technology for supporting a service that would meet NS/EP mission requirements. GETS leverages the PSN's vast resources — a \$393 billion infrastructure with more than 178 million access lines and approximately 26,000 switches. The ubiquitous, robust, and flexible PSN supports more than 90 percent of the Government's telecommunications needs. Despite its enormous size and complexity, the PSN averages 99.999 percent availability.

The first objective of GETS planners was to expeditiously field a service that would provide priority call treatment. They incrementally improved the service with

specialized calling features. The strategy of developing GETS by using existing PSN assets enabled early implementation and provided technical currency by leveraging the continual improvements made by industry. Embedding GETS primarily within the software resources of the PSN also alleviated the necessity for the Government to purchase, install, maintain, and eventually update network equipment.

The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This resulted in separate GETS contracts with AT&T, MCI, and Sprint, the three largest IXCs. These companies are the only IXCs that can authenticate and process GETS calls. As such, access to these carriers must be available at all PSN end offices. Although the IXCs began with the same basic set of functional requirements, the implementation approach pursued by each IXC and the inherent differences in the structure of the IXCs respective networks caused the operational features and capabilities to differ slightly among the providers.

After the IXC implementation, the focus of feature development shifted to the local exchange carrier (LEC) networks. Computer Sciences Corporation's (CSC) Network and Telecommunications Integrated Solutions Division won the integration contract for development and implementation of GETS features in the LECs and for overall GETS operation, administration, maintenance, and provisioning services. Advanced Intelligent Network (AIN) technology provided the basis for the first phase of GETS LEC feature deployment, alternate carrier routing (ACR). ACR enhances access by automatically attempting all three GETS IXCs.

The GETS integration contractor (IC) entered into contracts with four primary switch manufacturers [Lucent Technologies, Nortel Networks, AG Communications Systems (AGCS), and Siemens] for the implementation of priority treatment and enhanced routing features on their products. The GETS IC also contracted with LECs to deploy and operate these features. GETS features will appear on additional switches as they are upgraded to required software releases or as additional LECs are brought under contract. In addition, as networks are upgraded, the GETS program continues to deploy enhancements that will help GETS calls terminate from the PSN to customer premises and to simplify carrier provisioning of GETS features. As the PSN evolves into NGN technologies, including packet-based technologies, the NCS is working with industry to maximize and protect the NS/EP community's substantial investment in circuit-switched network enhancements. This work includes one-on-one meetings with carriers and vendors to gain an understanding of their network evolution plans, participation in standards bodies influencing how NS/EP calls may be processed in NGNs, and development of requirements related to next generation call processing in acquisition packages for the IC and IXC follow-on contracts.

Operations and Features

Access to GETS is quick and simple: Users dial the universal access number (710-NCS-GETS) using standard telephone equipment, such as a desk set, pay phone, secure telephone [such as Secure Telephone Unit-Third Generation (STU-III)], cellular phone, facsimile machine, or modem. Telephones on the Federal Technology Service (FTS), the Diplomatic Telecommunications Service (DTS), and the Defense Information Systems Network (DISN) also provide access to GETS.

When a user dials the GETS universal access number, a tone prompts for a personal identification number. Next, a voice recording asks for a destination telephone number. In case the access control system is inoperative, a fail-open feature will allow users to complete their GETS calls. The utility of this feature has been demonstrated many times, most notably during the September 11, 2001, attacks on America and again during the hurricane seasons of 2004 and 2005.

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the NCS has worked to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks. In 1993, the American National Standards Institute (ANSI) approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993, which provides a classmark for NS/EP-related signaling messages. ANSI reaffirmed this standard in December 1999 and revised it in 2005 based on NCS input. The classmark allows NS/EP calls to be recognized in any U.S. network, facilitating the application of available GETS features.

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

Message (IAM) Implementation Plan, which was brought to the NIIF.

In December 1997, the NIIF accepted Issue No. 0095, "Implementing POTS IAM Priority Level 0." Switches that comply with the standard serve more than 90 percent of the access lines in the Nation.

During 2004, the NCS developed Version 1 of a Next Generation Priority Service (NGPS) Reference Architecture, and demonstrated the world-wide interoperability of NGPS functionality under the auspices of the Multiservice Forum. The NCS conducted Voice over Internet Protocol (VoIP) laboratory testing at the BellSouth Technology Assessment Center during April 2005. The purpose of the testing was to investigate NGN support of NS/EP voice services during conditions of severe network stress.

Interoperability

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

Like other services, GETS must navigate the rapidly evolving, but highly competitive, telecommunications environment spawned by the *Telecommunications Act of 1996*. In some areas, this environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin telephones

and Private Branch Exchanges (PBXs). Previous testing showed these problems to be particularly prevalent for coin-operated telephones owned and operated by small businesses and PBXs operated by hotels and motels. Commonly encountered problems include the need to deposit coins into a coin-operated telephone before dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

Currently, the NCS is working with coin-operated telephone industry groups, such as the American Public Communications Council, and hospitality industry organizations and associations, to raise awareness of GETS as an emergency, toll-free service that should receive treatment similar to that provided for 911 emergency and toll-free calls.

Successes

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

Amid the hurricane seasons of 2004 and 2005, GETS assisted NS/EP emergency response and recovery communications along the Gulf Coast region. Following Hurricane

Katrina in August 2005, there were 32,829 GETS calls into or out of the Gulf Coast region; 95 percent of these calls were successfully routed. Additionally, the NCS issued 2,010 new GETS cards to support NS/EP activities.

In the past year, the GETS program has continued to make significant progress in its outreach efforts to all levels of Government (Federal, State, and local) and other qualified NS/EP industry and non-profit organizations. As of September 2005, 110,460 customers held active GETS cards, an increase of 13,462 cards during the past year. Customers fell into the following categories: Federal, 69,744; State, 11,317; local, 15,149; industry, 12,829; and other NS/EP organizations: 1,421.

Wireless Priority Service

Background

Like GETS, WPS facilitates emergency response and recovery operations, helping to return the Government, as well as the general population, to normal conditions after serious events, such as floods, earthquakes, hurricanes, and terrorist attacks.

In the past ten years, the number of wireless telephone subscribers has increased from 24.1 million in December 1994, to 181.1 million in December 2004. Early in 1995, the NCS recognized that the significant annual increases of wireless subscribers indicated a need for priority communications over the wireless networks and initiated efforts to develop and implement a nationwide cellular priority access capability in support of NS/EP telecommunications. Since then, the NCS has undertaken a number of activities to improve wireless call completion rates during times of network congestion. In 1998 and 1999,

the NCS worked with an industry switch vendor to demonstrate end-to-end wireless priority features.

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

The days following the tragic events of September 11, 2001, saw widespread wireless network congestion, with wireless traffic demand estimated at up to ten times the normal amount in the affected areas, and double nationwide. The need for WPS became a critical and urgent requirement. Reacting to these events, the National Security Council issued guidance to the NCS regarding the development and implementation of WPS. Responding to the NSC guidance, the NCS provided an off-the-shelf immediate WPS (I-WPS) solution, with limited capabilities, by the February 2002 Winter Olympics in Salt Lake City. The I-WPS was operational by May 2002 in Washington, D.C. and New York City. WPS achieved nationwide coverage in December 2002.

Operations and Features

Achieving the requirement for nationwide WPS coverage will necessitate multiple carriers and multiple access technologies. WPS is based on the two access technologies most widely available in the United States,

Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). WPS is provided by the major GSM carriers, including T-Mobile, Cingular Wireless, and Nextel (now Sprint Nextel). T-Mobile began deploying WPS FOC in December 2003, and Cingular Wireless began deploying WPS FOC in July 2004. The Sprint Nextel FOC was achieved in FY 2005. In GSM, the wireless carriers and feature enhancements, such as operational measurements, have been added. As a result, user subscriptions for WPS have more than doubled in FY 2005. The provision of WPS capabilities in CDMA is well underway with the major CDMA carriers, Verizon Wireless and Sprint Nextel. Verizon Wireless requested and received, with the support of the NCS, an FCC waiver to the Second R&O, allowing Verizon Wireless to deploy WPS in phases beginning in 2006. During FY 2005, the NCS provided to the FCC a second report on the status of the development and implementation of WPS. WPS satisfies the requirements of the FCC Second R&O for invocation of the service on a call-by-call basis by dialing the WPS prefix (*272) at the start of each NS/EP call. FOC provides a full, end-to-end capability as shown in Figure 1.

Many of the significant challenges facing WPS stem from technology upgrades, requiring the NCS to assure continued availability of WPS capabilities as wireless carriers move to next generation wireless technologies. During 2005, the NCS released the first phase Industry Requirements (IR) for Universal Mobile Telecommunications System (UMTS) for those GSM carriers implementing the UMTS technology into their networks. This first phase focuses on redirecting UMTS calls to the GSM network.

Industry Requirements

WPS is made possible by strong industry partnerships with Government during the development of IR documents. WPS is based on wireless standards and IR documents jointly developed through active and cooperative participation of all stakeholders, including major wireless equipment vendors and service providers. Stakeholders completed initial requirements in February 2002, only four months after receiving direction from the NSC. The FOC requirements for both GSM and CDMA are now complete. Industry is currently working on UMTS Phase 1 requirements. In addition to establishing engineering requirements, the

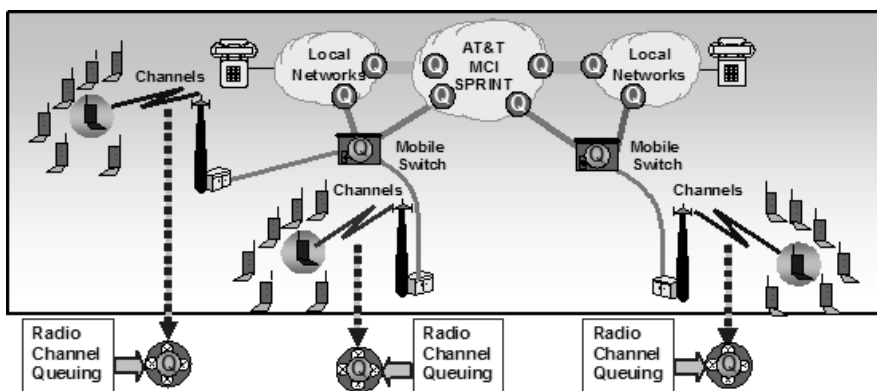


Figure 1 End-to-end call priority with WPS

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

Successes

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

In the past year, the WPS program continued to progress significantly in its outreach efforts to all levels of Government (Federal, State, and local) and other qualified NS/EP industrial and non-profit organizations. As of September 2005, 25,517 authorized users subscribed to WPS, a 136% increase over the past year, categorized as follows: Federal: 22,230; State: 833; local: 1,461; industry: 990; and other NS/EP organizations: 3.

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

NEXT GENERATION PRIORITY SERVICES

Traditional NS/EP priority services, such as GETS and WPS, were specified, engineered, and implemented when the public switched

telephone network (PSTN) operated exclusively on circuit-switched technology. Today's PSTN is incorporating, and eventually replacing, circuit-switched equipment with the packet-switched technologies that have supported Internet Protocol (IP) data networks for some time. This convergence into an NGN dictates the required evolution of GETS and WPS to NGPS. Using packet technology, the NGPS will provide priority NS/EP communications not only for voice, but also for video and data applications.

The NCS assessed emerging IP technologies and found that there is no overall priority or end-to-end Quality of Service (QoS) architecture in place on the Internet today. Service providers are deploying QoS and priority techniques only within their individual IP networks and only for limited applications and users. In light of that environment, the NCS will focus its research as follows:

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

The NCS awarded a contract to AT&T to investigate the problems involved in implementing NGPS on packet-based networks, research priority treatment options

available to NS/EP traffic on such networks, and standardize NGPS end-to-end requirements. As the NGPS architecture evolves and is modeled, the NCS will continue to coordinate with AT&T and other industry partners to jointly develop requirements, a highly successful tactic during development of the GETS and WPS programs. This strategy will ensure an effective NGPS is developed that provides NS/EP users the priority services they require while placing no undue hardships on either the communications industry or the public.

PRIORITY SERVICES TEAM STANDARDS DEVELOPMENT

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

Traditional NS/EP telecommunications services have been designed around the circuit-switched infrastructure of the PSTN. However, now evolving converged and public NGN are emerging with packet-switched design infrastructures. As this evolution continues, priority telecommunications services will be guided and implemented by commercial standards that stem from emerging technologies based on packet-switched infrastructures, such as IP-based networks.

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

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

Recognizing that IP and wireless communications are becoming increasingly vital to national security during NS/EP events, the Priority Services Team focuses on these two telecommunications media by working proactively with industry in standards development organizations.

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

- Alliance for Telecommunications Industry Solutions;

<ul style="list-style-type: none"> • Telecommunications Industry Association; • International Telecommunication Union, Telecommunications Sector; • Internet Engineering Task Force; • TeleManagement Forum; • Third Generation Partnership Project; and • Third Generation Partnership Project 2. 	<p>than a retrofitted fix in deployed systems, and investigating new features emerging in packet-based networks to enhance NS/EP operations (for example, e-mail, instant messaging, multicast video, web access, tunneling, and mobility);</p> <ul style="list-style-type: none"> • Performing and promoting independent testing and implementation of proposed technical solutions; and • Participating in the development of contemporary telecommunications industry acquisition tools, such as Service Level Agreements and associated application notes, to better specify criteria for availability, reliability, and quality performance of delivered NS/EP telecommunication services.
<p>Technical approaches employed for the development of priority services in the above organizations include:</p> <ul style="list-style-type: none"> • 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 work programs, in cooperation with industry and academia; • Developing and providing detailed technical proposals (such as NS/EP contributions) within industry standards programs, and encouraging industry participants in these programs to make technical proposals to augment NCS proposals; • Integrating NS/EP technical service agreements into operational systems as an inherent part of the underlying packet-based infrastructure rather 	<p>MODELING, ANALYSIS, AND TECHNOLOGY ASSESSMENT</p> <p>As directed by E.O. 12472, the NCS uses modeling and analysis techniques and applications to “...conduct technical studies or analyses...for the purpose of identifying...improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives.”</p> <p>Network Design and Analysis Capability Because the NS/EP community relies heavily on the PSN, the NCS developed the Network Design and Analysis Capability (NDAC) to analyze current U.S. networks and to evaluate the need for additional capabilities. The NCS has invested many years establishing strong working relationships with commercial carriers and</p>

Government departments and agencies, and developing PSN modeling methodologies, tool sets, and unique databases that include proprietary data from the major carriers. The NDAC serves as a tool to conduct studies that cover multiple communications areas such as wireline, wireless, and the Internet.

Backup Dial Tone/Route Diversity Analyses

The Backup Dial Tone (BDT) study uses the NDAC to examine methods and technology approaches to enhance communications reliability in the Washington metropolitan area under emergency conditions. This effort is in response to Executive Branch concerns that key Federal agencies and emergency responders may be at risk of losing essential wireline communications services under disaster or emergency conditions similar to those of September 11, 2001. Concurrently in Phases III and IV, the NCS is conducting demonstrations of Free Space Optics and other wireless technologies to determine their potential to enhance communications resiliency (Phase III). Phase IV included the development of a route diversity methodology to enable Federal agencies in the Washington D.C. area to assess their current level of diverse communications connectivity into the public networks. As directed by the White House, the NCS will continue to assist Federal agencies to analyze their communications and, when required, determine the optimum technical solution to increase resiliency.

NGN

The circuit-switched architecture of the PSN is converging with the packet-switched technology of the Internet, evolving into the NGN. As the architecture evolves, the tools and techniques used to assess the performance of the PSN must evolve as well.

Since the technology, architectures, protocols, and interfaces the service providers may use during this network evolution are in development, several likely NGN architectures and traffic streams (voice, data, and streaming video) were developed. After the baseline architecture and traffic models were created, multiple traffic overloading scenarios were applied to each to identify any potential network bottlenecks. In addition to traffic overloading scenarios, cyber attack and nuclear attack scenarios were applied to the simulated NGN architectures in order to assess their impact on overall network performance. A predictive analysis environment was then created to assess the candidate architectures upon network performance, cost, and ability to meet the NS/EP mission.

Internet Analyses

Although NS/EP communications have long been supported by the PSN, an increasing number of Government users are now using services offered through the Internet; consequently, the logical and physical infrastructures of the Internet must be modeled to support NS/EP analyses. With the on-going NDAC expansion to include packet-switched networks, the NCS has developed an Internet modeling capability that captures physical and logical interdependencies between Internet Service Providers (ISP) from both architectural and traffic perspectives. This capability is used to determine the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure.

IP Network Performance under Cyber Attack

Modeling and analysis capabilities must answer such questions as: What impact would a cyber attack have on Federal networks? Which Federal

telecommunications systems need to be protected? IP networks span the globe with the Internet being the largest and most well known. Cyber attacks against these networks often affect parts of the network beyond what was specifically targeted, causing a significant degradation to network performance in terms of packet latency, jitter, and loss. Now that an analytical model of an IP network under attack has been developed, simulation models and laboratory experiments of cyber attacks will be used to calibrate the analytical results.

Traffic Analysis of Critical Federal Telecommunications Infrastructures

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

Supervisory Control and Data Acquisition Modeling

A capability is being developed to model the interaction and dependency between telecommunications and Supervisory Control and Data Acquisition (SCADA) systems to enable detailed analyses of SCADA communications vulnerabilities. Combining the modeling and analysis capabilities of the NDAC with the Idaho National Lab, the SCADA test bed provides the ability to test variants of SCADA equipment, software,

protocols, and configurations. This collaboration, using real SCADA systems and their communications interfaces, will enable the calibration of the NDAC SCADA communications dependency and vulnerability models, and the development of technology, procedures, and recommended best practices for mitigating SCADA communications vulnerabilities.

Next Generation Priority Services eXperimental Testbed Environment

The NCS is developing the NGPS eXperimental Testbed Environment (XTE) to emulate a scaled-down version of the Internet and an ISP’s network, to provide the capability to inject severe congestion both on the network and NGN end systems, and to test and validate that emergency telecommunications services work properly from end-to-end. This is accomplished using call load generators and traffic generators coupled with a strong modeling and analysis capability.

The NGPS XTE consists of:

- Network devices (routers and switches) simulating an ISP’s backbone/core and access network;
- Security devices (such as firewalls, session border controllers, and intrusion detection capabilities) to protect the network assets by detecting and responding to simulated threats;
- Hosts and servers providing the invocation and termination of NGN services and priority services;

- Test and analysis equipment to generate voice and data traffic and to gather results of the effects of congestion on NGN services; and
- VoIP telephones and systems to represent a VoIP service provider's service infrastructure.

Technology Assessment Laboratory

The NCS has established a fully accredited Technology Assessment Laboratory (TAL), which provides the capability to:

- Evaluate Contract Deliverables: Some contracts have software and/or hardware deliverables; the TAL is used to evaluate these deliverables for acceptance purposes.
- Evaluate Products: The TAL provides a platform to research, identify, and evaluate off-the-shelf products (both commercial and Government) that may satisfy specific NS/EP requirements, often obviating development contracts.
- Host Applications and Databases: The TAL provides the host environment for several applications and associated databases developed specifically to ensure survivable and robust communications in support of NS/EP requirements. These applications include the NDAC which is a set of tools, data sets, and methodologies that enable modeling and analysis of the PSN.
- Provide Component-level Simulation: Although the NDAC provides a macro view of network behavior, it lacks the ability to adequately simulate the

behavior and interaction of individual pieces of software and hardware. The TAL provides for this type of simulation. Such simulations are useful for evaluating new technologies or proposed solutions such as NGPS.

- Participate in Community Research Projects: The TAL has enabled the NCS to move beyond its role as a patron or sponsor of research, to become an actual participant. Besides enhancing our engineers' and computer scientists' expertise in critical areas, Internet community projects-such as The HoneyNet Project-provide an excellent opportunity to increase the respect and recognition of the NCS within the research and development community.
- Training: The TAL provides an environment to support ongoing hands-on technical training, an alternative to expensive vendor-provided training.

Advanced Technology Group

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

communications. The following paragraphs address these topics in detail.

TEDE

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

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

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

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

- PSTN switching systems and infrastructure;

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

The NCS has published documents delineating the vulnerabilities of telecommunication systems to EMP, MHD effects, HPM, directed energy systems, high radiation environments, solar flares, and lightning.

The NCS participated in the work of the Congressional EMP Commission by making available legacy TEDE studies and providing a briefing of current efforts. This briefing focused on vulnerabilities to the total national infrastructure, with telecommunications being a critical part of that infrastructure.

The ATG continues to lead the effort in identifying the vulnerabilities of IP-based systems to TEDE.

The ATG examined the risk of TEDE from High Power Electromagnetic generators to the wireline, wireless, and ground-bases assets of the satellite telecommunication infrastructure. The analysis also determined equipment vulnerability to upset and damage through preliminary testing of telecommunications and satellite equipment; developed a preliminary model on the effects

of HPM threats on the telecommunication infrastructure; and performed a preliminary risk evaluation by determining the minimum combination of threat parameters needed to exceed equipment vulnerability thresholds, exploiting constraints on the threat through physical and practical trade-off.

VULNERABILITY ISSUES

The ATG published a number of Technical Information Bulletins (TIB) and technical reports concerning vulnerability issues associated with the telecommunications infrastructure. The following is a list of the vulnerability studies conducted during the past year.

Analysis aimed at the vulnerability of the common OSS infrastructure of the PSTN

The objective of this analysis is to capture the PSTN OSS infrastructure in a generalized model and assess OSS security vulnerabilities and risks brought about by technology evolution changes in the regulatory environment, and current business drivers. Also presented are the strategies and methods to mitigate the vulnerabilities and risks.

Analysis of the vulnerabilities of the service provider synchronization networks to various threats

The elements of the synchronization network, Primary Reference Sources and Timing Signal Generators, and the vulnerabilities of these elements to various threats, are highlighted.

Cyber vulnerabilities within telecommunications SCADA systems

This TIB examines the relationship between the Telecommunications Management Network (TMN) and the telecommunications system it controls. It focuses on security as it relates to potential cyber attacks against our Nation's ability to communicate in times of

need. The technical bulletin describes the evolution and architecture of the TMN; explores common and critical cyber threats to the TMN, which include the identification of potential attackers, possible attack types and methods, and subsequent consequences of an attack; explains both the voice and data sides of the underlying telecommunications network including control systems and assessments of vulnerabilities; shows how the voice and data networks are traversing down a path towards true convergence and exploring the emerging difficulties and security considerations such convergence brings; and provides recommendations on how to best move forward on securing this critical infrastructure control system.

