Statement of

DR. PETER M. FONASH

ACTING DEPUTY MANAGER,
NATIONAL COMMUNICATIONS SYSTEM
UNITED STATES DEPARTMENT OF HOMELAND SECURITY

WASHINGTON, D.C.

BEFORE THE

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON
TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

"*Terrorism and the EMP Threat to Homeland Security*"

MARCH 8, 2005

I. INTRODUCTION

Thank you, Mr. Chairman and distinguished members of the Committee. My name is Peter M. Fonash. I am the Acting Deputy Manager of the National Communications System (NCS). Sec. 201 (g)(2) of the Homeland Security Act of 2002 transferred the National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto to the secretary of Homeland Security. The NCS is aligned within the Information Analysis and Infrastructure Protection Directorate (IAIP) in the Department of Homeland Security (DHS). The NCS is governed under Executive Order 12472 of April 3, 1984, as amended by E.O. 13286, of February 28, 2003, which designates the Secretary of Homeland Security as Executive Agent for the body. As Executive Agent, the Secretary has designated the Assistant Secretary for Infrastructure Protection within IAIP to serve as the Manager of the NCS.

The NCS, as you know, is an interagency body that brings together the telecommunications assets of the Federal government that are of significance to national security and emergency preparedness (NS/EP). Pursuant to E.O. 12472, the NCS is responsible to ensure the existence of a national telecommunications infrastructure that is responsive to the NS/EP needs of the Federal government and capable of providing survivable NS/EP telecommunications services in all circumstances, including conditions of crisis or emergency. However, it is also important to frame NCS' activities relative to telecommunications in the context of other commercial infrastructures and to the interdependencies that exist among them across the nation.

Prior to my recent responsibilities as Acting Deputy Manager, during my almost seven-year tenure with the NCS staff, I also directed the Technology and Programs Branch and, thus, have

been actively involved in NCS' numerous technical and engineering efforts designed to improve the resiliency and reliability of the underlying public telecommunications networks under all types of scenarios, including its work relative to the impacts of nuclear electromagnetic pulse (EMP) on telecommunications. I am honored to appear before you today to discuss the issues surrounding the vulnerabilities of our nation's critical telecommunications infrastructure to nuclear electromagnetic pulse (EMP), and to other sources of telecommunications electromagnetic disruptive effects (TEDE), and NCS' efforts to address those vulnerabilities. TEDE is a high-intensity, short-duration burst of electromagnetic energy generated by nuclear or other devices. Unless properly shielded or designed power networks or electronic devices may be damaged by this energy surge.

II. BACKGROUND ON THE NCS

A. *The NCS Mission Generally – National Security/Emergency Preparedness (NS/EP) Telecommunications*

Since the height of the Cold War, the development and maintenance of survivable national telecommunications has been an enduring national objective. The nation's telecommunications infrastructure must possess a combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security. Over two decades ago, E.O. 12472 recognized the fundamental importance of reliable telecommunications to our national security, calling for a redundant and resilient telecommunications capable of absorbing an attack and continuing to function in support of multiple national objectives, such as connectivity for national leaders, military command and control, and continuity of government.

Similarly, in 1983, National Security Decision Directive (NSDD) No. 97 identified a survivable telecommunications infrastructure as a critical element of U.S. deterrence strategies. More

recently, Homeland Security Presidential Directive (HSPD) No. 7 recognized that, in addition to its specific national security significance, reliable telecommunications also constitutes one of the essential services that underpin American society as a whole and forms a crucial foundation for homeland security as well.

To help to achieve this objective, President Kennedy, in 1963, established the NCS "to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack." Two decades later, in 1984, President Reagan, issued E.O. 12472, which reaffirmed and expanded the membership and mission of the NCS.

In essence, the NCS is a consortium of key representatives of the Executive Office of the President (EOP) and 23 departments and agencies having national security and/or emergency preparedness (NS/EP) missions. As set forth in E.O. 12472, the NCS assists the President and the EOP in the coordination of the planning for and provision of NS/EP telecommunications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. E.O. 12472 charges the NCS to ensure development of a national telecommunications infrastructure that is:

- Responsive to the NS/EP needs of the President and Federal departments and agencies, including telecommunications support of national security leadership and Continuity of Government;
- Capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government, and privately owned telecommunications resources;
- Designed to incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain the survivability of NS/EP telecommunications in all circumstances; and

- Consistent, to the maximum extent practicable, with other national telecommunications policies.

When put into place at the height of the Cold War, the larger NS/EP goal was promotion of a survivable and resilient national telecommunications infrastructure. The primary focus was on a state-based, largely monolithic threat. The fear was that a single major power would launch a first strike against military and defense industrial base targets in the United States. In the post-9/11 environment, however, the U.S. faces more asymmetric threats and the potential targets expanded to include civilian, economic, and other critical targets. This change — fundamental in terms of actors, intent, capabilities, and tactics — creates new challenges for the U.S. Government.

Such evolving and expanding threats present three basic issues for the NS/EP Telecommunications community. They (1) undermine the ability to assure the delivery of essential telecommunications services; (2) blur traditional distinctions between wartime and non-wartime functions; and (3) complicate threat assessments to the national telecommunications infrastructure.. NS/EP telecommunications were originally conceived to serve at the nexus of national security and emergency preparedness, responding to any event that has the potential for catastrophic implications for the nation. The linkage of "NS" and "EP"—and their underlying statutory authorities—enabled the US Government to organize national response efforts regardless of the threat, whether it involved a nuclear attack or a natural disaster