Cyber vulnerabilities within the energy infrastructure's SCADA systems

This TIB examines the relationship between SCADA systems and national infrastructure security as it relates to potential cyber attacks against the Nation's natural gas distribution and water treatment infrastructure. It describes the current state of SCADA system architectures within each of the natural gas and water treatment industries, evaluates the extent to which SCADA is used within the operation of each industry, identifies cyber attack vulnerabilities within each of the industrial SCADA systems, and provides recommendations on how best to move forward on securing these critical infrastructure control systems.

EVOLVING ISSUES

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

Global Positioning System

This TIB examines global positioning systems (GPS) and how the different systems may be used in support of NS/EP and CIP missions. It addresses the space, user, and control elements of a GPS system, and examines the advantages and disadvantages of three GPS systems. The three systems investigated are: the U.S. NAVSTAR system, the Russian Global Navigation Satellite System, and the European Galileo System. The TIB also discusses the GPS security implications for each system as well as the U.S. GPS policies and standards.

VoIP/E9-1-1 for NS/EP

This TIB examines the current day state of VoIP technologies, as well as the existing emerging VoIP and Internet network technology and support for Enhanced 9-1-1 (E9-1-1) emergency traffic. Also, it identifies current issues associated with the deployment of VoIP/E9-1-1, and discusses the applicability within the overall NS/EP environment. Moreover, the TIB provides recommendations for NCS activities to track these technologies, influence the development of standards designed to minimize the impact of VoIP implementations, and to enhance NS/EP telecommunications in the future.

Institute of Electrical and Electronics Engineers Standard 802.1X For Local and Metropolitan Area Networks Port-Based Network Access Control

This TIB examines the Institute of Electrical and Electronics Engineers (IEEE) 802.1X Standard for Local and Metropolitan Area Networks for Port-Based Network Access Control and its development. It discusses the definition of Extensible Authentication Protocol (EAP) and how it relates to both wired and wireless networks. It also compares Transport Layer Security Protocol,

Tunneled Transport Layer Security Protocol, and Protected Extensible Authentication Protocol. Also, the TIB presents conclusions and recommendations reflecting state-of-the-art EAP development and provides recommendations for continuing study and additional research possibilities.

CRITICAL INFRASTRUCTURE PROTECTION DIVISION

The CIP Division includes five branches: the Operations Branch, the Planning, Training, and Exercise (PT&E) Branch, the Operational Analysis (OA) Branch, the Priority Telecommunications Services (PTS) Branch, and the Information Technology (IT) Branch. A Division Resource Coordinator and a CIP Project Coordinator assist the CIP Division Chief in managing and coordinating special projects and programs in the areas of budget, contracting, personnel, administrative oversight, and project management.

The Operations Branch is responsible for emergency response preparedness, operations, and information sharing activities with industry, Government, and international partners. The branch manages the day-to-day operations of the NCC, the Communications ISAC, and the 24x7 Watch Analysis Operations. Emergency response preparedness and operations activities include activating and responding to events impacting the communications infrastructure, including presidentially declared events of national significance; activating Emergency Operations Teams (EOT); producing and maintaining standard operating procedures; and maintaining the readiness of the NCC Watch Center and the NCC and OMNCS relocation sites.

The PT&E Branch is responsible for developing, conducting, and participating in NS/EP and CIP-related national, regional, and organizational exercises and operational training to ensure OMNCS staff and NCS member organizations are prepared to conduct essential emergency response telecommunications functions. The branch supports several interagency working groups focused on emergency response, continuity of operations (COOP), and continuity of Government (COG) planning. The Branch also administers the NCS Individual Mobilization Augmentee (IMA) Unit, which consists of U.S. Army Reserve Signal Corps officers who may be activated for duty to assist the OMNCS during emergency operations.

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

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

The PTS Branch is the operational arm of the NCS priority telecommunications programs to include associated outreach. OPT manages the administration of the GETS, WPS, and Telecommunications Service Priority (TSP) programs which allow NS/EP personnel priority access for telecommunication needs during crises on the public telecommunications infrastructure.

NCC

DHS/NCS manages the NCC, a joint industry-Government operation. The NCC encompasses the U.S. communications industry and Federal Government organizations that are involved in responding to the Federal Government's NS/EP communications service requirements and support planning for a more enduring national and international communications system to satisfy those requirements. NS/EP can be defined as, "any event or crisis which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the National Security Emergency Preparedness Posture of the United States." The mission of the NCC is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities.

The operational arm of the NCC is its 24x7 watch and analysis operation, the NCC Watch. Senior level information assurance analysts located on site in the NCC Operations Center staff the NCC Watch. These Watch analysts are closely integrated with the Government NCC operations staff and industry representatives from the NCC member companies. They foster technical working relationships with external liaison partners in industry and Government. Their technical expertise and collaboration efforts, coupled with evolving analysis capabilities, are key to adding value to the NCC Communications ISAC information sharing process.

On a daily, 24x7 basis, the NCC:

- Monitors the status of all essential communications facilities through consultation with both resident and non-resident industry partners,

<p>Government partners, and open source information;</p> <ul style="list-style-type: none"> • Consults with private industry to exchange status information and develop coordinated action plans; and • Focuses on NS/EP communications needs of the Federal Government. <p>In addition, the NCC hosts the Communications ISAC (formerly referred to as the Telecommunications ISAC), which supports the mission assigned by E.O. 12472 and the national critical infrastructure protection goals of Government and industry. The main emphasis of the Communications ISAC is to analyze reported events and symptoms as rapidly as possible to avert or minimize impending damage to telecommunications operations. A secondary goal is to establish causes after the fact to prevent future recurrences.</p> <p>Major NCC activities in FY 2005 included:</p> <ul style="list-style-type: none"> • Advised NCC membership of threats, vulnerabilities, switch outages, fiber cuts, power outages, and other incidents affecting the communications infrastructure. • Provided evaluation and analysis on multiple hardware and software vulnerabilities and exploits including Bagle, Skull B and Skull C Trojan, and Cabir Worm. • Participated in the June 2005 national-level exercise, PINNACLE. The event was a full-scale, scenario-based, interagency COOP exercise that provided a framework for each component agency across the Federal 	<p>Government to conduct its own internal COOP exercise focused on the specific purpose objectives of the organization.</p> <ul style="list-style-type: none"> • Maintained a high-alert posture and monitored, analyzed, and assessed approaching hurricanes during the 2005 hurricane season, including Hurricanes Katrina and Rita. The NCC Watch actively tracked and communicated pre- and post-landfall response activities in coordination with Emergency Support Function #2 (ESF-2) partners, field office components, and its telecommunications industry membership. The NCC also made widespread use of existing and established new information sharing channels with communications service providers, mitigated potential facility damage, and helped to reduce anticipated recovery times. • Completed an initial telecommunications impact assessment for Hurricane Katrina in August 2005 to prepare for possible impacts to the telecommunications infrastructure and gain a greater understanding of assets and personnel deployment needs in the near-term. • Identified priorities for restoration of the communications infrastructure, including security, fuel, and access, following the hurricanes, especially after Katrina's landfall. • Supported the use of NCS priority telecommunications programs to assist in restoration of the communications infrastructure
--	---

during and after Hurricane Katrina. The GETS provided assured communications for Government and military users, completing over 94 percent of calls that would otherwise have not been connected. The TSP system provisioned over 1,700 circuits, providing for prioritization of service restoration and provisioning of new services. Government users with the WPS feature achieved priority access to existing cellular networks.

- Hosted a semi-annual meeting of NCC industry and Government membership in November 2004 and May 2005. The semi-annual meeting brought together Communications ISAC members to discuss developments in CIP, coordination with DHS, the year's accomplishments, and strategies for the future. The meetings also serve as a means for introducing new members to the group, building relationships and trust, and familiarizing them with the functions of the NCC.
- Enhanced procedures to ensure effective information sharing, especially within DHS to include the NCSD and U.S. Computer Emergency Readiness Team, the Infrastructure Coordination Division and National Infrastructure Coordination Center (NICC), and the Homeland Security Operations Center's Infrastructure Protection NICC Desk.
- Developed a draft Cellular Shutdown Protocol after the London bombings and corresponding New York City

shutdown to facilitate coordination of requests for cellular service suppression in defined area(s) with the cellular service providers. The draft protocol was briefed to the State Homeland Security Advisory Panel and the major cellular service providers as to technical feasibility. Consideration is being given for issuance of an authoritative directive to elevate cellular shutdown from a "voluntary - best effort" to a higher level of requirement. Next steps include soliciting and receiving feedback on draft procedures with State authorities and industry and developing and scheduling a cellular shutdown procedure training exercise with appropriate State Government emergency officials and cellular service providers.

- Maintained an effective working relationship with both the Canadian Government and the telecommunications industry in Canada. Personnel from Industry Canada and the Public Safety and Emergency Preparedness Canada deploy to the NCC to coordinate response efforts requiring U.S./Canada cooperation.
- Continued a bilateral relationship with Mexico to foster the creation of a Civil Emergency Telecommunications Advisory Group between U.S and Mexico, and eventually a tri-lateral body to work critical telecommunications infrastructure cross border issues.

**COMMUNICATIONS
INFORMATION SHARING AND
ANALYSIS CENTER**

The NCC Communications ISAC is a function of the NCC and builds on the history of cooperation and established trust among the NCC members. The Communications ISAC facilitates voluntary collaboration and information sharing among its participants. The ISAC mission encompasses “all hazards” with the potential to affect the telecommunications sector. Hazards may appear as outages, anomalies, or other events or incidents, including a coordinated attack, in any of the systems that constitute or support the national telecommunications infrastructure.

Currently there are 35 industry member companies and associations in the Communications ISAC. Membership is open to companies that provide telecommunications or network services, equipment or software, select Competitive Local Exchange Carriers, ISPs, communications professional organizations/associations, and companies with participation/presence in the communications and IT sector. The 24x7 NCC Watch performs triage for all NCC functions, manages the NCC Communications ISAC information sharing process, and provides an analysis function for the NCC Communications ISAC. As part of the information sharing process, industry provides daily, weekly, and as-needed assistance on the following activities:

- Prompt analysis of service disruptions and identification of restoration actions;

- Coordination and restoration of telecommunications in support of NS/EP needs;
- Monitoring the status of essential telecommunications facilities;
- Identifying liaison points and subject matter experts in each company;
- Maintaining readiness to transfer operations from normal to emergency status;
- Coordinating and expediting the initiation of NS/EP telecommunications services; and
- Contributing to the development of technical standards and national network planning.

Major NCC Communications ISAC activities in FY 2005 included:

- Renamed the Telecommunications ISAC as the Communications ISAC to better reflect the inclusion of non-traditional telecommunications companies (such as, satellite providers) and the expansion of telecommunications providers into the IT services arena.
- Fostered relationship with the IT ISAC to support efforts related to the convergence of the telecommunications and IT sectors.
- Implemented additional strategies to encourage new membership to the NCC Communications ISAC, including satellite providers. During FY 2005, industry membership

expanded to include Globalstar, Internap, Intelsat, New Skies, and Cingular Wireless.

- Established the Communications Sector Coordinating Council (SCC) during the third quarter of 2005 to provide an institutionalized process for engagement with Government for programmatic planning, strategy, and policy. The Communications SCC elected a six-member steering committee and formulated written comments on the NIPP.
- Led the development of the Emergency Notification System as chair of the ISAC Council Working Group.
- Participated in several emergency response exercises, including Emergency Response Team training sessions and the April 2005 DHS Top Officials Three Exercise (TOPOFF 3), a Congressionally mandated exercise designed to strengthen the Nation's capacity to prevent, prepare for, respond to, and recover from large-scale terrorist attacks involving weapons of mass destruction.
- Maintained continuous 24x7 communication and collaboration with the Government prior to, during, and after Hurricane Katrina made landfall to coordinate response activities. The Communications ISAC facilitated the exchange of proprietary industry data to bolster situational awareness and operational response, and obtained critical information from the Government, including evacuee routes, curfews, and health

risks to assist communications companies in their planning and restoration efforts.

- Provided the Government with situational awareness related to the deployment of commercial assets in support of Government command and control nodes at all levels, deployment of response personnel, and assistance for displaced persons. During the 2004 and 2005 hurricane seasons, the Communications ISAC played a key role in informing Government of available emergency communications assets, including teams, satellite vans, cell sites on wheels, cell sites on light trucks, terrestrial communications equipment, and phone banks.
- Formulated lessons learned and mitigation strategies from emergency incidents such as Hurricanes Katrina and Rita, and the New York/New Jersey Cellular Outage.

ALERTING AND COORDINATION NETWORK

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

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

NETWORK SECURITY INFORMATION EXCHANGE ACTIVITIES

The joint meetings of the President's NSTAC and Government NSIE's provide a trusted environment in which industry and Government representatives can exchange information on threats to and vulnerabilities of the PSN. The NSIEs focus on technical issues affecting the security of the PSN, such as unauthorized penetration or manipulation of the public network software, databases, and other infrastructures supporting NS/EP telecommunications services.

The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the PSN and its supporting infrastructures. In FY 2005, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including IP convergence from U.S., Canadian and U.K. perspectives, SS7 and VoIP security, and offshore manufacturing. The NSIEs produced "An Assessment to the Risk of the Security of the Public Network" which was released April 2005. In FY 2005, the NSIEs held a meeting in Ottawa, Ontario, Canada to assist that country in establishing an NSIE structure similar to those already in existence in the U.S. and U.K.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARED RESOURCES (SHARES) High Frequency (HF) Radio Program is a key element of the developing NS/EP infrastructure. SHARES provides the Federal emergency response community with a single, interagency emergency message handling system for the transmission of NS/EP information by bringing together existing high frequency radio resources of Federal and Federally affiliated organizations when normal communications are destroyed or unavailable.

The SHARES HF Interagency Working Group, made up of 146 members representing 110 organizations, provides guidance and direction for the SHARES network, and to provide the Federal community a forum for addressing issues affecting HF radio. This body conducts three nationwide readiness exercises each year. The overall exercise objectives are to provide personnel training on operating procedures and message formats, expand SHARES awareness within the Federal emergency response community, and assess the interoperability of new HF technologies.

The SHARES master coordination station KGD-34 operates from the NCC radio operations center. It is configured for voice, data, automatic link establishment, HF to telephone, and HF e-mail operations. The center also maintains two 24-hour HF bulletin board systems and nine HF antennas.

The SHARES HF Radio Program provides emergency communications in support of special operations and all-hazards situations. The most important operation for SHARES

during FY 2005 was in support of the NCC response to Hurricane Katrina. SHARES began pre-activation planning 72 hours prior to Hurricane Katrina making landfall along the Gulf Coast on August 29, 2005. Eight hours prior to landfall, SHARES began full activation with over 500 highly trained volunteer HF radio stations taking part prior to, during, and after Katrina's landfall. SHARES passed approximately 3,000 pieces of emergency message traffic, or situation reports (SITREPS), for the Federal government during and after landfall of the Katrina event. SHARES worked closely with state and civilian emergency communications organizations to assist and facilitate nearly 45,000 pieces of emergency message traffic and SITREPS that were handled during the 10-day period following Katrina. Finally, recognizing the potential impact of Katrina, SHARES was utilized beyond its primary mission of transmitting emergency traffic between Federal entities, to include the collection of information from non-SHARES stations such as requests for assistance, status reports from the impacted area, and property damage. Examples of non-traditional SHARES traffic include:

- Passing calls received from DHS by the NCC indicating that persons were trapped in an attic in Biloxi. SHARES passed this information to one of its stations in Mississippi. The Mississippi station, in turn, contacted the Slidell, Louisiana, State Police, who passed this life-saving information along with the specific address of the personnel needing to be rescued.
- The SHARES Radio Room received a telephone call from a civilian in Maryland saying that students were stranded on the 5th floor of a building at Xavier College in New

Orleans, and needed rescue. SHARES coordinated with the Coast Guard air traffic control unit located in Mobile, Alabama, at the time, who passed this information to the rescue flight helicopter operations in the New Orleans area. As it turned out, the Coast Guard rescued nearly 100 students and nuns from this location due to the information SHARES provided.

In summary, the above events are but a small fraction of what the SHARES HF Radio Program provided to individuals at the Federal, State, and local levels for Hurricanes Katrina, Rita, and Wilma.

During FY 2005, the SHARES HF Radio Program also conducted one of three-planned nationwide SHARES exercise (CONTACT 05-01) on May 11, 2005, with 50 Federal SHARES stations participating and an additional 218 Federally affiliated SHARES stations. The remaining two planned exercises were supplanted by operational events supporting Hurricanes Katrina, Rita, and Wilma.

PLANNING, TRAINING, AND EXERCISE SUPPORT

The PT&E Branch is responsible for ensuring a cadre of skilled civilian and military reservist personnel are qualified and ready to provide emergency response support during crises and emergencies. As part of the implementation of the National Response Plan (NRP), NCS conducted extensive training through the Federal Emergency Management Agency's (FEMA) online training program throughout FY 2005. During FY 2005, the Branch successfully coordinated and performed the following activities:

Emergency Response Training Seminars

Emergency Response Training seminars are a highly visible and successful training program for the NCS. The PHASE 4 course of instruction showcases the NCS priority telecommunications programs, gives an overview of the NRP, and provides the seminar participants an interactive forum to discuss communications resources and challenges that impact emergency response operations. The seminar goals are to increase awareness of the mission and capabilities of the NCS; explain the NCS role as the primary Federal agency for ESF-2 within the NRP; and emphasize the best use of finite industry and Government resources. During FY 2005, seminars were presented to Federal, State and local government, and private industry emergency planners and operators in the National Capitol Region, Federal Region X (Seattle, Washington), Federal Region I (New London, Connecticut), and the Federal Region 2-Caribbean Region (San Juan, Puerto Rico and St. Thomas, Virgin Islands). This effective training outreach program reached a combined audience of approximately 366 attendees.

Emergency Operations Team Training

During FY 2005, internal training was provided to familiarize personnel with ESF-2 responsibilities during Incidents of National Significance. The training included introductory instruction about telephony principles, familiarization with FEMA's mission assignment process, and pre-deployment information for participation in Exercise PINNACLE. In addition, a COOP deployment was conducted with the NCC industry partners to familiarize the team members with the facilities at the NCS

Relocation Site and to familiarize the team members with austere work environment.

Exercises

The OMNCS conducts and participates in both internal and external exercises designed to maintain expert knowledge of, and proficiency in, the management, integration, and employment of NS/EP telecommunications resources. The exercises are conducted in accordance with scenario-driven phases — to include notification, deployment, and operations from designated relocation sites. During FY 2005 OMNCS participated in PINNACLE-05, TOPOFF 3 (Full Scale Exercise), as well as internal tabletop exercises designed to meet the requirements of Federal Preparedness Circular-65. Some of these exercises required the deployment of the NCS essential functions to an alternate site for a period of 2-3 days.

OMNCS INDIVIDUAL MOBILIZATION AUGMENTEE PROGRAM

The OMNCS continues its IMA Program, which is supported through the Department of the Army's IMA Program. The augmentees may be activated and deployed to assist the OMNCS staff, or they may deploy to regional locations as ESF-2 Emergency Communications staff to assist the NCS Regional Managers during national emergency operations and disaster response. The NCS IMA Program provides a valuable resource of skilled Army Reserve personnel to augment telecommunications response activities. During Presidentially declared disasters, the IMA Program provides the NCS with a surge capability to deploy and react to a myriad of situations associated with ESF-2

operations. IMA personnel are often among the first Federal disaster response personnel to reach a disaster scene. Many of these reserve officers are telecommunications professionals in their full-time civilian careers, and are able to apply their skills when responding to Federal emergencies. The IMA Program continues to provide an extremely important and invaluable service to the NCS NS/EP mission at the national and regional levels.

During FY 2005, the NCS Augmentees helped conduct a training session regarding the NCS priority telecommunications programs. The training was presented to a class of Customs Agents attending the Federal Law Enforcement Training Center in Brunswick, Georgia. Additionally, the IMAs were deployed to multiple locations in Federal Region IV (Southeast) and Federal Region 6 (Southwest) to support response and recovery efforts after Hurricane Katrina (August-September 2005) and Hurricane Rita (September 2005).

CONTINUITY OF OPERATIONS

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

A robust and effective COOP testing, training, and exercise program has been developed to determine the validity of the plans and to ensure the operational readiness of the

OMNCS personnel who will respond to the emergency. Through its involvement in DHS' COOP Working Group, the OMNCS participated in the planning and execution of the June 2005 National Capital Region deployed COOP training and exercise event, Exercise PINNACLE-05, for the Federal Executive branch.

CONTINUITY OF GOVERNMENT

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

PRIORITY

TELECOMMUNICATIONS SERVICES

The Priority Telecommunications Services office provides a One-Stop Shop Service (OSSS) enabling customers to acquire NS/EP priority communications information, services, programs, and operations from a single source. The goal of the OSSS concept, illustrated in Figure 2, is to provide an efficient and effective means of managing and supporting the consolidated operations/user support missions and functions of the NCS for priority communications services under any circumstance.

FY 2005 accomplishments include:

- Enhanced Priority Telecommunications Call Center capabilities to increase the call

handling capacity and reduce the number of calls going to voicemail. The Priority Telecommunications Call Center can be reached at 1-866-NCS-CALL (866-627-2255), or in the Washington, D.C. Metro Area at 703-760-CALL (703-760-2255). Normal operating hours are Monday through Friday, 8:00 AM to 6:00 PM Eastern Time.

- Streamlined the web-based application used by all NS/EP points of contact to request priority telecommunications services. Automated the last remaining paper documents required to establish NS/EP accounts.
- Further implemented an intensive marketing and outreach program to expand the user base for the Priority Telecommunications programs/services which is supported by a marketing strategy plan as well as development of various marketing tools using both web-technology and other media as appropriate. Additional personnel were contracted to conduct dedicated outreach activities by geographic region. A further expansion of outreach activities for FY 2005 included a focused effort to pursue briefing opportunities simultaneously with booth deployments at NS/EP conferences.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

The GETS Program is a White House-directed emergency phone service provided by the

NCS in the IAIP Division of DHS. GETS supports Federal, State, local, and tribal government, industry, and non-governmental organization personnel in performing their NS/EP missions. GETS provides emergency access and priority processing in the local and long distance segments of the PSN. It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

FY 2005 GETS activities included:

- Starting from a baseline of 97,000 GETS users and with an objective of adding 6,000 more during FY 2005 for a total of 103,000, the program goals greatly exceeded expectations by reaching 110,000 GETS users, more than doubling the expected increase in participation across the full range of eligible sectors;
- Automated the front end process of arranging sponsorship for, and establishing, GETS accounts, replacing a manually intensive 4-step, paper-driven process with a web-based, single step operation; and
- Streamlined GETS account annual validations by replacing the cumbersome exchange of data files with a simple on-line certification method.

WIRELESS PRIORITY SERVICE

WPS is a White House-directed NS/EP program for priority cellular network access. WPS was approved by the FCC for NS/EP requirements on a call-by-call priority basis. The NCS executes the program on behalf of the EOP.

FY 2005 WPS activities included:

- Starting from a baseline of 11,000 WPS users and with an objective of adding 3,000 more during FY 2005 for a total of 14,000, the program goals again greatly exceeded expectations by reaching over 19,000 total WPS users among the four carriers that provide this capability, almost tripling the expected increase in participation by all sectors for this year; and
- Automation and streamlining efforts achieved for GETS were also applied to WPS operations, helping to minimize administrative workload on the points of contact who manage these accounts and also encouraging greater participation by reducing the management overhead involved with establishing and maintaining WPS service.

TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM

The TSP Program, established by an FCC R&O dated November 17, 1988, provides a regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications services. The FCC

authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments. FY 2005 TSP activities included:

TSP Operations

The OMNCS, in close coordination with the TSP Oversight Committee (OC), continued the day-to-day management of the TSP Program, placing special emphasis on the future direction of the program in a changing homeland security environment.

Currently there are more than 86,000 total active TSP assignments in support of NS/EP communications. During FY 2005, the OMNCS issued more than 2,700 provisioning TSPs to aid in the installation of critical circuits. The TSP user base increased by more than 200 new organizations, with significant new representation from State and local Governments and the private sector, with the Federal Government being one of the largest users of TSP services.

The OMNCS facilitated meetings of the TSP OC, which identifies, reviews, and recommends actions to correct or prevent systemic problems in the TSP Program. Working with the TSP OC, the OMNCS continued to focus its efforts on several operational TSP issues, to include determining appropriate vendor response in relation to the priority levels for TSP assignments. The OMNCS continues with the revalidation of expired TSP assignments and the vendor confirmation process.

TSP Information Technology Solutions

The OMNCS continues to utilize innovative IT solutions in support of TSP Program operations. During FY 2005, the NCS TSP Program Office IT efforts continue to focus on enhancing the usability and data integrity

of the Priority Telecommunications Services, the information system used to support TSP provisioning and restoration, by exploring the development of a web-based application. These enhancements will result in more efficient processes by which OMNCS, TSP users, and telecommunications vendors can input and update information related to crucial NS/EP telecommunications circuits and assets.

**PRIORITY
TELECOMMUNICATIONS
OUTREACH**

The NCS CIP Division had more than 40 trade show exhibits this year across diverse venues within the United States. The program’s goal is to promote awareness of the NCS and its priority telecommunications services to support NS/EP efforts across Federal, State, and local Government, critical infrastructure industries, and other authorized NS/EP organizations. The telecommunications programs that are featured with fact sheets and other media materials are TSP, GETS, WPS, SHARES, and OSSS. CIP services support the initiation, coordination, and restoration of NS/EP telecommunications during national crises or emergencies, and regional disasters. The Outreach Program identifies the ways in which these services can benefit various emergency management organizations and the importance of incorporating the services into their emergency response plans.

The Tradeshow Outreach Program is proving to be an effective way for the NCS to reach out to its current and future customers. The information booth will continue to travel around the country providing critical information to NS/EP audiences about the

NCS and priority telecommunications programs and services. Identified below are the tradeshow events where the booth was displayed during FY 2005.

- Anchorage, AK, September 27-October 1, 2004: Association of State and Territorial Health Officials.
- San Diego, CA, October 15-20, 2004: International City/County Management Association Conference.
- Atlanta, GA, October 19-24, 2004: Emergency Medical Service Exposition.
- Dallas, TX, November 7-11, 2004: International Association of Emergency Managers/Emergency Management Exhibition.
- Las Vegas, NV, November 12-14, 2004: FireRescue Magazine.
- Arlington, VA, November 22-23, 2004: Global Homeland Security.
- Philadelphia, PA, December 5-8, 2004: EPA Region III Emergency Preparedness & Prevention.
- Las Vegas, NV, December 6-9, 2004: National Guard Bureau IT.
- Washington, D.C., January 31-February 1, 2005: American Association of Railroads Railway Security.

<ul style="list-style-type: none"> • Washington, D.C., February 1-2, 2005: Marine Log Maritime & Port Security. • Orlando, FL, February 4-7, 2005: International Disaster Management. • Washington, D.C., February 22-23, 2005: Armed Forces Communications & Electronics Association Homeland Security. • Orlando, FL, March 6-9, 2005: Disaster Recovery Journal — East. • New Orleans, LA, March 14-16, 2005: Cellular Telephone & Internet Association. • Philadelphia, PA, March 18-22, 2005: Emergency Medical Services Today. • New Orleans, LA, March 21-25, 2005: National Hurricane Conference. • Tampa, FL, April, 4-8 2005: DOD Emergency Preparedness Liaison Officer. • Williamsburg, VA, April 5-8, 2005: VA State Emergency Management Association. • Oklahoma City, OK, April 10-12, 2005: American Water Works Association Security. • Baltimore, MD, April 25-27, 2005: NAVIGATOR 2004. • Orlando, FL, April 30-May 4, 2005: National Disaster Medical System. 	<ul style="list-style-type: none"> • Tampa, FL, May 9-13, 2005: FL Governor’s Hurricane (FL GHC/“FL Hurricane”). • Omaha, NE, May 17-22, 2005: Adjutants General Association of the United States. • Long Beach, CA, May 22-25, 2005: United Telecom Council. • Hunt Valley, MD, June 2-5, 2005: International Association of Fire Chiefs HAZMAT. • Los Angeles, CA, June 4-8, 2005: Fire Department Instructors Conference — West. • Kansas City, MO, June 4-8, 2005: Association of Food and Drug Officials. • Long Beach, CA, June 26-30, 2005: National Emergency Number Association. • New Orleans, LA, June 27-29, 2005: Government Symposium on Information Sharing & Homeland Security. • Boston, MA, July 12-15, 2005: Association of State and Territorial Health Officials. • Eureka, CA, August 5, 2005: Humbolt & Del Norte Counties - Post Earthquake/Tsunami warning Emergency Managers Meeting. • Chicago, IL, August 13-18, 2005: GSA/Federal Technology Service Network Services.
---	--

- Denver, CO, August 21-25, 2005: Association of Public-Safety Communications Officials.
- Anchorage, AK, August 28-31, 2005: National Emergency Management Association.
- San Diego, CA, September 10-14, 2005: National Defense Transportation Association.
- Nashville, TN, September 15-20, 2005: American Association of State Highway and Transportation Officials.
- San Diego, CA, September 18-21, 2005: Disaster Recovery Journal — West.
- New York, NY, September 20-21, 2005: U.S. Maritime Security.
- St. Louis, MO, September 25-29, 2005: Academy of Certified Hazardous Materials Managers.

A new technique to reach more NS/EP customers has been to actively pursue articles in NS/EP publications and newsletters. The following articles were published in 2005:

- “Powerful Technology Stronger Response,” February 1, Government Security
- “New Wireless Communications Capability Available to Emergency Responders,” March/April, International Municipal Signal Association Journal
- “National Communications System Offers Important Priority Communications

- *Capabilities to First Responders,* May, International Association of Emergency Managers Bulletin
- “In Emergency, dial NCS,” June, Homeland Protection Professional
- “National Communications System,” August, Association of Public Safety Communications Officials Bulletin
- “NCS Priority Telecommunications Services— Ensuring Essential Communications for First Responders,” October, Emergency Fire/Rescue & Police Magazine

OPERATIONAL ANALYSIS BRANCH

The OA Branch of the CIP Division serves as the focal point for providing relevant and timely analytical products for the NS/EP community to help ensure the availability of telecommunications services despite threats or disruptions to the infrastructure.

Analytical initiatives conducted during FY 2005 include:

Prioritization of Telecommunications

Assets

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* identifies the need to take stock of key assets to reduce the degree of vulnerability resulting from a physical attack on the Nation’s critical infrastructures. In addition, Homeland Security Presidential Directive - 7 (HSPD-7) establishes a national policy for identifying, prioritizing, and protecting critical infrastructure assets.

The OA Branch has developed, and is in the process of implementing, an iterative

methodology that prioritizes telecommunications assets in relation to six consequences described in HSPD-7. These consequences are described as the ability to:

- cause catastrophic health/mass casualties;
- impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- undermine State, and local Government capacities to maintain order and to deliver minimum essential public services;
- damage the private sector's capability to ensure orderly functioning of the economy and delivery of essential services;
- have a negative effect on the economy through the cascading disruption of the critical infrastructure and key resources; and,
- undermine the public's morale and confidence in our national economic and political institutions.

Based on a request from ASIP Stephan to develop a list of the Top 100 "at risk" assets in each critical infrastructure, the OA Branch leveraged its prioritization methodologies and coordinated with the NCS Technology and Programs Division (N2) to assist in developing a list of telecommunications assets. Together, the OA Branch and the N2 Division developed and implemented a flexible methodology to generate a candidate list of 100 telecommunications facilities of

"high interest." This methodology incorporated a two-pronged approach - leveraging both the OA Branch prioritization methodology based on HSPD-7 consequences and the N2 "systems" level analysis, which examined various classes of telecommunications assets, based on users and capacity.

Streamlined Analysis Processes

To improve the response time for future analysis requests, the OA Branch streamlined, standardized, enhanced, and documented its processes for producing its analysis products. The OA Branch developed standardized report formats and identified specific data sets and methodologies for each type of analysis. This streamlining effort enhances the capability of the OA Branch to provide consistent and timely analysis results in as short as 30 minutes during crises, disasters, and other national security events. During FY 2005, the OA Branch implemented these new procedures to provide quick turn-around support for the following events: Hurricanes Frances, Ivan, Dennis, Katrina, Wilma and Rita; the Mount St. Helens Volcanic Eruption; several National Special Security Events (NSSE) (for example, the National Republican Convention, Presidential election and inauguration, and the President's State of the Union Address); and several high threat targets such as the Super Bowl and multiple financial locations in the United States. The OA Branch continually re-evaluates its analysis methodologies to ensure that all data sets and capabilities are relevant and up-to-date with evolving technologies.

Analytic Support for Incident Command and Response

The OA Branch provided analytic support on numerous levels during the increased period

of hurricane activity on the Gulf Coast in 2005. Prior to landfall of Hurricanes Katrina, Rita, and Wilma, the OA Branch conducted a pre-landfall assessment of the telecommunications assets in the paths of each hurricane. This assessment included the potential impact to wireline and wireless assets, GETS switches, WPS tower locations, and point of presence locations. Immediately following hurricane landfall, the OA Branch tracked and analyzed status information from the industry and Government situation reports, to include telecommunications outages as well as location and quantity of deployed assets, status of the telecommunications infrastructure in the affected areas by flooding, dewatering projections, and results of automated call completion and Internet trace routes to the affected areas.

The OA Branch also tracked restoration progress of the telecommunications network in the areas affected by Hurricanes Katrina, Rita, and Wilma. Initially, the OA Branch documented the general approach for an NCS/Industry incident response, to include an overview of authorities, drivers, and coordination processes between NCC representatives and Government. After the landfall of each hurricane, the OA Branch reviewed actions taken by telecommunications service providers and Government before and during each hurricane and analyzed restoration progress of the telecommunications network in the areas affected by the hurricanes.

Regional Characterization

The OA Branch identified the need to perform in-depth telecommunication data gathering and analysis, in advance of an actual event, at a regional level for those areas of the country that historically

command a high interest for NS/EP activities. As a pilot during FY 2005, this effort focused on characterizing communications networks supporting key sites in the National Capital Region. Based on the results of the pilot, the OA Branch is currently working to conduct analyses and characterizations in several other regions to prepare for quick turnaround requests. Several overarching benefits are derived from conducting regional characterizations. As part of the characterization, the OA Branch conducts interviews with site personnel to obtain information on private communications systems and networks supporting specific sites in the area. In addition, completing regional characterizations prepares the OA Branch to respond to scenarios or events and enhances the existing capability to quickly and accurately assess telecommunications impacts.

INFORMATION TECHNOLOGY SUPPORT

In support of NCS users, the IT Branch collected requirements and is working with DHS preparing for an agency move. As the DISA local area network (DISALAN) liaison, the IT Branch represented OMNCS interests in areas such as proposed DISA network enhancements, and the migration of desktops to Win2000.

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

upgrading STU-III phones to Secure Terminal Equipment phones in order to comply with National Security Agency (NSA) regulations. The IT Branch also obtained secure mobile phones in order to be used during national travel and have facilitated an organization-wide re-key due to NSA compromise.

As IT security has gained additional public scrutiny over the past year, the IT Branch has continued to work toward a secure environment and has assisted in efforts for the certification and accreditation of various systems according to DHS and DISA policies. The Branch ensured that NCS systems and practices are maintained within evolving security guidelines. We have led the migration of the NCS homepage server from DOD to DHS network assets. We are currently the acting Information Systems Security Office for NCS until a permanent solution has been decided.

PLANS AND RESOURCES DIVISION

The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, manpower allocations, and other human capital related matters. The Plans and Resources Division exercises authority and ensures accountability over all resources allocated to NCS programs. The Division serves as the interface with the DHS Directorates on financial and acquisition matters; DHS Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The Division conducts analyses and makes

recommendations to the OMNCS on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

Planning

The Planning Team documents the OMNCS leadership's near-, mid-, and long-term strategic direction, vision, and priorities through the development of Business Plans, Performance Plans, Future Year Homeland Security Planning documentation, Advanced Acquisition Plans, and budgetary expertise to strategic planning efforts.

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

Financial Management

The Financial Team provides the overall fiscal direction to the OMNCS for day-to-day operations. The Financial Team develops and produces all PPBS-related documentation for the OMNCS, including documentation for program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits.

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

availability of funds and compliance with fiscal laws, regulations, and policies.

Acquisition Management

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

CUSTOMER SERVICE DIVISION

NATIONAL COMMUNICATIONS SYSTEM COMMITTEE OF PRINCIPALS/COUNCIL OF REPRESENTATIVES

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

As an interagency body, the COP serves as a forum for the member departments and

agencies to exchange ideas, coordinate interagency activity, and form recommendations on current and emerging telecommunications issues to be delivered directly to the Manager of the NCS, the Secretary of Homeland Security, and the President. Each Principal on the COP provides the position of its parent organization on NS/EP issues. The COP is also responsible for issuing comments and recommendations on current and prospective NCS programs to the NCS; the Homeland Security Council (HSC); the National Security Council (NSC); the Office of Management and Budget (OMB); and the Executive Agent. Additionally, the COP performs any other duties that may be assigned by the President or his authorized designee.

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

In FY 2005, the COP provided recommendations on HSPD 7 — *Critical Infrastructure Identification, Prioritization, and Protection* [regarding the establishment of the Telecommunications Government Coordinating Council (TGCC) Working Group and the CSCC.] The TGCC Working Group is responsible for coordinating the implementation of the NIPP and the corresponding Telecommunications Sector Specific Plan that will outline the strategy for coordination across the U.S. Government and between Government and the telecommunications sector.

The COP also submitted comments for the revision of the NIPP, the base plan detailing how DHS and its partners jointly provide protection of the Nation's critical infrastructure and key resources. Additionally, the COP initiated a process to better implement recommendations received from the President's NSTAC.

Council of Representatives

The Council of Representatives (COR) is a permanent subordinate group of the COP, established by the COP Bylaws to assist the COP in the execution of its assigned responsibilities. The COR membership consists of the 23 departments and agencies that make up the COP. COR members participate in dedicated working groups to conduct special studies and make recommendations to the COP on matters concerning NS/EP telecommunications.

Critical Facilities Working Group

In January 2003, the NCS COP established the Critical Facilities Working Group (CFWG) to study the use of facility redundancy and diversity for Federal departments and agencies encountering difficulty in procuring highly reliable telecommunications services for their NS/EP mission essential functions. The objectives of the CFWG were to define and identify options for facility diversity that may improve the reliability of NS/EP communications, and recommend a strategy for enhancing the reliability of Federal telecommunications.

In its final report, the CFWG evaluated the options available to achieve facility diversity and redundancy. The CFWG also recommended steps individual Federal departments and agencies could take to improve the reliability of their essential telecommunications services and methods for

improving the reliability of essential NS/EP communications services across the Federal Government.

The NCS forwarded the CFWG's report to the EOP for its consideration in July 2004.

Continuity Communications Working Group

In June 2004, the Continuity Communications Working Group (CCWG) began meeting with the purpose of developing a Continuity Communications (CC) Federal Enterprise Architecture Framework (FEAF) and overseeing the development of a CC Federal Enterprise Architecture (FEA) to support the performance of Federal Executive Branch (FEB) minimum essential functions under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The DOD serves as CCWG chair and FEMA, serves as vice-chair.

The group defined a set of requirements and in October 2004, established a CC Enterprise Architecture (EA) Program Office, with a mission to:

- Document existing CC requirements;
- Translate requirements into actionable performance criteria;
- Normalize existing FEB CC EAs;
- Develop a single, common CC EA;
- Determine and document where shortfalls exist and planned capabilities overlap; and

- Make recommendations to effectively implement FEB CC requirements.

Throughout the year, the CCWG completed the following products :

- *Continuity Communications Federal Enterprise Architecture Strategic Vision* — provides the overarching objectives, general operational concept, and key technical characteristics for the CC FEA. The COP approved the document on November 23, 2004;
- *Continuity Communications Requirements and Performance Criteria* — describes the minimum essential requirements for CC based on existing policy and translates the requirements into actionable performance criteria. The CCWG delivered the document to the COP on January 20, 2005, and the COP approved it on January 27, 2005;
- *U.S. Federal Executive Branch Continuity Communications Enterprise Architecture Roadmap* — defines timelines, milestones, and responsibilities for developing the CC FEAF and CC FEA. The CCWG delivered the Roadmap on March 14, 2005, which the COP approved;
- *Continuity Communications Enterprise Architecture Framework* — integrates and normalizes existing FEB CC FEAs by defining a common approach for departments and agencies to develop a plan for implementation of the CC FEAs. The document was completed on May 31, 2005, and
- *U.S. Federal Executive Branch Continuity Communications Enterprise Architecture*

(Initial Report) — defines an integrated and evolutionary telecommunications architecture that meets current and future Federal Government continuity communications requirements. The CCWG delivered the final document to the COP on August 31, 2005. The COP subsequently granted its approval by electronic vote.

Priority Services Working Group

The NCS COP established the Priority Services Working Group (PSWG) at the December 16, 2003, COP Meeting. The PSWG includes membership from a broad spectrum of agencies that participate in the COP and the COR. Mr. Kenneth Moran, FCC, chairs the working group. The PSWG reports to the COP on the status of working group activities and facilitates an open discussion with COP members on the work of the PSWG and its findings.

The PSWG scope of work called for the group to conduct: (1) an evaluation of current priority service programs; (2) an examination of outreach efforts; (3) an assessment of cost issues; and (4) an analysis of the potential impact of future technologies and their bearing on priority telecommunications programs. The PSWG’s focus included three NS/EP priority communications programs: (1) GETS, which provides emergency access and priority processing in the local and long distance segments of the public switched telephone network; (2) TSP, which provides service vendors with an FCC mandate for prioritizing service requests by identifying those services critical to NS/EP; and (3) WPS, which provides priority cellular network access. The group’s initial study examined TSP according to the four tenets of its scope of work.

In September 2005, the PSWG hosted briefings on priority telecommunications services from industry and Government experts. The group toured the Maryland, Virginia, and Pennsylvania EOC to gain a more detailed understanding of how EOCs could utilize priority service programs to aid in crises. They also gathered and discussed information on each major telecommunications service provider's TSP operating procedures, among other activities. The working group prepared a memorandum for distribution to all NCS member departments and agencies to determine the level of priority services coverage needed by each department or agency, and developed a white paper on the need for expanded use of DHS grants for State and local responders.

Most recently, the working group analyzed TSP participation and funding levels at Federal, State, and local departments and agencies. Based on the information gleaned from discussions with TSP service providers and experts at various Government agencies, the PSWG drafted a report of TSP recommendations, which was submitted to the TSP OC for comment on July 22, 2005. The *Final Report on TSP* will next be sent to the COP and COR for review and approval. Upon approval, the report will be forwarded to the NCS, DHS, and the EOP.

Moving forward, the working group plans to examine similar participation and funding issues associated with GETS and WPS, and to make recommendations regarding strategies to improve the visibility and participation levels of both priority service programs.

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

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

The NSTAC held its 28th Annual Meeting on May 11, 2005, in Washington, D.C., at which time the NSTAC Principals and senior Government officials reviewed the activities of the past cycle and discussed emerging issues for consideration during the NSTAC XXIX Cycle. The NSTAC also met quarterly via conference call. Topics discussed included network convergence, telecommunications and electric power interdependency, and identity authentication issues.

Industry Executive Subcommittee

During FY 2005, the NSTAC's Industry Executive Subcommittee (IES) continued to identify communications issues critical to NS/EP activities for consideration by the NSTAC Principals. In support of the NSTAC, the IES addressed a variety of issues, including: trusted access to key infrastructure facilities; the provisioning of NS/EP services over the NGN; telecommunications and electric power interdependency; the evolving role of the NCC; NSTAC outreach efforts; research and development (R&D) issues; and legislative and regulatory issues. Specific subgroup activities and the results of their analysis, work, and subsequent NSTAC

recommendations to the President are discussed further below.

The IES also received several briefings during the year, including an overview of homeland security issues facing the 109th Congress, a classified briefing on the U.S.

Telecommunications Infrastructure Security Study undertaken by Johns Hopkins University, an overview of the termination of cellular communication services in New York and New Jersey tunnels after the July 7, 2005, London bombings, and a briefing from the Federal Government Leadership Forum on assured communications and information sharing.

Trusted Access Task Force

The NSTAC established the Trusted Access Task Force (TATF), following the NSTAC XXVI Meeting, to address the Administration’s concerns that the telecommunications infrastructure may be vulnerable because trusted physical access to critical telecommunications facilities is routinely granted to individuals who require access to telecommunications assets to perform their jobs without ensuring that the individual will not pose a threat to the facility or the telecommunications infrastructure at large. Specifically, the TATF was charged to help mitigate potential threats to the telecommunications infrastructure by working with Government representatives, at the Federal, State, and local levels to develop guidance for the creation of national standards for security personnel screenings and verification/credentialing procedures for key personnel.

The TATF, in its *Screening, Credentialing, and Perimeter Access Controls Report*, concluded that no standard process exists for the private sector

to ensure personnel accessing critical telecommunications facilities do not pose a threat to NS/EP communications.

Furthermore, the task force asserted that Government can assist industry with its background screening challenges by allowing industry to leverage the resources available to the Federal Government, specifically the Transportation Security Administration (TSA) within DHS, for conducting screening investigations.

The TATF also concluded that physical protection of the infrastructure must include protecting NSSE sites and consequently, developed a pilot screening program to pre-screen a group of industry employees who required access to physical sites or critical information during NSSEs to Federal terrorist lists and Government databases. The pilot was very successful and industry continues to work with Government to share information and pre-screen NSSE participants.

The *Screening, Credentialing, and Perimeter Access Controls Report* provides several recommendations directing Federal

departments and agencies to take the following actions:

- Implement and support a standardized screening process for industry to voluntarily conduct screenings on persons who have regular and continued unescorted access to critical telecommunications facilities (such as, switching facilities), including telecommunications employees and vendors, suppliers, and contractor staff, including:
 - Modeling such a program after the current TSA program

<p>by including different relative background investigation levels for various facilities and personnel types;</p> <ul style="list-style-type: none"> • Partnering with DHS, through TSA, to, upon request from industry, conduct screenings for industry personnel working at critical private telecommunications facilities; and • Working with the Network Reliability and Interoperability Council to develop industry best practices defining specific criteria for determining which telecommunications employees should be subject to screenings. • Make available a standard tamper-proof, certificate-based picture identification technology to enable the positive identification of screened individuals at critical sites and to support both physical and logical access for such individuals to critical telecommunications facilities and related networks and information by building on the ongoing work of the GSA Federal Identity Credentialing Committee. • Build on the recommendations in the Communications ISAC report, <i>Preparing for a National Special Security Event</i>, to develop a national plan for controlling access at the perimeter of an NSSE or a disaster area. To facilitate the development of a national perimeter access plan for incorporation in the NRP, the Government should continue to 	<p>support the screening program coordinated by the NCC ISAC with screenings facilitated by DHS and the U.S. Secret Service.</p> <ul style="list-style-type: none"> • Partner with the ISACs across infrastructures to implement screening, credentialing, and access control policies mirroring those recommended for the telecommunications infrastructure for all critical infrastructures. <p>The TATF sunset during the NSTAC XXVIII cycle.</p> <p>Next Generation Networks Task Force</p> <p>The convergence of wireless, wireline, and IP networks into the global NGN is causing a shift in the way that Governments and critical infrastructures will meet their needs for NS/EP communications today and in the future. At the NSTAC XXVII Meeting held on May 19, 2004, the NSTAC Principals agreed to create a task force to engage subject matter experts (SME) in an examination of NS/EP requirements and emerging threats to the NGN.</p> <p>Accordingly, the NGNTF was created to:</p> <ul style="list-style-type: none"> • Agree upon a high-level description of the NGN’s expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely; • Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and
---	---

<p>accountability among network participants and network layers will work; and</p> <ul style="list-style-type: none"> • Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements. <p>The NSTAC Principals also agreed that the NGNTF should explore international issues, both in terms of NS/EP functions that must be provisioned internationally as well as international threats to the NGN. The NGNTF assembled a group of SMEs and Government stakeholders in August 2004 to discuss and determine the key issues for the NGNTF to examine. As a result of the meeting, the group identified five fundamental issues as essential to the work of the task force: (1) a description of the NGN; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. The NGNTF created working groups to address each of these areas.</p> <p>Remarks from Government stakeholders raised questions regarding how NS/EP communications would be affected by the transition to the NGN. Of particular interest were efforts that could be taken immediately to preserve or enhance NS/EP communications for the future. The NGNTF formed the Near Term Recommendations Working Group (NTRWG) to examine near-term opportunities for using existing technology to improve the security and availability of NS/EP communications on converging networks. The NTRWG also examined areas needing Government involvement in the near term because of the immediacy of events such as NGN standards</p>	<p>and systems development activities that may be proceeding without consideration of NS/EP needs.</p> <p>Based on the NTRWG’s analysis of near-term threats and opportunities, the NSTAC offered the following recommendations to the President in its <i>Near Term Recommendations Report</i>:</p> <ul style="list-style-type: none"> • Use existing, appropriate cross-Government coordination mechanisms to track and coordinate cross-agency NGN activities and investment; • Explore the use of Government (civilian and DOD) networks as alternatives for critical NS/EP communications during times of national crisis; • Use and test existing and leading-edge technologies and commercial capabilities to support NS/EP user requirements for security and availability; • Support the development and use of identity management mechanisms, including strong authentication; • Study and support industry efforts in areas that present the greatest NS/EP risks during the period of convergence, including: <ol style="list-style-type: none"> (1) gateways; (2) control systems; and (3) first responder communications systems; • Review the value of satellite systems as a broad alternative transmission channel for NS/EP communications;
--	---

<ul style="list-style-type: none"> • Participate more broadly and actively in the NGN standards process in partnership with the private sector in the following areas: web services; directory services; data security; network security/management; and control systems; and • Focus on developing cohesive domestic and international NS/EP communications policy and conduct inter-governmental discussions on NS/EP communications. 	<p>vulnerabilities from an NS/EP perspective.</p> <p>The VTMWG, ESWG, and IMWG are continuing to finalize their findings and recommendations that focus on issues such as priority for NS/EP communications over the NGN, alternative communications, software and hardware assurance, and identity management.</p> <p>Other recent NGNTF activities include co-hosting the second SME Meeting, with the National Coordinating Center Task Force (NCCTF), on August 30, 2005. The SME Meeting brought together Government stakeholders and industry experts to discuss incident management in the NGN. Participants deliberated over incident management in the converged environment and how industry and Government can cooperate during an NGN-related incident. Attendees received briefings on Verizon's recovery activities following September 11, 2001, and on the mission and functions of the Homeland Security Operations Center. They also verified the work to date of the ESWG, SURWG, and VTMWG, and worked through an incident management scenario with NGN implications.</p>
<p>The remaining four NGNTF working groups continued their work into the NSTAC XXIX cycle and include:</p>	<p>The NGNTF plans to complete its final report and recommendations prior to the NSTAC XXIX Meeting in May 2006.</p>
<ul style="list-style-type: none"> • The Scenarios and User Requirements Working Group (SURWG), which worked to develop scenarios for NS/EP communications on the NGN, including Presidential-level communications, critical Government networks, public safety, continuity of Government, industry/critical infrastructure user, and non-critical services; • The Incident Management Working Group (IMWG), which developed recommendations concerning the concept of operations for an NS/EP incident on the NGN; • The End-to-End Services Working Group (ESWG), which developed an explanation of how the NS/EP functional requirements may be met on the NGN; and • The Vulnerabilities and Threat Modeling Working Group (VTMWG), which considered relevant threats and 	<p>National Coordinating Center Task Force</p> <p>The NCCTF was formed at the request of Mr. F. Duane Ackerman, BellSouth and NSTAC Chair, following the October 21, 2004, NSTAC Principals' Conference Call. The NCCTF was tasked with studying the long-term direction of the NCC, including but not limited to: (1) where the NCC should be in one year, three years, and five years; (2) how the NCC</p>

should continue to partner with Government; (3) how the NCC should be structured; and (4) how the new DHS Sector Coordinating Council approach could impact the NCC.

The NSTAC believes the NCC must reconsider its structure, organization, and approach to keep pace with rapid legal and regulatory changes in the homeland security environment, particularly in light of the NCC's unique role coordinating the restoration and provisioning of NS/EP telecommunications services and facilities during all-hazards events, from natural disasters to terrorist attacks.

The NCC currently holds responsibility for three distinct missions:

- Serving the White House and NCS member agencies through its NS/EP mission;
- Serving DHS through its CIP mission; and
- Fulfilling information sharing requirements through the Communications ISAC.

The task force has worked to reconcile the NCC's NS/EP and CIP missions, affirming a definition of NS/EP communications that includes CIP activities, and to resolve NCC/ISAC membership issues. The task force also agreed that the telecommunications and information technology industry representatives should make an effort to work closely together towards an anticipated convergence of the industries. Additionally, the NCCTF discussed ways in which information sharing within the NCC can be improved. The task force agreed that

there should be a shift toward proportional information sharing to include more Government-to-industry and industry-to-industry information sharing, in addition to industry-to-Government sharing. Industry members of the NCC expressed their desire to be involved in NCS risk analyses of industry assets, which would assist the NCS in producing more accurate assessments. Other issues under discussion by the NCCTF include the NCC's role in international mutual aid agreements.

The NSTAC expects to complete its NCC report prior to the NSTAC XXIX Meeting in May 2006.

Telecommunications and Electric Power Interdependency Task Force

While the interdependencies between the telecommunications and electric power infrastructures have long been recognized and discussed within and between the sectors, increased attention to the situation recently arose as a result of elongated power and telecommunications outages in the wake of the hurricane season of August and September 2004 in the southeast region of the U.S. Mr. Ackerman highlighted his concerns related to these increasing sector interdependencies in his address to the participants at the Research and Development Exchange (RDX) Workshop in Monterey, California, in October 2004, during which he noted the need for enhanced battery technology. In addition, he stated that, as the network becomes increasingly distributed, issues of reliability and ease of communication and coordination between telecommunications and electric power industries will become ever more important during natural disasters and/or terrorist incidents.

In December 2004, the NSTAC's IES recommended the NSTAC convene a scoping group to determine the need to establish a task force to investigate any NS/EP issues associated with the interdependencies between the telecommunications and electric power sectors. Following development of a report by the scoping group, the NSTAC decided to create the Telecommunications and Electric Power Interdependency Task Force (TEPITF) to continue the examination of these interdependencies. The task force's membership includes representatives from the telecommunications and electric power infrastructures in the U.S. and Canada. The task force is also reaching out to include and leverage the ongoing efforts from other bodies such as Industry Canada, the IEEE, the NCS, and National Laboratories to augment its work.

The TEPITF was tasked to examine both the near-term and long-term interdependency issues between the two sectors. Suggested near-term topics to address included the need to improve the coordination of people and processes involved with situational awareness, priority restoration, and information-sharing, while the long-term issues included the effects of technology changes, such as the evolution of the NGN, on interdependency vulnerabilities, as well as the need to develop initiatives to mitigate such vulnerabilities.

The task force sponsored a one-day workshop in August 2005 which brought together representatives from the telecommunications and electric power industries to discuss lessons learned from prior interdependency-related exercises and historical incidents. The information gathered at this workshop has been used to establish the baseline set of issues to be discussed and debated by the task

force. In addition, task force members have received briefings from DHS representatives with experience participating in exercises, including PINNACLE and TOPOFF 3, to inform their debate.

The task force has focused its initial efforts on completing its near-term work and estimates it will transition onto consideration of long-term issues early in 2006.

Research and Development Task Force

On October 28-29, 2004, the Research and Development Task Force (RDTF) of the President's NSTAC conducted its sixth RDX Workshop titled, *A Year Later: Research & Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness*. This Workshop, held in Monterey, California, reconsidered the R&D issues associated with trustworthy NS/EP telecommunications addressed at the 2003 RDX Workshop and examined progress made, unfinished work, and new challenges. Specifically, participants focused on major cyber and software, physical, human factor, and integration research issue areas and discussed the need for information exchange and collaboration efforts within the R&D community.

Mr. Richard M. Russell, Associate Director of the White House OSTP, and Dr. Charles E. McQueary, Under Secretary for Science and Technology (S&T), DHS, presented keynote addresses during the opening plenary session of the RDX Workshop. Mr. Russell highlighted the importance of a trusted exchange of information between the public and private sectors and identified a number of research

topic areas that the OSTP believed deserve increased attention and investment.

Dr. McQueary discussed several telecommunications and cyber-related infrastructure protection initiatives within the S&T Directorate and emphasized the value provided by the RDX Workshop to provide guidance to the Government on critical needs and to influence the strategic planning and decision making processes.

During the two-day event, participants also heard from leaders in industry and academia and engaged in a facilitated dialog including both plenary and breakout sessions. From these sessions, five major findings regarding trustworthiness of NS/EP telecommunications and information systems emerged:

- Collaboration is essential for successful R&D initiatives;
- Ubiquitous, interoperable identity management and authentication systems must be embedded in future networks;
- A need exists to examine interdependencies between critical infrastructures, especially the implications of the intersection between telecommunications and electric power;
- A need exists to influence business drivers and policy levers, and provide other incentives to promote a culture of security; and
- Agreement on a common agenda is critical to achieve progress in trustworthiness R&D.

In December 2004, the RDTF reviewed the findings from the RDX Workshop and identified the development of R&D collaboration tools and the study of authentication and identity management as issues meriting further attention from the task force.

In January 2005, the task force conducted a panel discussion with representatives from VeriSign, the GSA, and the National Institute for Standards and Technology on authentication and its impact on NS/EP as a follow-up to concerns expressed on the issue at the RDX Workshop. The issue was examined again at the task force's July 2005 Meeting when the group received a briefing from a DOD representative on the use of federated identity management solutions to meet the Department's authentication and identity management requirements.

Legislative and Regulatory Task Force

On March 10, 2005, the Legislative and Regulatory Task Force (LRTF) completed its examination of the national and homeland security implications associated with the availability of open source critical infrastructure information on the Internet. The examination was initiated in FY 2004 at the request of the NSTAC Principals and the ASIP. The tasking came in response to a discussion, led by one of the NSTAC Principals, on an industry analysis of open source infrastructure information, which concluded that information regarding network architecture, local exchange routing guides, connectivity, and fiber-optic routing data is publicly available on the Web sites of numerous Government agencies, universities, telecommunications providers, and State and local Government regulatory agencies. In

response, the Principals agreed that the NSTAC should review its Web publishing practices and policies, and individual companies should be encouraged to conduct similar reviews. In addition, the ASIP, DHS, encouraged a review of available information with an emphasis on data required by Federal, State, and local regulators. During the January 2004 IES Meeting the IES tasked the LRTF with analyzing the availability of open source infrastructure information on the Internet.

Throughout FY 2004, the LRTF examined the Web publishing practices and policies of Government Web sites, telecommunications carrier Web sites, and third-party Web sites. The examinations indicated that significant critical infrastructure information is available on the Internet through industry, Government, and third-party aggregator Web sites that could be easily used by a terrorist or adversary to launch an attack on the U.S. telecommunications infrastructure. In FY 2005, the NSTAC assessed its findings and made recommendations to send to the President. Specifically, the LRTF recommended that:

- The Federal Government develop and adopt Web publishing and access guidelines incorporating provisions that protect industry-sensitive critical infrastructure information provided to the Government;
- Federal departments and independent agencies be encouraged to adopt Web publishing and access guidelines; and
- The appropriate departments and agencies be directed to promulgate Web publishing and access guidelines for dealing with sensitive but

unclassified critical infrastructure information.

As follow-on to these recommendations, the NSTAC Principals tasked the LRTF to undertake an examination of open source infrastructure information on academic Web sites. The LRTF reviewed the October 2003 American Association of University Professors' Special Committee's report, *Academic Freedom and National Security in a Time of Crisis*. The LRTF concluded that the issue includes complicated and controversial issues related to academic freedom and national security, including constitutional issues such as freedom of speech, which go beyond the scope of the NSTAC Charter. For this reason, the LRTF developed a summary report to the NSTAC Principals explaining that the issue is outside the scope of the NSTAC and should not be further examined.

The LRTF also continued to examine NS/EP concerns associated with implementation of the *Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act*. The task force received a briefing from Ms. Wendy Howe, Office of SAFETY Act Implementation, DHS, on the Department's efforts to revise the SAFETY Act regulations and application kit. The LRTF agreed to continue to examine the issue of SAFETY Act implementation and, if the task force identifies specific issues of concern relating specifically to telecommunications NS/EP services, the LRTF will develop recommendations to the President.

Finally, the LRTF initiated an examination of NS/EP issues associated with proposed amendments to the Defense Production Act (DPA) and E.O. 12919, *National Defense Industrial Resources Preparedness*, which resulted from an Interagency Review of the DPA

intended to update the DPA to include homeland security. The LRTF developed a list of concerns with the proposed amendments, and if appropriate, will develop recommendations to the President.

NSTAC Outreach Task Force

The NSTAC Outreach Task Force (NOTF) operates to foster the exchange of information between key NSTAC stakeholders from both industry and Government on telecommunications-related NS/EP activities. 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 2005 by:

- Providing briefings on NSTAC reports and recommendations to key stakeholders (including regular briefings to the NCS COP/COR, and meetings with several agencies in the EOP);
- Updating the NSTAC video;
- Participating in the GSA/Federal Technology Service Conference;
- Participating in the United States Telecom Association’s Telecom 2005 Conference; and
- Meeting with officials from the U.S. Northern Command and North

American Aerospace Defense Command.

Each new cycle brings with it a new focus for the NSTAC in the protection of our Nation. The NOTF, as a standing task force, will continue to work with key stakeholders to ensure participation in NSTAC efforts as well as awareness of NSTAC work.

SPECIAL PROJECTS

HSPD-7 Coordinating Councils

The CSCC and the TGCC were established in the late spring 2005, to facilitate inclusive organization and coordination of the policy development, infrastructure-protection planning, and plan implementation activities within the sector. Specifically, the CSCC and GCC will undertake activities to assist the communications sector in finalizing and implementing the Telecommunications Sector Specific Plan annex of the NIPP. Activities will include: broad-based planning; development of suggested practices and evolution of these practices over time to best-practice standards; promulgation of programs and plans; and development of requirements for effective information sharing, R&D, and cross-sector coordination.

NCS Issuance System

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

The following is a status of issuances addressed during FY 2005:

These Issuances are in the EOP, awaiting consideration by the Assistant to the President for National Security Affairs prior to signature by the Assistant to the President for Science and Technology and the Director of OMB:

- NCS Directive 1-1, *NCS Issuance System*;
- NCS Directive 1-2, *NCS Membership*; and
- NCS Manual 1-2-1, *NCS Committee of Principals*.

The following Issuances are in development:

- NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* (In coordination at EOP prior to consideration by the Assistant to the President for National Security, the NCS Executive Agent, the NCS Manager, and the NCS COP);
- NCS Manual 3-10-1, *Required Minimum Continuity Communications Capabilities*;
- NCS Handbook 3-10-1, *NCS Backup Dial Tone Project — Abridged Route Diversity Methodology Procedure*;
- NCS Directive 3-11, *Government Emergency Telecommunications Service*;
- NCS Manual 3-11-1, *Government Emergency Telecommunications Service Manual*; and
- NCS Directive 3-12, *Wireless Priority Service*.

The following Issuances were revised as recommended by the NCS COP from its PSWG Administrative Changes Report for Top-Level NCS Priority Services Guidance:

- NCS Directive 3-1, *Telecommunications Service Priority* (Currently awaiting potential changes from OSTP); and
- NCS Directive 3-3, *Shared Resources (SHARES) High Frequency Radio Program* (Returned to internal coordination process for possible changes recommended as a result of Hurricane Katrina After Action Report).

NCS Communications and External Affairs

The NCS answers inquiries from national media outlets such as the major television networks, national wire services, leading national newspapers, Government-focused telecommunications magazines, and specialized telecommunications periodicals. The NCS coordinates all inquiries with the communications director for the DHS IAIP Directorate to ensure that the Department approves all requests for interviews and information about the NCS.

Inquiries generally focused on the NCS emergency preparedness programs and their role with the DHS, but peaked during the NCS efforts during Hurricane Katrina and the early stages with Hurricane Rita. Inquiries focused on the NCC and its Communications ISAC, the WPS program, GETS, TSP program, the SHARES High Frequency Radio Program, and the NCS mission to work with industry in support of emergency communications.

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

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

Outreach

The NCS continues to spearhead an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences. NCS representatives attend and participate in Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and CIP. Since the inclusion of the NCS in DHS in March 2003, there have been numerous opportunities for NCS leaders to participate in panel discussions and other public events to promote and describe the NCS, DHS, and its critical role in homeland security and NS/EP communications.

Web Sites

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

sites of its 22 Federal agency members into its site redesign, as well as upgrading two DHS Intranet sites — DHS Interactive and DHSOnline.



IV

NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF MEMBER ORGANIZATIONS



DEPARTMENT OF STATE (DOS)

NS/EP Telecommunications Mission

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

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

Telecommunications Staff Organization

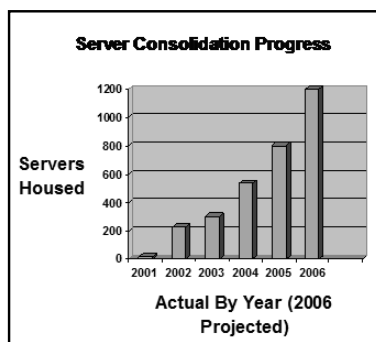
DOS manages its telecommunications through the Bureau of Information Resource Management and the Diplomatic Telecommunications Service Program Office.

Current/Ongoing NS/EP Telecommunications Activities

IT Facilities Consolidation

The Department continues to progress on consolidating its enterprise server

operations. This project was started in mid-fiscal year (FY) 2001 with the strategic goal of establishing a comprehensive "server farm" concept for consolidating information technology (IT) facilities and processing resources, such as servers, databases, and applications into centrally managed facilities and systems. The benefits are savings in manpower and facilities throughout the Department, improved security, data integrity, operational reliability, technical support, and around-the-clock availability. As of 2005, the server farm infrastructure (also termed ESOC — Enterprise Server Operations Center) now consists of two main ESOCs, providing Department-wide systems backup and recovery, and serving as a continuity of operations centers for key business and mission critical initiatives such as the Department's financial service center in Charleston and the bureau of Consular Affairs' VISA and Passport name check lookup system. Based on existing growth trends, upwards of 1,200 servers are expected in the ESOC by the close of FY 2006.



Global Information Technology Modernization Program

The Global IT Modernization (GITM) program, which was initiated on

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

Interagency Collaboration

The Department is committed to the enhancement of inter-agency communications and collaboration. It is pursuing several complementary approaches toward that objective: acceleration of a modern messaging and archiving system — State Messaging and Archive Retrieval Toolset (SMART); expanded use of Open Source Information System (OSIS) and Secret Internet Protocol Router Network (SIPRNet). DOS coordinates with other agencies through the Inter-Agency Collaboration Working Group chaired by Christine Liu, Deputy Chief Information Officer, Acting, for



DEPARTMENT OF STATE (DOS) continued

Business, Planning and Customer Service.

The Department has expanded greatly the publication of classified reporting on SIPRNet; more than 175 embassies and bureaus maintain pages linked from its gateway site at <http://www.state.sgov.gov>. The Department is also moving ahead to improve communications and collaboration among agencies via the OSIS. OSIS is a virtual private network for securely transmitting unclassified information between agencies. The Department is increasing the amount of information it makes accessible through its site on the OSIS network, including consular data, administrative data, and information on State Department regulations and administration of embassy activities. In addition, the Department uses web log technology provided by OSIS to underpin a growing number of communities of practice based on country, regional or functional interests of members of the U.S. Government foreign affairs agencies. Both to save resources and to improve the means for interagency knowledge sharing and collaboration, the Department is vigorously pursuing creation of a Foreign Affairs Virtual Environment that would build on existing agency networks and authentication programs to enable members of foreign affairs agencies to access their own and each others' networks at home and abroad.

The Department and the Agency for International Development have established Joint Management Council to build a common management foundation. As a result, the two agencies are working toward common

use of networks, consolidation of technical and operational support, development of a joint Enterprise Architecture, and collaboration on Knowledge Management strategies. We are participating in each other's IT Capital Planning and Investment processes and developing joint Office of Management and Budget Exhibit 300 submissions for major IT projects.

eDiplomacy

The office of eDiplomacy is charged to enhance the Department's leadership in American diplomacy by promoting a knowledge-sharing culture and by putting the power of innovation in technologies and practices at the fingertips of the individual user. This plan provides for initial implementation of a new enterprise search engine by early 2005 as the first step in a phased approach to introducing an Enterprise Information Portal (EIP). The search engine implementation project is already well underway, having implemented basic functionality of the Autonomy search engine on an enterprise-wide basis (available via the iNet intranet page).

The enterprise-wide search engine project's intent is to leverage existing technological assets and resources to implement a robust, accurate, and feature-rich search capability across the enterprise. This plan provides for the continued, expanded implementation of a new enterprise search engine to replace the former search tool's basic features and functions, index more documents and sites, and return more relevant results. The search engine implementation project is well into its second phase, which includes completing the installation of "general" search

features (such as, non-personalized, basic features), conducting two pilots to explore advanced features with expanded coverage reaching many more Department intranet data sources; and implementing non-personalized advanced search features (such as additional sorting options, filters/search parameters to limit results).

The search engine implementation is considered a first step toward implementing an enterprise-wide portal. Updating the search engine was both a proof of concept for the kind of services that a portal would be able to provide, and a first step toward drawing users to the central iNet page where links to Departmental information reside, as a way to encourage and acclimate users to a single gateway to Department information. Ultimately, eDiplomacy will work with stakeholders to then establish an EIP project. Completion of this plan would serve Department and Federal strategic objectives such as ready access to foreign affairs applications and information, knowledge sharing and collaboration, access to expertise, and joint management and knowledge leadership with USAID. It will complement other programs by integrating the broad array of services provided through those efforts.

Secure Voice Program

The Department completed the Secure Terminal Equipment (STE) for Secure Telephone Unit (STU) replacement in June 2004. We have deployed more than 4,800 STE units worldwide. The program is continuously receiving replaced STU's for destruction or transfer to the National Security



DEPARTMENT OF STATE (DOS) continued

Agency. The Department continues to evaluate newly introduced Secure Voice technology. Secure mobile telephones are being evaluated and fielded. We are supporting and fielding secure radios to Embassy Baghdad and the Regional Embassy Offices in Iraq. The Department recently procured replacement units for the Secretary of State's mobile secure voice devices patterned after the White House Communications Agency Presidential secure voice support. The Department is engaged in the Operations and Maintenance phase of the STE program.

Anti-Virus Program

The Department's Anti-Virus program has intercepted and destroyed over 4,000,000 virus attacks in the calendar year 2005 to date. More than 15,000,000 pieces of spam have been stopped in addition. This program has resulted in no major network outages during 2005 due to malicious code. A combination of robust network design, perimeter and desktop anti-virus tools has resulted in a very successful program. In an effort to educate users and to prevent unknowingly introduction of malicious codes, nearly 60,000 Anti Virus software CDs have been provided to the Department employees for home use during the same period. This proactive measure controls virus incidents from emails or documents prepared by employees at home. The Anti-Virus program is now deploying new desktop software that will also scan for adware and spyware in addition to malicious codes thus further protecting the Department of State IT infrastructure.

Communication Security (COMSEC) Modernization

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

The Department has implemented the NSA mandated Electronic Key Management System. The Department's primary communications hub, Beltsville Management Center, has been completely converted from paper based to electronic COMSEC keying material. The migration over the next two years to full electronic keying material distribution over the existing

Department network infrastructure will provide the capability to distribute keying material in near real time without the risks and time associated with using the Diplomatic courier system.

Communication Security (Public Key Infrastructure)

The Department is currently operating a Public Key Infrastructure (PKI) at the Federal PKI Policy Authority (FPKIPA) high assurance level. In a team effort, the Diplomatic Security and Information Resource Management Bureaus, have issued over 26,000 intelligent Smartcard IDs that are being used for both physical access and logical PKI functions on the Department's unclassified Sensitive But Unclassified (SBU) systems. PKI hardware and software have been installed to over 25,000 domestic and overseas workstations with projected completion to occur in FY 2006. The FPKIPA has cross-certified the Department's X.500 directory based PKI and allowed it to connect to the Federal PKI interagency bridge. This gives the Department's current 26,000 (43,000 at full deployment) PKI users the ability to share SBU information rapidly in a secure manner, with 13 Government agencies and the State of Illinois through the use of PKI digital certificates. Currently the Department's PKI program is providing the "smartcard" based access control technology to the Department of Justice's Bureau of Citizenship and Immigration Services (BCIS), formally Immigration and Naturalization Service users at 103 locations around the country. BCIS estimates PKI services provided by the Department have saved taxpayers conservatively over \$700,000 annually. The PKI



DEPARTMENT OF STATE (DOS) continued

program with the Consular Affairs Bureau, is integrating PKI into the congressionally mandated electronic intelligent passport also known as the Machine Readable Travel Document program. This system digitally signs passport information using the Department's PKI to ensure the official issued information can be verified and has not been altered in real time at the Nation ports of entry. 300 e-passports have been issued to show that the Department can produce these enhanced-security travel credentials. In the FY 2006 timeframe, this system will support the production capacity of 7 to 10 million U.S. passports a year. The Department is implementing the Biometric Logical Access Development and Execution program to improve system security and enable a limited single sign-on capability for several PKI-enabled desktop applications, including network logon. This solution eliminates the need for users to remember passwords, instead using their fingerprint biometric to authenticate to their DOS Smart ID card for access to their personal PKI certificates. Biometric logon has begun domestically in several offices and will be tested in an overseas post in the next six months, and will thereafter be part of overseas deployment efforts.

Domestic Wireless Program

The Domestic Wireless Program provides UHF radio services to 24 Diplomatic Security Field Offices, Diplomatic Security protective details and the buildings security force. Conversion to a new industry baseline/interoperability standard (APCO 25) allows equipment to meet new Federal 12.5 kHz "narrow-band" standards and ensures interoperable

capabilities among local, State and Federal public safety and law enforcement agencies. The replacement of analog by digital equipment significantly improves voice quality and voice communications security. Significant funds are dedicated annually for this program to support new security communications requirements, especially an expanding fleet of Diplomatic Security vehicles requiring mobile radio equipment and installations. 23 of 24 Diplomatic Security Field Office upgrades have been completed, with the final field office coming online November 2005.

The Radio Programs Branch is also moving forward on a radio interoperability program, which directly supports the President's Management Agenda eGovernment Initiative - SAFECOM. SAFECOM is the umbrella program within the Federal government to oversee all communication and interoperability initiatives and projects. Through SAFECOM, the Federal government is addressing public safety communications issues in a more coordinated, comprehensive and, therefore, effective way. The Department of State's Radio Programs Branch initiated a pilot radio interoperability program in FY 2003 to meet this goal. LWS/RPB was accepted into the Department of Justice/Alexandria Police Department sponsored radio interoperability network located in the Greater Washington, D.C. Area. The CommTech program (formerly known as AGILE) utilizes JPS ACU 1000 interoperability units. LWS/RPB is researching new venues for additional interoperability networks throughout the United States and overseas. Radio

interoperability is an important tool used to coordinate interagency communications in support of Homeland Security efforts.

Washington Area Radio Network (WARN)

The WARN upgrade will introduce new SIMULCAST technology to improve radio coverage. Conversion to a new industry baseline/interoperability standard (APCO 25) allows equipment to meet new Federal 12.5 kHz "narrow-band" standards and ensures interoperable capabilities among local, State and Federal public safety and law enforcement agencies. The replacement of analog by digital equipment will significantly improve voice quality and voice communications security by allowing for an improved version of the Digital Encryption Standard to be utilized. In the Greater Washington, D.C. Area, WARN provides dedicated radio communication networks for all major Diplomatic Security divisions, most notably, Secretary of State's Protective Detail, Dignitary Protection, Domestic Facilities Protection, and Washington Field Office. Upon completion of upgrade (expected completion 12/2005), WARN will provide effective voice-radio communications in the Greater Washington, D.C. area to all subscribers.

High Frequency Radio Network

The High Frequency (HF) program utilizes 500-watt radios to provide long-range Emergency & Evacuation communications between embassies and consulates, DOD assets, other governments, non-governmental organizations, and in some countries, other U.S. citizens. The new HF



DEPARTMENT OF STATE (DOS) continued

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

Technical Security Efforts

The Department continues to apply Defensive Technical Counter Intelligence techniques through implementation of technical security methods and processes across programs, systems and agencies to mitigate risks associated with close access to the Department's IT assets both domestically and overseas. The technical security efforts complement the ongoing computer, cyber and information security efforts to provide a balanced security infrastructure across all layers of the Department's Enterprise Architecture.

Secure Video and Data Collaboration

The DOS Secure Video and Data Collaboration (SVDC) program provides secret-high video teleconferencing capability to overseas embassies and consulates as well as domestic bureaus and offices. This capability greatly reduces costs

incurred by travel and other methods of communication, by providing a means of immediate and secure communication as situations and needs dictate. Additionally, it allows for, and encourages, more frequent, routine communications, increasing inter-office availability and functional efficiency, without increasing costs. The SVDC program continues to expand as more sites gain the appropriate approval and equipment to participate in this program. Our partnerships with the Arms Control Verification Office (VC/VO) and the DOD European Command have allowed our growth to encompass close to ninety European and African posts. SVDC continues to work closely with VC/VO as they provide installation and training to overseas posts. Domestically, the number of bureaus and offices participating in SVDC, continues to increase as the benefits and cost savings become more apparent. Future prospects include partnerships with additional DOD commands and support to other DOS geographical arenas. Current initiatives include provisions for improved methods of connectivity, network throughput, and equipment availability. The SVDC Help Desk has increased its number of personnel, during this fiscal year, to support the growing customer participation in the program. It is expected to continue growth exponentially as the SVDC customer base expands.



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 Chief Information Officer (CIO) is responsible for ensuring, through the exercise of program management authority, that Treasury Bureaus have access to a cost-effective, technologically sound, telecommunications infrastructure for executing and carrying out their respective financial support missions.

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

Ongoing NS/EP Telecommunications Activities

Treasury Communications System

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

During fiscal year (FY) 2005, cyber security was improved through two avenues. In FY 2005, the first avenue saw the implementation of a layered approach to IDS management. IDS instances were deployed at various Bureaus and departmental agencies allowing each organization to monitor and respond to their own internal alerts. Additionally, data is being sent to the central TCS Security Operations Center allowing for a larger consolidated view of activity across the Treasury network. Currently for FY 2005, total sensor count remains at 26 deployed across the Treasury network. The Bureaus fielding IDS instances include the Office of the Controller of the Currency and the Bureau of Public Debt. Additional agencies include the Departmental Offices (DO), Community Development Financial Institution, and HRConnect.

The second avenue involves the ability to provide host-based intrusion detection systems (HIDS) allowing for individual system monitoring. To date, one additional HID has been added for a total of 19 HIDS deployed to various TCS and bureau assets. These additional capabilities extended the



DEPARTMENT OF THE TREASURY (TREAS) *continued*

breadth of our cyber security monitoring and allows for quicker response times to major incidents.

Furthermore, the TCS Continuity of Operations Plan (COOP) continues to evolve. The TCS AOF was completed June 2004 and currently supports all Treasury Bureaus' alternate operating facilities and serves as its Disaster Recovery backup site. Periodic exercises are conducted to test system functionality, train emergency personnel, and validate COOP requirements.

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

Additionally, Treasury Headquarters and associated Bureaus have designated which circuits and locations are to be supported through the NCS TSP Program. The TSP Program provides for enhanced service restoration by the telecommunications service providers based upon circuits designated as either Command and Control (TSP Level 1) or Critical Operations (TSP Level 2). Telecommunications service providers are required to restore service in priority order according to the TSP level indicator and before any non-TSP circuits are restored in case of a national emergency or disaster. This capability continues to be used to restore sites in the Southern United States that suffer damage from hurricanes. The Department of the

Treasury currently maintains 746 TSP 1 & 2 circuits.

Certification and Accreditation

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

In FY 2005, the TCS Security Assurance Program maintained its own accredited environment by ensuring that new services or changes added to the General Support System or Major Applications go through the complete C&A process as the original systems. In addition, the TCS Security Assurance Program has also performed C&A packages for other Bureaus and agencies including: the Treasury Human Resources, the Treasury Intranet, the Treasury Enterprise Virtual Private Network, and the ProSight Pilot Implementation Project used to support Treasury-wide capital planning and investment control.

Currently, TCS Security Assurance Program is in the process of certifying and accrediting the Treasury Executive Office of Asset Forfeiture project, the Secure Extranet Gateway, and the Treasury Self Administration Service. There are also three-year re-certifications in progress on the Foreign Credit Reporting System, and the Treasury Enterprise Directory Service. Additionally there is one re-certification in progress on the

ProSight pilot project due to major modifications.

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

The Certification team has also completed yearly updates in compliance with *Federal Information Security Management Act of 2002* requirements for the TCS including the TCS System Security Plan, Personnel and Physical Security Plan, TCS Risk Assessment, and TCS Self assessment in accordance with NIST 800-26.

Digital Telecommunications Switching System

IT Security

To carry out their wide ranging responsibilities, employees and managers of the U. S. Department of the Treasury have access to a complex telecommunications infrastructure that provides local capabilities to Treasury sites in the Washington, D.C., area, including sites in suburban Maryland and Northern Virginia, and physical interfaces to other telecommunications programs and services. To have this access to Treasury's complex telecommunication, the Digital



DEPARTMENT OF THE TREASURY (TREAS) continued

Telecommunications Switching System 2 (DTS2) network provides voice, data, and video services via analog, Integrated Services Digital Network (ISDN) Basic Rate Interface and ISDN Primary Rate Interface service to the DTS2 user community. The various business and law enforcement functions within Treasury depend on the confidentiality, integrity, and availability of these systems and their data.

The mission of the Department of the Treasury is to:

- Promote prosperous and stable American and world economies;
- Manage the Government's finances;
- Safeguard our financial systems, protect our Nation's leaders, and secure a safe and drug-free America; and
- Continue to build a strong institution.

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

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

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

DSX Access System

The cardkey system consists of the following hardware and software located at the DTS Customer Service Center at 633 3rd ST, NW, Washington, D.C.: the DSX 1022 system is one standard PC running Windows XP, six analog modems, one modem controller board, one proprietary application — WinDSX, manufactured by DSX Access Systems, Inc. of Dallas, TX — and 200 keys. There are six analog lines connected to the PC via modems. They have telephone numbers 926-9061 through 927-9066 and are on jacks MINT-1001-038A, B, C and 039A, B, and C. Dial-up modems are located at numerous remote sites.

System Overview

The original cardkey system was installed in 1996 and was originally intended to control all remote switch rooms as well as the Host switch room. Keys would be issued to people who were authorized by Treasury. Initially 150 keys were delivered with the system, and approximately 120 of those keys were issued when the system was placed into service. An additional 50 keys were obtained in July 1999. Not all of the Treasury bureau sites are on the DSX Cardkey system. After system installation, some Treasury Bureaus decided to use their existing systems and did not implement this particular (For example, the main Treasury building) system. To enter a switch room, a user must have either a Cardkey or a metal key to the door lock. When a Cardkey is issued, the Cardkey Administrator will program the master computer by filling out a form that contains the following information: Name of the key holder, work address, Social Security Number,



DEPARTMENT OF THE TREASURY (TREAS) continued

work telephone number, supervisor's name and number, imprinted key number, key code associated with the imprinted key number (supplied by Cardkey Systems or DSX) and access to offices or one office. When an authorized key is entered into the key slot (number side must be up), the door will click and can be pushed open. If the key is not authorized, the door will not open. The system polls each onsite controller and uploads information as to who has accessed the switch room and any alarms that were registered. Alarms include: blocking the door open, key not authorized, opening the door without using the key to exit the switch room, and controller status (loss of power, modem does not answer, etc.).

Federal Blue Pages Project

The Blue Pages Project began as a Vice Presidential Government-wide customer service initiative in October 1995. This customer-friendly approach to Government listings would become as familiar, convenient and consistent as the Yellow Pages. The project was lead by the National Performance Review (NPR), General Services Administration (GSA), and the President's Management Council. Additionally, Federal Executive Board and Federal Executive Association members participated.

Blue Pages is currently managed by GSA in conjunction with Blue Page Coordinators established within each Government agency. Public outreach supports U.S. Citizens through printed and electronic media to access Government citizen services. The Department of Treasury's Blue Page Coordinator provides program guidance, user training, and

disseminates essential program information to each special Bureau element. The Coordinator also supports the Senate Committee Report Act Section 3709 mandate requiring the Internal Revenue Service to publish directory listings in telephone directories.

Treasury's Blue Page Coordinator improved project management processes and enhanced citizen services that resulted in significant program cost containment. Initial guidelines, procedures, and training were established. Bureau Blue Page Coordinators attended training sessions, received user login access to GSA's Electronic Production System (EPS), and received guidance to determine market strategies within each special Bureau element. As a result of obtaining user access to the EPS system, and the elimination of redundant market listings during FY 2002 the cost containment was \$210,116.00. FY 2003 resulted in additional savings of \$144,673.00 due to a streamlined Bureau template and enhanced Bureau participation. Pacific Bell and Qwest covered approximately 14 U.S. States for market submissions. These telephone companies overcharged foreign listing fees to Federal agencies with Blue Page listings. Treasury Coordinator disputed these incorrect foreign listing charges that resulted in FY 2004 cost savings of \$1,898,385.00. Beginning in FY 2005 Treasury changed billing algorithms from percentage based to actual charges. This significant change proved additional cost savings during FY 2005 to the Department of Treasury \$30,000. Thus far, overall total cost containment for the Blue Pages Program is \$2,283,174.00.

Treasury Emergency Management Center Capability

As part of Treasury's COOP, Treasury Headquarters established interim Emergency Management Centers for responding and reacting to crises, disasters and emergencies. These centers are currently integrated with the Treasury's communications system network operations facilities for ensuring continuous operations of the Treasury Department in a crisis or emergency. Currently, these centers are being improved and modernized around changes in the Treasury Department's operating principles and practices and the associated information technology systems for enhancing their business management information systems.

The continuity of operations requirements for the Treasury Communications System have been fully coordinated and synchronized with the plans and programs operating under the Treasury Department's Office of Emergency Preparedness. Notwithstanding the devolution of the Treasury law enforcement organizations to the Department of Homeland Security, the issuance of Government Emergency Services (GETS) Telecommunications Services (GETS) cards continued to increase in FY 2005. Treasury expanded the Treasury Emergency Management/Operations Center within the greater Washington, D.C./metropolitan area to further strengthen Treasury's emergency preparedness posture.



DEPARTMENT OF THE TREASURY (TREAS) continued

Key operational functions and capabilities expanded in FY 2005/2006 are:

- Additional Department of Treasury Emergency Management Centers with associated system monitoring and management tools;
- Office space for senior Treasury Department leadership and their core emergency staff;
- Communications connectivity to other Bureau Alternate Operating Facilities (via the TCS W2 Site) and associated emergency preparedness staffs;
- Local Treasury Headquarters connectivity to Treasury enterprise services, such as e-mail, business applications and other information services;
- Development of a High Frequency Radio Network in support of Federal Preparedness Circular-65 requirement for emergency back up communications. Purchased HF radios for Treasury Headquarters, Treasury headquarter COOP site, all Bureau COOP sites and selected bureau headquarter locations. This network will facilitate communications between Headquarters and COOP sites at the secure level;
- Obtained additional GETS personal identification numbers that can be transferred to Treasury staff in order to respond to

immediate crisis such as the recent Hurricanes;

- Expanded WPS phone use by: insuring all Secretary Snow's successors have WPS capability; and by including Bureaus, that is, Bureaus are now obtaining WPS phones for senior staff; and
- In the process of obtaining secure and non-secure Video Teleconferencing capability between Alternate Headquarters and Bureau alternate facilities.

Support for the Federal Public Key Infrastructure Development

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

Treasury's enterprise PKI system is capable of issuing digital certificates to nearly 150,000 Treasury contractors and employees, and to date has had active participation by 11 of its 12 Bureaus.

Additionally, Treasury is one of six Federal agencies that have been cross-certified with the Federal Bridge Certification Authority providing PKI trust interoperability. This effort has allowed Treasury to strengthen its secure communications processes across a common infrastructure landscape. Treasury has also been working closely 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.

Treasury's PKI interest and usage is expected to increase dramatically in the near future as its digital certificates will be used to provide strong authentication services to address the Homeland Security Presidential Directive #12, and its requirement to establish a standardized and interoperable means of Personal Identity Verification amongst Federal employees and contractors.

Public Safety/Law Enforcement Wireless Activities

In 2005, the Department of Treasury re-established the Treasury Wireless Programs Office (WPO) to affect an enterprise approach in managing wireless technologies. As such, the WPO has aggressively worked to increase Treasury's representation and impact on two important fronts, departmental wireless asset management and participation in the Integrated Wireless Network (IWN) Program.

For asset management, Treasury secured its permanent departmental representation on the Interdepartment Radio Advisory Committee (IRAC) and with other Federal committees. Having a presence at the IRAC ensures that Treasury's spectral assets are managed appropriately to meet the department's spectrum needs for wireless public safety and law enforcement communications. In addition, to further increase Treasury's spectrum efficiency, Treasury is actively continuing efforts for timely compliance with the National



DEPARTMENT OF THE TREASURY (TREAS) *continued*

Telecommunications and Information Administration narrowband mandate as well as developing a Treasury Spectrum Strategic Plan in response to the Presidential Determination on spectrum management.

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

Once completed, these enhancements and modernization initiatives for FY 2005 and 2006 will allow Treasury to respond, operate and function in a crisis, emergency or national disaster.



DEPARTMENT OF DEFENSE (DOD)

NS/EP Telecommunications Mission

Under the provisions of Executive Order (E.O.) 12472, Department of Defense (DOD) maintains the following national security and emergency preparedness (NS/EP) telecommunications responsibilities:

- Provide, operate, and maintain the telecommunications services and facilities to support the National Command Authorities and execute the responsibilities by E.O. 12333, "U.S. Intelligence Activities," December 4, 1981;
- Ensure that the Director, National Security Agency, provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications; and
- Execute the functions listed in Section 3(1) of E.O. 12472.

Telecommunications Staff Organization

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

for Networks and Information Integration (NII).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense and the ASD for NII.

Current/Ongoing NS/EP Telecommunications Activities

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

In 2005, ASD NII with the Joint Staff J6 launched a project called Net Centric Operating Environment to deliver needed Global Information Grid (GIG) related products in time to support the execution of multiple programs. The objective is to synchronize programs, acquisitions, standards, architectures, and funding to ensure DOD has quality of service, network management, and information assurance within the GIG from an end-to-end standpoint in order to achieve net-centric operations.

NII's major investment areas are:

- The Bandwidth Expansion program, or GIG BE, which provides a secure, robust, optical IP terrestrial network;
- Joint Tactical Radio System, which offers a family of software reprogrammable radios based on an open-communication architecture that will provide interoperable tactical wideband IP communications capabilities;
- Transformational SATCOM which provides very high throughput satellite communications with optical quality bandwidth and satellite to satellite and satellite to ground routing;
- Net-Centric Enterprise Services, which supplies the infrastructure and services to support the broad range of applications and data used in a Net-Centric enterprise;
- Information Assurance, which is vital to support all efforts to ensure that the Internet is robust, reliable, and trusted;
- The DOD Teleport System that provides a gateway to the GIG for deployed warfighters; and
- Within the six major investment areas, these are the three enabling concepts: Network Operations, data



DEPARTMENT OF DEFENSE (DOD) *continued*

strategy, and Spectrum efficiency and utilization.

DOD continues its partnership with DHS on the SAFECOM program. DHS is the lead Federal Agency charged with assisting State and local governments address barriers to interoperability. They do this through requirements, definitions, and the development of interoperable communications standards and guidelines. DHS Office for Domestic Preparedness, have responsibility for the actual implementation of interoperability programs, such as grants for equipment, training, and technical assistance. We have continually updated our Memorandum of Agreement with DHS to support SAFECOM and E-Gov initiatives.

In direct support of the NS/EP community of interest, the Continuity Communications Working Group (CCWG) was established on 2004 as an interagency body reporting to the National Communications System Committee of Principals. The purpose of the CCWG is to develop a Continuity Communications (CC) Federal Enterprise Architecture Framework (FEAF) and oversee the development of a Continuity Communications Federal Enterprise Architecture (CC FEA) to support the performance of Federal Executive Branch (FEB) minimum essential functions under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The final product for this activity was delivered September 1, 2005.

The mission of the CCWG is to define a CC FEA strategic vision, document continuity communications

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

DHS is responsible for development and implementation of the National Command Capability (NCC), with strong support from DOD and other agencies. DHS has proposed forming an Interagency NCC Office (INCCO) to support NCC implementation. The INCCO is proposed to be made up of dedicated staff from each major department and agency, and serve as the single, dedicated entity responsible and resourced to develop, implement, and continuously improve the NCC. Ultimately, the NCC will support operations across all Federal, State, and local levels. The NCC is an integrated set of capabilities across the Federal, State, Tribal, and local levels to effectively support information sharing, situational awareness, collaborative decision-making, and coordinated operations between governments and public/private entities to continuously protect and care for the public and to achieve

national objectives during any emergency and through all hazards. The NCC emphasizes and is geared towards collaborative decision making in order to support to citizens and general welfare, and defend the Nation. It needs to be a ubiquitous capability to ensure it can operate under all circumstances without warning.



DEPARTMENT OF JUSTICE (DOJ)

NS/EP Telecommunications Mission

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

Telecommunications Staff Organization

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

Current/Ongoing NS/EP Telecommunications Activities

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

- The Deputy Chief Information Officer, Enterprise Solutions Staff provides representation for DOJ on the National Communications System (NCS) Committee of Principals (COP);
- OSS provides representation for DOJ on the NCS Council of Representatives;
- A OSS representative serves on the Telecommunications Service Priority (TSP) Oversight Committee;
- DOJ continues its active participation in the NCS activities of the COP, and participates in NCS NS/EP telecommunications support, activities, and programs;
- DOJ continues its vigorous support of the activities of NCS NS/EP planning, program, and contingency programs, and emerging NS/EP telecommunications programs. DOJ has sponsored full access to TSP services for a number of commercial companies which are either departmental component contractors or engaged in NS/EP support in their normal duties (such as remote security alarm sensing, 911 and enhanced 911 services in several Midwestern States; and for environmental and emergency response services for cleanup of waste at clandestine drug laboratories); and
- Additionally, the department is an active participant in the Government Emergency Telecommunications Service Program, the Wireless Priority Service Program, the Telecommunications Service Priority Program, and the Shared Resources High Frequency Radio Program.



DEPARTMENT OF THE INTERIOR (DOI)

NS/EP Telecommunications

Mission

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

Current/Ongoing NS/EP Telecommunications Activities

DOI mission critical long distance voice and data communications is primarily provided by MCI via the GSA FTS2001 contract. We are in process of consolidating our bureau backbone data communications networks to a single Department-wide Multi Protocol Label Switched based architecture with enhanced network security functionality. We are also consolidating ISP access throughout the Department.

Conversion of DOI's wideband LMR systems to narrowband digital operation is a high priority activity. We continue to investigate sharing opportunities with the USDA, Justice, Homeland Security, Treasury and other cooperators to improve interoperability and reduce costs. We have a multi-vendor multi-year contract to supply

digital narrowband radios and systems in response to the National Telecommunications and Information Administration mandated transition to narrowband LMR operations. This contract, available to all Federal agencies, provides lower-cost standardized interoperable digital radios. We participate in the e-Gov SAFECOM program which will improve interoperability of public safety radio systems.

Key officials, emergency coordinators, and telecommunications managers throughout the Department have Government Emergency Telecommunications Service Cards for long distance emergency telephone communications and Wireless Priority Service. Cellular phones have been provided to key officials in Washington, D.C. Secure Telephone Unit III and 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 have received Telecommunications Service Priority designation.

DOI Significant Accomplishments

Additional DOI Digital Narrowband Contracts were awarded. The National Park Service, Park Police, digital narrowband Very High Frequency trunked radio system for the National Capital region design has been completed and submitted to the National Telecommunications and Information Agency for approval. A draft memorandum of understanding with Justice, Treasury and Homeland Security for interoperability with the Integrated Wireless Network is under

review. DOI has signed a memorandum of understanding with the State of South Dakota for land mobile radio support. This agreement will significantly improve interoperability between Federal, State and local radio users in South Dakota.

The Department's consolidated Enterprise Services Network Phase 1 deployment is completed. This included completion of agency intranet and Internet access points of presence. Phase 2 includes completion of multi protocol label switching and transferring all network devices to managed services. DOI received and reviewed the NCS provided FTS2001 Traffic Analysis as part of the ongoing effort to provide critical infrastructure analyses for the COP. The findings of this excellent analysis are being considered for the DOI Electronic Switched Network project.



U.S. DEPARTMENT OF AGRICULTURE (USDA)

NS/EP Telecommunications Mission

The United States Department of Agriculture (USDA) engages in a number of national security and emergency preparedness (NS/EP) telecommunications activities. These activities support USDA missions to: provide for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment; inspect livestock, poultry, and other products to ensure the safety and wholesomeness of food; and, manage the protection and use of national forests, national grasslands, wilderness areas, and other public lands and facilities under USDA jurisdiction. This includes managing wildland fire control activities on these lands in coordination with local authorities and co-op forestry activities in support of State and local fire protection.

Current/Ongoing NS/EP Telecommunications Activities

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

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

a secure component into the USDA Enterprise Architecture.

Activities planned for FY 2006 will include infrastructure installation between key NS/EP designated sites; the development and implementation of a training program for network administrators, users, and non-cleared personnel; and, the implementation of a pilot.

USDA has replaced over 85% of the original Secure Telephone Units, Third Generation with the Secure Terminal Equipment, and has installed and/or ordered additional to meet the growing requirements of the Homeland Security, Continuity of Operations relocation sites, and mission areas. In addition USDA participates in the Cellular Priority Access Service, and is in the process of installing a secure video conferencing system to support Homeland Security requirements. USDA also supports the Government Emergency Telecommunications (GETS) program and in an ongoing effort, ensures all persons in NS/EP leadership positions have GETS cards

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

The USDA Office of the Chief Information Officer's Telecommunications Services and

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

NS/EP Partnership Activities

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

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



U.S. DEPARTMENT OF AGRICULTURE (USDA) continued

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

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



DEPARTMENT OF COMMERCE (DOC)

NS/EP Telecommunications

Mission

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

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

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

census, which is the basis of representative democracy.

Telecommunications Staff Organization

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

Current/Ongoing NS/EP Telecommunications Activities

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

- The DOC is actively involved in Homeland Security initiatives and efforts to enhance preparedness with the necessary information technology equipment, software and hardware upgrades. Its headquarters in Washington, D.C. has implemented a new Emergency Broadcast System (EBS) that can send pre-recorded or ad hoc messages to every Voice Over Internet Protocol telephone in the Herbert C. Hoover Building (HCHB). The EBS alerts users at their desks by turning on lights on the phones and playing audio messages through the phones' speakers and handset. A text message, identical to the audio message, simultaneously appears on the 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, and the White House Visitors' Center.

- To enhance our Continuity of Operation Planning, the Employee Notification System was successfully piloted within the HCHB during the first half of calendar year 2005. In addition, the system was used to successfully conduct an accountability test for Office of the Secretary employees during the Pinnacle exercise of June 22, 2005. As of September 30, 2005, the ENS contains approximately 20,000 employee records from across all of the bureaus. The system automatically notifies all identified employees using any of several available means (such as, telephone, cell phone, pager, email, etc.) within a reasonable period of time. Notifications are based on grouping structures and other criteria. Employees are able to report their status and availability for duty, as well as enter and update their own contact information.

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



DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

NS/EP Telecommunications Mission

To provide the necessary technical and support capabilities for preparation, mitigation, response, and recovery the U. S. Department of Health and Human Services (HHS) has continued a strong commitment to designing and implementing sound technology that meets the diversity necessary for national security and emergency preparedness (NS/EP) telecommunications systems.

Current/Ongoing NS/EP Telecommunications Activities

Each core operating division of HHS has focused on developing and implementing the necessary strategies to provide voice and data systems for:

- Communication on Public Health issues within the Federal Government;

- Communication on Public Health issues with State and local Cooperators; and
- Communications on Public Health issues with Non-Governmental Organizations.

Current emphasis is on providing a consolidated approach for the delivery of integrated Information Technology (IT) and communications systems to support the Department's mission for the protection of the health and welfare of the American public. An area of focus for the Department continues to be provisioning of IT infrastructure that allows bidirectional communications regardless of atmospheric or terrain restrictions. In addition, emphasis has been placed on the interoperability of systems that can communicate with all of the Federal, State, local and tribal partners involved in the support of the Department's primary Emergency

Support Function #8 response. With the further definition being provided by the National Communications System and other organizations, the Department is rapidly moving toward standardization of IT related resources for its continuity of operations and continuity of Government functions and is working towards compliance with both the SAFECOM and Disaster Management initiatives.

In an effort to increase the ability for global surveillance of health issues affecting the American public, the Department of Health and Human Services has established collaborative relationships with health organizations around the world to ensure rapid identification and treatment of health threats. These extensions of the Department's capabilities have created a more vigilant environment to discover and analyze emerging public health threats such as Severe Acute Respiratory Syndrome and Avian Influenza.



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

Current/Ongoing NS/EP Telecommunication Activities

Support of NCS Activities

The Department continues its active participation on the National Communications System's (NCS) Committee of Principals and Council of Representatives, the President's National Security Telecommunications Advisory Committee, and actively supports NCS national security and emergency preparedness (NS/EP) activities and programs. The Department has designated a member of the Chief Information Officer's staff to liaison with the NCS. This DOT

representative is working to further ensure that the Department is receiving full benefit of the various NS/EP programs and services offered by the NCS.

Government Emergency Telecommunications System

The Department of Transportation is actively involved with the Government Emergency Telecommunication System (GETS). The GETS calling cards have been assigned to Regional Emergency Transportation Coordinators and Representatives within the United States and abroad to be used during natural, man made disasters and other emergency situations. The Department has also been instrumental in the sponsorship of Federal, State, and local Governments for the GETS program. The Department has recently been approached by and has offered support to transportation's private sector (Alaska Airlines, Frontier Airlines and Adirondacks Trailways Bus Services) similar telecom support. The Department coordinates and offers assistance to all qualified applicants.

Telecommunication Service Priority

Due to the secure nature of the Department's continuity of operations (COOP) sites and frequent COOP exercises, the Department is also participating in the Wireless Priority Services program. The T-Mobile, Globalstar, and Iridium satellite handsets, as well as desktop sets have been distributed to individuals that perform the NS/EP functions. This association greatly enhances the Department's capability to communicate during emergency situations.

Other NS/EP Programs

The Department is also a participant in the Federal Telecommunication Committee Standards Program, the Shared Resources, High Frequency Radio Program, and the Communications Resource Information Sharing Initiative. DOT participated in the TOP Officials 3 exercises co-sponsored by Department of Justice and Department of State.

Other Emergency Support

During the recent deluge of hurricane related disaster recovery efforts, DOT took an active role in supporting the Federal efforts in the hurricane stricken areas not only as Emergency Support Function 1 to the Federal Emergency Management Agency (FEMA) under the National Response Plan, but also with support from each of the Operating Administrations. DOT IT supported this effort with equipment, technicians, telecommunications expertise, and developed an "Electronic Support Go Kit".

DOT, along with several other operating administrations, was a participant in the Pinnacle exercise sponsored by FEMA. Per instruction, DOT developed scenarios particular to its functionality that were introduced at the event. The information gathered and disbursed throughout the Department resulted in a very positive response to emergency situations and continuity of government.

Additionally, the Department is well underway towards the consolidation of 12 operating Administrations into one centralized IT function to include print desktop services, e-mail, and active directory, as well as server and file



DEPARTMENT OF TRANSPORTATION (DOT) continued

services. This will simplify the maintenance, backup, and recovery procedures in all situations. Consolidation will streamline and improve support capabilities while reducing costs and increasing security.



DEPARTMENT OF ENERGY (DOE)

NS/EP Telecommunications Mission

DOE Emergency Communications Network

The Emergency Communications Network (ECN) re-established the satellite system at the Remote Sensing Laboratory on Nellis Air Force Base to support a growing need for mobile communications within the Office of the Associate Administrator for Emergency Operations. A Mobile ECN platform that provides a reach-back capability of data, voice and video connectivity into the network is in development. This Mobile ECN platform, while still in development, supported the Strategic Petroleum Reserve's Presidential directive to start pumping down the reserve after Hurricane Katrina. Data, voice and video connections were established at three SPR locations and were directly responsible for the success of this Presidential directive.

DOE Headquarters Networks

During fiscal year (FY) 2005, the Department of Energy (DOE) improved the fault-tolerant design of the headquarters (HQ) network with an additional Internet uplink, redundancy from the network demilitarized zone to the Internet, and deployed Hot Standby Routing Protocol (HSRP). HSRP provides network redundancy for Internet Protocol networks, ensuring that user traffic immediately recovers from first hop failures in network edge devices or access circuits. The HQ Internet service was upgraded to a new circuit configuration designed with a fully automatic internet failover configuration from the GTN OC-3 to the Forrester DS-3.

In response to the loss of both primary and continuity of operations (COOP) operational facilities for the SPR (Harahan, Louisiana) after hurricane Katrina, the Chief Information Officer's Office was able to successfully provide all network services in the standup of an alternate COOP location. Through the coordination of Telecommunications Service Priority provisioning network and Internet connectivity and other Information Technology services were delivered to the COOP within a 24-hour period in direct support of the Presidential directive to manage the petroleum reserves.

Kansas City Plant

The Kansas City Plant Installed a digital trunked land-mobile radio system in FY 2005. The new system complies with National Telecommunications and Information Administration mandate to migrate Federal users to narrowband radio and provides call encryption and interoperability with public safety first responders in the greater Kansas City metro area.

Nevada Site Operations

A new frequency plan was granted for the State-Wide Safety Net (Net 12) and the system was configured for back-up radio service for the Trucked Radio System. Migration of all very high frequency (VHF) Radio Nets to the new narrow band VHF channel plan was completed

Oak Ridge Operations

Oak Ridge Operations completed installation of a Wide Area Radio System for the Oak Ridge Reservation. This system is a three site 25 channel simulcast narrowband trunked radio system and provides interoperability between DOE security, Emergency Management and local law enforcement agencies, and other agencies.

Richland Operations Office

DOE-Richland achieved Federal mandate narrowband compliance for its Safeguards and Emergency Service organizations as part of its radio migration effort (Project L-347, Narrowband Radio Migration). A new narrowband Land Mobile Radio system replaced conventional wideband analog radio systems. DOE-Richland completed implementation of a new E911 system at the Hanford's Patrol Operation Center.

Savannah River Operations Office

The site-wide ultra high frequency (UHF) radio system which consists of 2000 radios is used by site maintenance to perform their work in the areas they are assigned. A project plan was developed to upgrade the number of UHF channels to 10 to reduce interference and crowding and all radios will be narrow band capable — planned completion January 2008. Upgraded to full T1 for the two U.S. Forest Service remote Centracom dispatch console systems from RS-232 19.2 Kbps to full T1 links with full redundant capability. This greatly improved the reliability of the remote dispatch consoles performance. As a result of this success, the data network path for SRS Site Communications own remote dispatch console was also upgraded to T1 bandwidth.



DEPARTMENT OF VETERANS AFFAIRS (VA)

NS/EP Telecommunications Mission

Wide Area Networking

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

VA Nationwide Teleconferencing System (VANTS)

VANTS provides 24 X 7 audio and video teleconferencing services for business meetings, program planning sessions, distance learning, interviews and hearings. VANTS customers include VA employees, emergency personnel, State officials, hospitals, universities and other Federal Government agencies, including the Department of Defense. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 Kilobit per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 960 audio ports for voice teleconferencing.

Frequency Management Automation

To expedite the engineering of new radio frequencies, VA uses the latest

frequency management software, Spectrum XXI. Additionally, VA has joined the National Telecommunications and Information Administration in pioneering a Government-wide, classified data exchange has made the Government Master File of Radio Frequency Authorizations available, in real time over the public switched telephone network.

Enhanced Mobile Satellite Services

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 at geographically dispersed locations to allow the handsets to dial directly into VA facilities via the satellite network. Many of the handsets are also equipped with approved Type I communications security devices to support secure voice communications.

VA Trans-America Radio Program

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

capabilities to manipulate antenna propagation for long range.

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

Office of the Inspector General (IG) Network

The VA Radio Frequency Management Office, working with the IG, has completed implementation of a nationwide, narrowband fixed/mobile radio network. The Very High Frequency digital network integrates the investigative arm of the IG's Office with Federal and civilian law enforcement services nationwide, and provides unique narrowband radio frequencies for six VA regions. The radio system provides the highest degree of security in communications available today for IG field operations.



DEPARTMENT OF HOMELAND SECURITY (DHS)

NS/EP Telecommunications Mission

Since being established in 2003, the Department of Homeland Security (DHS) has made it a priority to cultivate partnerships and leverage synergies with other entities focused on preparedness and response missions. DHS has also been working to consolidate and improve existing national communications infrastructure and programs within the Department and with other Federal agencies (such as, Department of the Treasury, and Department of Justice). DHS continually strives to meet communications needs and requirements to ensure the safety of the Nation and protect critical infrastructure and key resources.

To execute its mission and unify agencies with wireless homeland security missions, the Department has created and maintains several initiatives to improve wireless communications capabilities across all levels of Government. Included in this effort is the expansion of secure communications infrastructure, equipment, and training.

Current/Ongoing NS/EP Telecommunications Activities

DHS is involved in the following national security and emergency preparedness (NS/EP)-related telecommunications activities:

DHS Wireless Management Office

The DHS Wireless Management Office (WMO) was formed to set forth wireless technology policy and overall DHS goals in an effort to improve homeland security while reducing

technology costs. In fiscal year 2005, the DHS WMO was involved in the following NS/EP-related activities:

- Provided wireless communications support for Hurricane Katrina by providing mobile satellite telephones to various DHS components, including the Homeland Security Operations Center and Customs and Border Protection, for use at the disaster site. The DHS WMO also served as a clearinghouse for requests for assistance from DHS components and offers to assist from vendors and other entities;
- Procured and installed subscriber units to support wireless communications systems (such as, Plum Island Animal Disease Center and Federal Law Enforcement Training Center in Cheltenham, MD), and DHS tactical components (such as, Customs and Border Protection, and the U.S. Secret Service);
- Developed Integrated Wireless Network (IWN) Southwest Service Area operational requirements to support the implementation of the IWN;
- Completed downselect process to identify most competitive vendors to move forward with the IWN, and received and reviewed cost and technical proposals from

vendors in support of the IWN Acquisition Strategy;

- Initiated Seattle-Blaine Phase II to enhance the existing IWN system in the Northwest Service Area;
- Developed and assisted with executing an operational communications plan for local, State, and Federal law enforcement agencies at the Professional Golfer's Association's U.S. Open;
- Formed various working groups (such as, wireless, wireless applications, security) to leverage and coordinate efforts and foster synergies among DHS Components;
- Initiated the development of operational processes, procedures, and plans for coordinating and managing DHS wireless resources during crisis situations to ensure continuity of operations; and
- Began developing the Wireless Enterprise Architecture (EA) to establish a framework, organizational structure, and development of a Wireless Enterprise Information Technology Architecture for integration with the DHS EA.

SAFECOM

SAFECOM, a program within DHS Science and Technology Directorate's



DEPARTMENT OF HOMELAND SECURITY (DHS) continued

Office for Interoperability and Compatibility (OIC), serves as the umbrella program within the Federal government to help local, tribal, State, and Federal public safety agencies improve emergency response through more effective and efficient interoperable wireless communications. SAFECOM was developed by public safety for public safety and has involved law enforcement, fire, and EMS officials, including the broader public safety community.

SAFECOM's accomplishments include:

- Continued revision to version 1.0 of the first Public Safety Statement of Requirements for Communications and Interoperability;
- The availability of the Statewide Communications Interoperability Planning (SCIP) Methodology. The SCIP Methodology, which can be downloaded from SAFECOM's Web site, outlines a step-by-step process for developing a locally-driven statewide strategic plan for enhancing communications interoperability;
- Coordinated grant guidance that was subsequently incorporated into the FY 2005 Community Oriented Policing Services awards and FY 2005 Office for Domestic Preparedness awards; and
- The OIC and SAFECOM, a program of OIC, have

launched a quarterly newsletter entitled Interoperability Today. The newsletter will cover relevant topics pertaining to public safety interoperability in three focus areas — communications, equipment, and training.

National Incident Response Unit/Technical Maintenance Facility (NIRU/TMF)

NIRU/TMF provides rapid deployment support of radio equipment and personnel for emergency response and large event activities (presidential inauguration). This support includes two-way radio support for Immigration and Customs Enforcement offices nationwide including distribution, programming, and repair and maintenance of subscriber (handheld and vehicle) and infrastructure radio equipment. NIRU/TMF support ensures reliable interoffice and inter-agency communications for agents and officers enabling more efficient completion of daily law enforcement duties and enhanced officer safety.

NIRU/TMF provided the following NS/EP support during FY 2005:

- Distributed over 800 mobile and portable radio assets and associated equipment to ICE offices nationwide totaling over four million dollars;
- Loaned 107 portable radios to ICE components for use during short-term operations.

- Provided radio equipment and programming support for the following events:
 - Presidential election
 - Presidential Inauguration; and
- Provided radio equipment, programming, training, and personnel support for the following natural disasters:
 - Hurricane Katrina
 - Hurricane Rita.

Customs and Border Protection (CBP), Tactical Communications Organization (TCO)

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

During FY 2005, CBP was partially funded to begin modernization of its existing VHF land mobile radio network with the primary focus on the Arizona Border. This modernization process will provide for interoperability among CBP users, DHS, and in certain locales, among other state and local law enforcement officials.



DEPARTMENT OF HOMELAND SECURITY (DHS) continued

Homeland Security Operations Center (HSOC)

Homeland Security Information Network (HSIN)

The core mission of the HSOC, as mandated by Congress, is information sharing with all levels of Federal, State, and local government and law enforcement officials, as well as the private sector. The primary mechanism used by the HSOC to receive and distribute information on a real-time basis to relevant organizations and individuals is the HSIN. All 50 states and 50 major metropolitan areas are connected to HSIN.

HSIN State and Local Deployment

During 2005 a pilot program was conducted to evaluate deployment process, training requirements, procedures, and policy of expanding HSIN beyond high level State offices down to fusion centers, Emergency Operation Centers, local law enforcement, and emergency management organizations. Based on the lessons learned from the pilot program, over 20 additional states have initiated HSIN activation to their state, local, and tribal constituents.

HSIN Federal Deployment

Aviation Law Enforcement CBT Training and related portlets are being implemented. The Federal Flight Deck Officers (FFDOs) were added to the HSIN-LE Community of Interest. Over 250 Border Patrol Intel Analysts are being added to HSIN and are receiving related training. An Open Source XML feed into HSIN Federal Operation Center and HSOC portals was established. DHS Continued HSIN deployment to 12,000 Federal Air

Marshals and is working with the United States Coast Guard (USCG) and the Office of the Chief Information Officer to implement the Coast Guard's Alert and Warning System. Additionally, DHS worked with USCG Sector Portsmouth, VA to activate HSIN in the Command Center. The Department developed a plan to reach other Federal agencies. DHS is pursuing FEMA leadership to establish a deployment plan that encompasses the following scheme: *Category I—EP&R (FEMA)—(Response, Preparedness, Mitigation, Recovery); Category II—FEMA's 10 Regions; and Category III—The 14 Emergency Support Function Groups.*

Technology Operations Program

The Technology Operations Program (TOP) is responsible for day-to-day operations of all the technologies required for smooth, effective running of the Homeland Security Operations Center. During FY 2005 the Program made major strides in improving the efficiency, reliability, and survivability of the HSOC by implementing a suite of radio communications systems, including HF and VHF radio systems; expanded the capabilities of the operational LAN within the HSOC, including deployment of additional computers, network connections, and software; established high-bandwidth data connectivity at the HSOC alternate site. The TOP also provided significant support to DHS response personnel deployed to the hurricane disaster areas, including assembly and deployment of special communications personnel and kits.

Homeland Security Data Network (HSDN)

In FY 2005, DHS deployed the first phase of HSDN to 56 government sites, providing a unified system and program that enables the sharing and protection secret-level data between its Federal partners. The HSDN will significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the Department's dependence on networks external to DHS.

FEMA National Radio System (FNARS)

DHS provided partial funding for the first phase of a multi-year program to upgrade FNARS, FEMA's HF radio system. FNARS provided long-range tactical communications support during all major hurricanes, as well as Continuity of Operations and other NS/EP communications exercises. The National Emergency Coordination Net, which utilizes FNARS equipment and frequencies, was activated during the hurricanes to provide a common calling channel for all Federal responders, State Emergency Operations Centers, and the American Red Cross to coordinate their response activities.



CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP Telecommunications Mission

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

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

Telecommunications Staff Organization

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

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

Current/Ongoing Telecommunications Activities

The following CIA activities support NS/EP objectives:

- Active participation in the National Communications System activities of the Committee of Principals/Council of Representatives;
- Continued support of the Government Emergency Telecommunication Services, the Federal Telecommunications Standards Committee, and the Telecommunications Service Priority System;
- Actively transitioning our legacy secure telephone units to the new secure terminal equipment; and
- We have an active program to add secure video teleconferencing to our desktops.

Significant Accomplishments

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

- Provided enhanced telecommunications services between the CIA, other U.S. Government organizations, and the U.S. military services;
- Continued support to Defense Message System objectives and architecture; and
- Added redundancy and eliminated single points of failure for our commercial and secure voice networks.



FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP Telecommunications

Mission

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

Current/Ongoing NS/EP Telecommunications Activities

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

- Plans for, provides, operates and maintains information technology and telecommunications services and facilities as part of the National Emergency Management Information System (NEMIS);
- Designs and develops emergency networks and information systems;

- Provides communications support to State and local officials to help disseminate warnings of risks and hazards;
- Accumulates and assesses damage information;
- Deploys telecommunications and information technology assets to incident areas and coordinates Telecommunications Service Priority and other requests for communication service and connectivity; and
- Coordinates the assignment and use of all Federal radio frequencies at an incident site.

Significant Accomplishments

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

NEMIS supported 134 disaster and emergency declarations, the most ever faced by FEMA. NEMIS was upgraded and web-enabled so disaster victims could apply for assistance using the Internet.

Interactive voice response service was added to the FEMA telephone network to enable disaster victims to check the status of their applications. Telephone messages were sent to disaster victims to confirm receipt of their substantiating materials. FEMA's data network bandwidth was increased to

OC-3 to meet unprecedented load and relieve saturation. Improved security features were added to communications networks joining Federal Continuity of Operations sites.

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

The FEMA National Radio System multiphase upgrade project started in FY 2005. Engineering, design and acquisition of resources for architectural upgrade, a network control station and two remote stations were performed. Upgrades will begin in FY 2006.



THE JOINT STAFF (JS)

NS/EP Telecommunications Mission

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

The J6 oversees C4 support for the National Military Command System.

Telecommunications Staff Organization

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

Significant Accomplishments (Refer to DOD Section)

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

Pending Issues (Refer to DOD Section)



GENERAL SERVICES ADMINISTRATION (GSA)

NS/EP Telecommunications Mission

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

The GSA Federal Technology Service (FTS) mission is to provide information technology solutions, professional services, and network services that deliver the best value and innovations to support our customers' missions worldwide.

The GSA national security and emergency preparedness (NS/EP) missions are specified as provided in following orders and plans:

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

Current/Ongoing NS/EP Telecommunications Activities

GSA/FTS provides a variety of network services, information technology, and professional services that support Federal agencies. These services

include local and long distance voice, data and video telecommunications, building and campus telecommunications infrastructure support, information technology solutions, and professional services.

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

GSA continues to support the National Communications System (NCS) and Executive Office of the President, Office of Science and Technology Policy emergency management programs.

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

Other services offered by GSA/FTS include:

- Multi-Tiered Security Profiles, designed to provide enhanced Network Service offerings by integrating various security layers into the current portfolio of contracts; and
- Access Certificate for E-Services program provides digital certificates and

managed PKI services to assist Federal agencies in meeting the requirements of the Government Paperwork Elimination Act.

Significant Accomplishments

- Provided support on continuity of operations (COOP) and NS/EP exercises throughout the country and provided telecommunications support to FEMA as required for numerous disasters;
- Supported activities of the Committee on National Security Systems; and
- Coordinated the implementation of the FTS Incident Master web-based Crisis Management Software which supports COOP, NS/EP response personnel and multiple expert planners from varied FTS directorates. This software was utilized during Exercise Pinnacle to test the application's usability. This analytical tool proved very beneficial in providing near-real-time event data concerning asset deployment, and was found to be very useful in simplifying record keeping requirements for historical purposes. The FTS Incident Master is a fully compliant "Incident Command System/Unified Command" tool that provides web-based incident tracking, asset management and resource sharing mechanisms required in an ever changing



GENERAL SERVICES ADMINISTRATION (GSA) *continued*

emergency preparedness
environment.

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



NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP Telecommunications Mission

The National Aeronautics and Space Administration (NASA) shall (pursuant to an Executive Order dated February 28, 2003) coordinate with the Secretary of Homeland Security to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautics-related systems, equipment, and methodologies applicable to national security emergencies.

Telecommunications Staff Organization

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

NASA's George C. Marshall Space Flight Center, located in Huntsville, Alabama, maintains lead center responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network (NISN).

Current/Ongoing NS/EP Telecommunications Activities

NASA continues to support the NCS in achieving its assigned missions and the

successful accomplishment of national-level programs approved by the White House. This includes Telecommunications Service Priority, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, and the National Telecommunications Management Structure.

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

NS/EP Telecommunications Assets

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

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

NASA Deep Space Network supports deep space interplanetary, high-Earth

orbiting spacecraft, and radio science missions.

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

NASA Research & Education Network is NASA's component to the Next Generation Internet initiative. It operates as a test bed for developing Internet technologies, applications, and networking tools.

Significant Accomplishments

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



NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP Telecommunications Mission

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

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

Current/Ongoing NS/EP Telecommunications Mission

The NRC Emergency Telecommunications System (ETS), which provides NS/EP communications from nuclear power plants and major fuel cycle facilities, consists of FTS2001 Direct Access Lines at most locations throughout the country. Every location that participates in ETS has

Telecommunications Service Priority coverage assigned to at least one Emergency Notification System circuit. Twenty-three locations do not utilize ETS through FTS2001. Instead, they use their own corporate communication systems to meet the requirement.

The NRC supports National Communications System (NCS) NS/EP programs and remains active in NCS Committee of Principals and Council of Representatives activities.

A satellite phone program that provides equipment to headquarters, regions, and Federal inspectors located at each commercial nuclear power plant is well established.

The NRC is currently implementing Wireless Priority Service (WPS) on the cell phones of key agency staff and members of the incident response organization at both headquarters and regional offices.

The Government Emergency Telecommunications Services (GETS) continues to be highly recommended by the NRC as a means of enhancing access to long distance service. The NRC's participation in the program continues to increase. The NRC recently implemented an agency-wide quarterly telecommunications testing program that encompasses the testing of GETS alone and with satellite phones. This program will include the testing of WPS in conjunction with GETS in the second quarter of Fiscal Year 2006.

The NRC maintains an Alert and Coordination Network phone in the headquarters Operations Center in

addition to a Critical Warning Infrastructure Network terminal and phone.

Secure communications capability exists between NRC headquarters, regional locations, and all licensed nuclear facilities. A procedure to conference up to three Secure Terminal Equipment units was recently documented and distributed. The NRC successfully launched a Secure Video Teleconferencing system in the headquarters Operations Center and all of the NRC regional Incident Response Centers.

Significant Accomplishments

- Wireless Priority Service is being applied to the cell phones of key management and staff;
- Telecommunications testing program instituted for Government Emergency Telecommunications Service, Wireless Priority Service, and satellite phones;
- Secure Video Teleconferencing system established in the headquarters Operations Center and all of the NRC regional Incident Response Centers; and
- Critical Warning Infrastructure Network terminal and phone established at NRC's Headquarters Operations Center.



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP Telecommunications Mission

The National Telecommunications and Information Administration (NTIA) national security and emergency preparedness (NS/EP) mission as tasked under Executive Orders 12046, 12472, and 12656 includes serving as the Executive Branch telecommunications policy adviser to the President, serving as the manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board (JTRB). Thus, among other things, NTIA advises and assists the President in the administration of a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support NS/EP functions.

Current/Ongoing NS/EP Telecommunications Activities

The NTIA/Office of Spectrum Management (OSM) continues its efforts to develop a United States spectrum policy for the 21st century in response to the President's Spectrum Policy Initiative of May 2003. OSM developed a spectrum policy reform initiative implementation plan to guide its efforts in this regard. Part of OSM's vision is to use information technology (IT) to automate the spectrum management business processes and to be more effective and efficient in Federal spectrum use. Specific examples of activities in this regard include the following:

- Using an OSM Enterprise Architecture Council to

develop IT requirements of the Federal spectrum management community and an implementation plan to satisfy those requirements;

- Continuing efforts under a memorandum of agreement with the Federal Communications Commission and the Department of Defense's Joint Spectrum Center to leverage available resources in developing common spectrum management systems and approaches as appropriate;
- Continuing to partner with the Department of Defense's Joint Spectrum Center to develop and field improvements to the SPECTRUM XXI and other automated capabilities for use by all Federal spectrum managers;
- Continuing to plan and implement, using a phased approach, a series of Federal spectrum management system improvements to include the capability for total electronic transfer and use of Federal spectrum management information and data; 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 electromagnetic spectrum

during NS/EP and normal conditions.

In addition, NTIA is continuing to:

- Serve as a non-resident member of the National Communications System's (NCS) National Coordinating Center and the Communications Infrastructure Sharing Analysis Center;
- Participate in various activities and endeavors relative to national emergency management and continuity of Government as well as agency continuity of operations;
- Participate in various activities and endeavors of the President's National Security Telecommunications Advisory Committee;
- Provide Co-Chair of the Government Emergency Telecommunications Service (GETS)/Wireless Priority Service User Council, participate in Council endeavors, and provide GETS user authorizations to all new NTIA emergency employees;
- Participate in NCS Committee of Principals (COP) and Council of Representatives activities and endeavors to include the NCS COP Priority Services Working Group and Continuity Communications Working Group; and



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) *continued*

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

Significant Accomplishments

- Participated with other JTRB members in Federal response to Hurricanes Katrina and Rita to include processing over 3,000 frequency assignment actions submitted by Federal agencies for new frequency assignments in support of the Federal response to the hurricanes;
- Established an NTIA radio station as part of the NCS SHARES HF Coordination Network;
- Conducted over 200 meetings of the IRAC and its Subcommittees and ad hoc groups;
- Conducted interagency spectrum management portion of Exercise PINNACLE 2005; and
- Represented the U.S. Government on many spectrum policy matters at various meetings of International Telecommunications Union working groups, study groups, and more.



NATIONAL SECURITY AGENCY (NSA)

NS/EP Telecommunications Mission

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

Information Technology and Information Assurance

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

- The NIARL conducts and sponsors research in the technologies and techniques needed to secure U.S. national security systems, to include cryptography, high-confidence software and systems, authentication, high speed security solutions, secure wireless multimedia, secure operating systems and network management, privilege management, and controlled sharing.
- The IA enterprise teams across academia, industry, and Government to provide IA solutions to keep U.S. national security systems safe from harm. This mission involves detecting, reporting, and responding to cyber threats, as well as making encryption

codes to securely pass information among systems. It includes embedding IA measures directly into the Department of Defense's emerging Global Information Grid (GIG); building secure audio and video communications equipment; making tamper protection products; providing trusted microelectronics products; testing the security of systems; providing operational security assistance; as well as evaluating commercial software and hardware against nationally set standards.

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

In accordance with its National Security Systems Manager responsibilities under National Security Directive 42, NSA IA products and services also are applicable across the Government for the protection of classified and sensitive national security information. NSA's customers include a broad range of users of the National Information Infrastructure and the critical infrastructure communities. IA activities include close working relationships with the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), and other entities with information assurance responsibilities.

Current/Ongoing NS/EP Telecommunications Activities

NSA Commercial Solutions Center for NS/EP Telecommunications

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

NSA Threat Operations Center for NS/EP Telecommunications

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



NATIONAL SECURITY AGENCY (NSA) *continued*

Cryptographic Modernization Initiative Supporting NS/EP Telecommunications

- The Cryptographic Modernization Initiative is a DOD-directed/NSA-led effort to transform and modernize IA capabilities for the 21st century. The initiative coordinates and oversees modernization of DOD IA capabilities by replacing an aging cryptographic product inventory, meeting increased interoperability needs, keeping pace with the evolution of information technology, and achieving objectives needed to enable the information assurance component of the DOD GIG architecture.
- Achieved two major milestones: Assessment of Type 1 Cryptographic Inventory, January 2005, which lists all known cryptographic devices; and issuance of 11 Cryptographic Decertification messages signed by the NSA Director of IA in September 2005.

Electronic Key Management System for NS/EP Telecommunications Systems

- The Electronic Key Management System (EKMS) — the multi-tiered, distributed key management system designed to generate and distribute electronic key and automate the

management of physical key and cryptographic equipment — continues to evolve.

- Continued operations and upgrading EKMS Phase 4 systems. All Army and Air Force Central Office of Record (COR) Accounts were upgraded to EKMS Phase 4 and consolidated COR functionality at the Common Tier 1 sites. Navy accounts are scheduled to be converted in fiscal year 2006.
- Developed, tested, and deployed a major communications upgrade (SIPRNET and ISDN capability) to the Tier 0 and Common Tier 1 Sites under the EKMS Phase 5 project. Installation and operation of the Tier 2 Nodes (Local Management Device (LMD)/Key Processor) is scheduled for FY 2006. The LMD's software, Local Communications Security Management Software (LCMS), was updated with the capability to support Store and Forward Enhanced FIREFLY Rekey (LCMS version 5.0.3). This Software upgrade was developed and tested in FY 2005 and is scheduled for deployment in FY 2006. Message Server software version 6.2 baseline was completed and fielded. This Message Server baseline corrected a number of high priority discrepancy reports uncovered during testing operation.

High Assurance Internet Protocol Encryption

Work continues towards securing the high-speed transport pipe with 100 Mbps inline network High Assurance Internet Protocol Encryptors with migration to 1 Gbps and 10 Gbps encryptors.

Security Assessments Supporting NS/EP Telecommunications

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

IA Services Supporting NS/EP Telecommunications

- NSA continues to provide a variety of IA services. In 2005, NSA issued the following IA guidance documents for use by industry and the Government: Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF; Center for Internet Security Benchmark for Oracle 9i/10g, Version 2.0; and Center for Internet Security Exchange Server 2003 Benchmark, Version 1.0.
- A Defense Advanced Research Projects Agency employee was honored with the NSA 2005 Rowlett Individual Excellence Award for breakthrough research into



NATIONAL SECURITY AGENCY (NSA) continued

cyber defense to include technology that automatically quarantines computer-based worms, limiting their migration and restoring the user's computer to its pre-infected state within minutes. This individual achievement award is given annually to the individual within a Government organization making the most significant contribution to improving his/her element's information systems security posture, IA readiness, or the conduct of defensive information operations (DIO).

- A Department of State organization was awarded the NSA 2005 Rowlett Organizational Excellence Award for demonstrating exceptional ingenuity and leadership in assisting the Federal law enforcement and intelligence communities in carrying out the *President's National Strategy to Secure Cyberspace*, as well as helping meet the emerging cyber security challenges outlined in the *President's National Counterintelligence Strategy*. This award is given annually to the Government organization recognized as making the most significant contribution to the improvement of national information systems security, operational IA readiness, or the DIO posture of the United States.

- The United States Naval Academy took top honors over each of the five U.S. service academies (Army, Air Force, Coast Guard, and Merchant Marine) in the 2005 Cyber Defense Exercise (CDX), a one-of-a-kind training tool to prepare the students to protect and defend the nation's critical information systems. The CDX is just one example of NSA's educational outreach.
- NSA and DHS continue their joint management of the National Centers of Academic Excellence in IA Education by approving the addition of eight more universities. Additionally, NSA/DHS approved the re-applications of seven other universities.
- NSA and NIST jointly announced the public availability of the Extensible Configuration Checklist Description Format (XCCDF). NSA and NIST collaborated with industry to develop the XCCDF specification to promote the use, standardization, and sharing of effective security checklists. XCCDF is vendor-neutral, and provides a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, thereby fostering a more widespread application of good security practices.

National Security Incident Response Center

The National Security Incident Response Center (NSIRC) provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique, tailored, time-critical and term reporting based on NSIRC's ability to detect, react, warn, and respond to intrusions into U.S. Government cyber networks and to provide all-source threat reporting on Signals Intelligence threats to operations, exercises, information systems and force protection.

Defensive Information Operations Assessments/Monitoring

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



NATIONAL SECURITY AGENCY (NSA) *continued*

Global Information Grid

The NSA Enterprise IA Architecture and Systems Engineering office, in partnership with the GIG community, leads the effort to define the enterprise level IA strategies, guidance, standards, policies, systems requirements and technologies necessary to realize DOD's net-centric GIG vision. While the office's principal focus is in supporting the DOD's GIG, its work is broadly applicable to net-centric enterprise efforts across the Intelligence Community, Department of Homeland Security, Information Sharing Environment and other Federal information technology (IT) enterprise efforts. These national security communities require the development of an assured global national security IT enterprise to transform the way they operate, communicate and use information to accomplish their missions. NSA's IA support will help ensure that communications, information sharing and infrastructure availability are not barriers to the Nation's security.



U.S. POSTAL SERVICE (USPS)

NS/EP Telecommunications Mission

The United States Postal Service (USPS) is an independent establishment of the Executive Branch of the United States Government. It operates in a businesslike way.

In the more than two centuries since the USPS began, it has grown and changed with America. Discovering the history of the Postal Service is a journey into the history of transportation, economics, industrialization, communications, and Government.

Today, the Postal Service delivers hundreds of millions of messages each day to more than 141 million homes and businesses.

This is the story of the evolution of the Postal Service and the important role it has played in the development of the United States.

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

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

FY 2005 IT Fact Sheet	Quantity
Key Telephone Systems	7,000
PBX Telephone Systems	453
Wireless LAN Access Points	2,202
Telephone Business Lines	150,000
Desktop Firewalls	103,000
Blackberries	5,700
Satellite Connections	11,829
Cellular Devices	30,000
Authorized Radio Frequencies	3,060
Internal emails annually	1,508,000,000
National Applications	650
Visits to usps.com	256,200,000

Current/Ongoing NS/EP Telecommunications Activities

Universal Computing Connectivity

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

The Postal Service recognizes that as the organization and general commerce evolve, new advanced information services will be necessary to meet new or changed requirements, to improve performance and reliability, and to reduce operating expenses.

In 2005, IT enhanced and expanded the infrastructure of its BlackBerry system. This wireless communications system provides remote communications capability to more than 5,700 Postal Service managers and Continuity of Operations team members, even when Postal Service facilities are without power or shut down. The BlackBerry system now

includes additional functionality and twice the coverage area.

In 2005, IT upgraded the bandwidth at more than 9,000 locations to improve system performance when employees are connected to the network. IT has also upgraded 750 VSAT equipped offices throughout the infrastructure for improved performance.

Enterprise Data Warehouse

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

Over the past year, use of EDW has grown from a few hundred individual users who generated approximately 600 reports per week to over 3,000 users creating more than 40,000 reports per week. To manage this growing data environment and to assure the business value of EDW initiatives and the consistency and quality of its data, IT created an EDW governance infrastructure in 2005. Recent improvements in the efficiency of frequently executed reports, as well as a planned upgrade to the EDW infrastructure, will enable IT to meet the challenge of EDW's rapid growth and institutionalization.

IT continues to add new data sources to EDW, focusing particularly on those systems that manage the movement of mail. In 2005, IT added Delivery Confirmation data, and plans are underway to add other sources, such as International Mail.



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

Enhancing Security

During fiscal year (FY) 2005, the USPS Information Technology Corporate Information Security Office made significant progress in creating a climate where employees, customers, and partners understand that security brings real business value to our products and services. The Postal Service had no significant breaches or viruses that could have prevented us from serving our customers or conducting our day-to-day business functions.

Also during FY 2005, the Postal Service designed and put into operation a layered defense that includes strengthening firewalls, guarding the network perimeter, implementing initial baseline hardening standards, and enhancing access controls.

Supplementing the USPS layered defense initiative are:

- Enhanced intrusion detection software;
- Scheduled infrastructure vulnerability assessment tests that include critical and high-risk sites as well as identified vulnerabilities;
- Scheduled network scans to identify potential risk areas; and
- Robust patch management oversight to ensure operating system and application fixes are applied in a timely manner to prevent exploitation of commonly known vulnerabilities.

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

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

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

Such measures cover a lot of territory:

- Over 13 million Internet email messages scanned monthly for viruses.
- Over 55 billion network data packets scanned monthly for evidence of intrusion.
- Over 52,000 employees viewing the Postal Service security awareness video.
- Over 2.3 million files a month being transferred securely using Assured File Transfer.

Working with the Department of Defense

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

- This past year the Postal Service and DOD continued to improve the Automated Military Postal System, which automates many military postal processes and provides



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

detailed information on military post operations, transportation costs, and daily retail financial transactions. The system will reduce paperwork and labor costs, and improve timing and accuracy of air carrier payments.

The Postal Service has also worked closely with DOD to ensure that mail destined to our troops Iraq and Afghanistan keeps flowing from home.



FEDERAL RESERVE BOARD (FRB)

NS/EP Telecommunications

Mission

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

Telecommunications Staff Organization

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

Current/Ongoing NS/EP Telecommunications Activities

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial telecommunications infrastructure and payment systems. The FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential

telecommunications services supporting large-value payment systems, large-value clearing and settlement systems, major financial services exchanges and utilities, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. In addition, the FRB administers the TSP program for financial service organizations sponsored by the Securities and Exchange Commission (SEC), Office of the Comptroller of the Currency (OCC), Commodities and Futures Trading Commission (CFTC), National Credit Union Administration (NCUA) and the Office of Thrift Supervision (OTS).

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

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

Significant Accomplishments

The FRB focused its NS/EP activities on its sponsorship role for assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993 and expanded in 2002. The FRB

continues to sponsor TSP assignments for the following:

- circuits used for Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions;
- voice and data circuits supporting Federal Reserve open market and foreign operations, the automated auction processing system for Treasury securities, and critical central bank functions;
- circuits used by other payment systems (such as, the Society for Worldwide Interbank Financial Telecommunications and the Clearing House Interbank Payments System) that meet the FRB's eligibility criteria;
- circuits used for large-dollar clearing and settlement services, including access circuits to the Federal Reserve's net settlement service, the networks of Automated Clearing House (ACH) operators, the Continuous Linked Settlement (CLS) bank, and other qualifying financial service utilities;
- circuits used by ACH operators and the CLS bank



FEDERAL RESERVE BOARD (FRB) *continued*

that meet the FRB's eligibility criteria;

- circuits connecting customers of sponsored payment system, foreign exchange, and clearing and settlement utilities that meet the FRB's eligibility criteria;
- circuits used by capital and futures exchange utilities and key participants that meet the SEC and CFTC eligibility criteria;
- circuits used by market data providers that supply critical information needed by financial institutions; and
- circuits used by the World Bank to ensure continuity of operations.

By the end of this fiscal year, there will be approximately 4,500 active TSP assignments including circuits directly sponsored by the FRB as well as those circuits administered for the SEC, OCC, CFTC, NCUA and OTS.

The FRB has implemented GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption. In December 2002, the FRB began sponsoring other key participants in the nation's payment systems. By the end of this fiscal year, the FRB will have sponsored approximately 54 institutions.

During the last fiscal year, the FRB continued to participate in the evolution of the WPS program. The FRB has sponsored 25 institutions for WPS with approximately 381 users currently enrolled in the service.

During 2005, the FRB served as chair of an interagency task force formed by the NCS to review all existing FCC orders and NCS directives related to the TSP program and made recommendations for numerous revisions. FRB also organized and conducted the first-ever on-site reviews of the major telecommunications service providers' TSP processes and procedures.

The NCS developed route diversity (communications routing between two points over physically separate paths) recommendations for the FRB to enhance telecommunications resiliency for its Washington, D.C. location. Using the NCS route diversity methodology, the FRB assessed the physical diversity and resiliency of its voice and data telecommunication systems, identified vulnerable assets, and developed mitigation strategies.

FRB Coordinated the financial sector response to Hurricane Katrina to re-establish critical telecommunications for financial institutions regulated by the FRS, SEC, OCC, NCUA, FDIC, and OTS. Additionally, FRB worked with approximately 30 financial institutions and issued approximately 120 TSP priority provisioning codes.



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 that promote access to effective communications services in emergency situations by public safety, health, defense, and other emergency personnel, as well as all consumers in need;
- Evaluating and strengthening measures for protecting the Nation's critical communications infrastructure;
- Facilitating rapid restoration of the U.S. communications infrastructure and facilities after disruption by any cause;
- Participation in international organizations and conferences to coordinate protection of the global communications infrastructure; and
- Coordination with industry and other Federal, State, tribal, and local agencies on matters of public safety, homeland security, and disaster management.

Current/Ongoing NS/EP Telecommunications Activities

- On November 3, 2005, the Commission adopted a Report

and Order (R&O) and Further Notice of Proposed Rulemaking (FNPRM) addressing the Emergency Alert System (EAS). The R&O expands the Commission's EAS rules to include the following digital media technologies: digital television and radio, digital cable, and satellite television and radio. The FNPRM seeks further comment on how the Commission, along with Federal, State and industry partners, can develop a robust, state-of-the-art, digitally-based public alert and warning system. The Commission also seeks further comment on how to ensure that EAS messages more effectively reach individuals with hearing and vision disabilities and individuals who do not speak English.

- On May 19, 2005, the FCC adopted rules requiring providers of interconnected Voice over Internet Protocol phone service to supply enhanced 911 (E9-1-1) emergency calling capabilities to their customers. The Order placed obligations on interconnected VoIP service providers that are similar to traditional telephone providers. The Commission also stated its intention to adopt, in a future order, an advanced E9-1-1 solution that includes a method for determining the customer's location without the customer

having to self report this information.

- To resolve the ongoing and growing problem of interference to public safety radio systems operating in the 800 MHz band, in 2004 the Commission adopted a new band plan for the 800 MHz band. In 2005, the Commission's Wireless Telecommunications Bureau continued to implement the plan by taking actions to address the cause of the interference problem by relocating incompatible technologies from the 800 MHz band, with costs to be paid by Nextel Communications, Inc.
- In an August order, the Commission decided that providers of certain broadband and interconnected voice over Internet Protocol (VoIP) services must be prepared to accommodate law enforcement wiretaps. The Commission found that circuit-switched voice service and dial-up Internet access can essentially replace conventional telecommunications services currently subject to wiretap rules, and as such, are covered by the Communications Assistance for Law Enforcement Act (CALEA). The Commission also adopted a Further Notice of Proposed Rulemaking that seeks more



FEDERAL COMMUNICATIONS COMMISSION (FCC)

continued

information about whether certain classes or categories of facilities-based broadband Internet access providers should be exempt from CALEA.

Significant Accomplishments

- The Commission hosted a two-day Continuing Legal Education Seminar entitled “Representing the Communications Client in the Era of Homeland Security.” This seminar featured participants from private industry, law firms, and the Federal Government, and covered issues including homeland security considerations in transactions involving foreign investment in U.S. infrastructure, programs to provide priority telecommunications access to qualified entities, Network Reliability Interoperability Council (NRIC) and Media Security and Reliability Council (MSRC) best practices, and the role of these industry best practices in the marketplace.
- The Commission held a Telecommunications Services Priority (TSP) Summit. This summit provided an opportunity for affected parties to discuss the communications needs of State and local emergency service providers, including Public Safety Access Points and to provide insight into

how the telecommunications service priority program can best serve affected communities.

- The Commission established a joint Federal/State VoIP E9-1-1 Enforcement Task Force to facilitate the timely and effective enforcement of the Commission’s VoIP E9-1-1 rules.
- The Commission took a number of initiatives to support relief and communications efforts related to Hurricanes Katrina, Rita, and Wilma, including: outreach to all segments of the communications industry to determine requirements and assets for rapid recovery of essential communications services; grant of more than one hundred special temporary authorizations and temporary frequency assignments for wireline, wireless, satellite, and broadcasters to expedite recovery of communications services; and provision of over \$200 million in universal service funding for reestablishment of communications services in the disaster area.



A

ACRONYMS

A

NCS RELATED ACRONYMS

A		C	
ACH	Automated Clearing House	C4	Command, Control, Communications and Computer Systems
ACN	Alerting and Coordinating Network	C&A	Certification and Accreditation
ACR	Alternate Carrier Routing	CALEA	Communications Assistance for Law Enforcement Act
AGCS	AG Communications Systems	CBP	Customs and Border Protection
AIN	Advanced Intelligence Network	CBRN	Chemical, Biological, Radiological, and Nuclear
AgPRS	Agriculture Public Safety Radio System	CC	Continuity Communications
ALE	Automatic Link Establishment	CCPC	Civil Communications Planning Committee
ANSI	American National Standards Institute	CCWG	Continuity Communications Working Group
ASD (HD)	Assistant Secretary of Defense for Homeland Defense	CDMA	Code Division Multiple Access
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration	CDX	Cyber Defense Exercise
ASIP	Assistant Secretary for Infrastructure Protection	CEP	Civil Emergency Planning
ATG	Advanced Technology Group	CEPTAG	Civil Emergency Planning Telecommunications Advisory Group
B		CFTC	Commodities and Futures Trading Commission
BCIS	Bureau of Citizenship and Immigration Services	CFWG	Critical Facilities Working Group
BDT	Backup Dial Tone	CIA	Central Intelligence Agency

CIO	Chief Information Officer	DISN	Defense Information Systems Network
CIP	Critical Infrastructure Protection	DO	Departmental Offices
CLS	Continuous Linked Settlement	DOC	Department of Commerce
COG	Continuity of Government	DOD	Department of Defense
COMSEC	Communications Security	DOE	Department of Energy
COOP	Continuity of Operations	DOI	Department of the Interior
COP	Committee of Principals	DOJ	Department of Justice
COR	Council of Representatives (III-40)	DOS	Department of State
COR	Central Office of Records (IV-38)	DOT	Department of Transportation
CSC	Computer Sciences Corporation	DPA	Defense Production Act
CSCC	Communications Sector Coordinating Council	DTS	Diplomatic Telecommunications Service
CTCP	Canadian Telecommunications Cyber Protection	DTS2	Digital Telecommunications Switching System
CTIA	Cellular Telecommunications and Internet Association	E	
CY	Calendar Year	E9-1-1	Enhanced 9-1-1
D		EA	Enterprise Architecture
DHS	Department of Homeland Security	EAP	Extensible Authentication Protocol
DIO	Defense Information Operations	EBS	Emergency Broadcasting System
DISA	Defense Information Systems Agency	ECN	Emergency Communications Network
DISALAN	Defense Information Systems Agency Local Area Network	EDW	Enterprise Data Warehouse
		EIP	Enterprise Information Portal
		EKMS	Electronic Key Management System
		EMP	Electromagnetic Pulse

E.O.	Executive Order	FTS2001	Federal Telecommunications System 2001
EOC	Emergency Operations Center	FY	Fiscal Year
EOP	Executive Office of the President	G	
EOT	Emergency Operations Team		
EPS	Electronic Production System	GETS	Government Emergency Telecommunications Service
ERLink	Emergency Response Link	GIG	Global Information Grid
ESF-2	Emergency Support Function #2	GITM	Global IT Modernization
ESOC	Enterprise Server Operation Center	GN	Ground Network
ESWG	End-to-End Services Working Group	GPRA	Government Performance and Results Act
ETS	Emergency Telecommunications System	GPS	Global Positioning System
F		GSA	General Services Administration
		GSM	Global System for Mobile Communications
FBI	Federal Bureau of Investigation	H	
FCC	Federal Communications Commission	HCHB	Herbert C. Hoover Building
FEA	Federal Enterprise Architecture	HF	High Frequency
FEB	Federal Executive Branch	HHS	Department of Health and Human Services
FEMA	Federal Emergency Management Agency	HIDS	Host-Based Intrusion Detection Systems
FPKIPA	Federal Public Key Infrastructure Policy Authority	HPC	High Probability of Completion
FNARS	FEMA National Radio System	HPM	High Power Microwave
FOC	Full Operational Capability	HQ	Headquarters
FPC	Federal Preparedness Circular	HSC	Homeland Security Council
FRB	Federal Reserve Board	HSCL	Homeland Security Communication Link
FTS	Federal Technology Service	HSDN	Homeland Security Data Network

HSIN	Homeland Security Information Network	ISAC	Telecommunications Information Sharing and Analysis Center
HSOC	Homeland Security Operations Center	ISDN	Integrated Services Digital Network
HSPD	Homeland Security Presidential Directive	ISP	Internet Service Provider
HSRP	Hot Standby Routing Protocol	IT	Information Technology
HSTL	Homeland Security Telephone Link	ITD	Information Technology Directorate
I		IWN	Integrated Wireless Network
IA	Information Assurance	I-WPS	Immediate Wireless Priority Service
IAIP	Information Analysis and Infrastructure Protection	IXC	Interexchange Carrier
IAM	Initial Address Message	J	
IC	Integration Contractor	J6	Command, Control, Communications, and Computer Systems Directorate
IEEE	Institute of Electrical and Electronic Engineers	JS	Joint Staff
IES	Industry Executive Subcommittee	JTRB	Joint Telecommunications Resource Board
IG	Inspector General	L	
IMA	Individual Mobilization Augmentee	LAN	Local Area Network
IMWG	Incident Management Working Group	LEC	Local Exchange Carrier
INCCO	Interagency National Coordinating Center Office	LCMS	Local Communications Security Management Software
INE	Inline Network Encryption	LMD	Local Management Device
IP	Internet Protocol	LMR	Land Mobile Radio
IR	Industry Requirements	LRTF	Legislative and Regulatory Task Force
IRS	Internal Revenue Service		

M			
MHD	Magneto Hydro Dynamics	NIARL	National Information Assurance Research Laboratory
MSRC	Media Security and Reliability Council	NICC	National Infrastructure Coordination Center
		NIIF	Network Interconnection Interoperability Forum
N			
NASA	National Aeronautics and Space Administration	NIPP	National Infrastructure Protection Plan
NATO	North Atlantic Treaty Organization	NISN	NASA Integrated Services Network
NCC	National Coordinating Center for Telecommunications	NIST	National Institute of Standards and Technology
NCCTF	National Coordinating Center Task Force	NOTF	NSTAC Outreach Task Force
NCS	National Communications System	NRC	Nuclear Regulatory Commission
NCSC	NSA Commercial Solutions Center	NRIC	Network Reliability and Interoperability Council
NCSD	National Cyber Security Division	NRP	National Response Plan
NCUA	National Credit Union Administration	NSA	National Security Agency
NDAC	Network Design and Analysis Capability	NSC	National Security Council
NEMIS	National Emergency Management Information System	NS/EP	National Security and Emergency Preparedness
NGN	Next Generation Networks	NSIRC	National Security Incident Response Center
NGNTF	Next Generation Network Task Force	NSIE	Network Security Information Exchanges
NGPS	Next Generation Priority Service	NSSE	National Special Security Event
		NSTAC	President's National Security Telecommunications Advisory Committee
		NTIA	National Telecommunications and Information Administration
		NTOC	NSA Threat Operations Center

NTRWG	Near Term Recommendations Working Group	PDD	Presidential Decision Directive
O		PKI	Public Key Infrastructure
OA	Operational Analysis	PN	Public Network
OC	Oversight Committee	POTS	Plain Old Telephone Service
OCC	Office of Comptroller of Currency	PPBS	Planning, Programming, and Budgeting System
OCIO	Office of the Chief Information Officer's	PSN	Public Switched Network
OHS	Office of Homeland Security	PSTN	Public Switched Telephone Network
OMB	Office of Management and Budget	PSWG	Priority Services Working Group
OMNCS	Office of the Manager, National Communications System	PT&E	Planning, Training, and Exercise Branch
OSD	Office of the Secretary of Defense	PTS	Priority Telecommunications Services
OSIS	Open Source Information System	Q	
OSM	Office of Spectrum Management	QoS	Quality of Service
OSSS	One-Stop Shop Service	R	
OSS	Operations Services Systems	R&D	Research and Development
OSTP	Office of Science and Technology Policy	R&O	Report and Order
OTS	Office of Thrift Supervision	RDTF	Research and Development Task Force
P		RDX	Research and Development Exchange
PAS	Priority Access Service	S	
PBX	Private Branch Exchange	S&T	Science and Technology

SAFECOM	Wireless Public Safety Interoperable Communications Program	STU III	Secure Telephone Units, Third Generation
SAFETY Act	Support Anti-Terrorism by Fostering Effective Technologies Act	SURWG	Scenarios and User Requirements Working Group
SATCOM	Satellite Communications	SVDC	Secure Video and Data Collaboration
SBU	Sensitive But Unclassified	T	
SCADA	Supervisory Control and Data Acquisition	TAL	Technology Assessment Laboratory
SCC	Sector Coordinating Council	TATF	Trusted Access Task Force
SCIP	Statewide Communications Interoperability Planning	TCS	Treasury Communications System
SEC	Securities and Exchange Commission	TCO	Tactical Communications Organization
SHARES	Shared Resources High Frequency Radio Network	TEDE	Telecommunications Electromagnetic Disruptive Effects
SIPRNET	Secure Internet Protocol Router Network	TEPITF	Telecommunications and Electric Power Interdependency Task Force
SITREP	Situation Report	TGCC	Telecommunications Government Coordination Council
SMART	State Messaging and Archive Retrieval Toolset	TIB	Technical Information Bulletin
SME	Subject Matter Expert	TMN	Telecommunications Management Network
SPP	Security and Prosperity Partnership	TMP	Telecommunications Modernization Project
SS7	Signaling System 7	TOP	Technology Operations Program
SSA	Sector Specific Agency	TOPOFF	Top Officials Exercise
SSAA	System Security Authorization Agreement	TSA	Transportation Security Administration
SSP	Sector Specific Plan		
STE	Secure Terminal Equipment System		

TSO	Telecommunications Services and Operations	W	
TSP	Telecommunications Service Priority	WAN	Wide Area Network
U		WARN	Washington Area Radio Network
UCC	Universal Computing Connectivity	WG-P	Postal Working Group
UHF	Ultra High Frequency	WG-T	Telecommunications Working Group
UMTS	Universal Mobile Telecommunications System	WMO	Wireless Management Office
USDA	U.S. Department of Agriculture	WPS	Wireless Priority Service Response Team
USG	United States Government	X	
USPS	United States Postal Service	XCCDF	Extensible Configuration Checklist Description Format
USS	United States Ship	XTE	Experimental Testbed Environment
V			
VA	Department of Veterans Affairs		
VANTS	Veterans Affairs Nationwide Teleconferencing System		
VHF	Very High Frequency		
VoIP	Voice over Internet Protocol		
VTMWG	Vulnerabilities and Threat Modeling Working Group		



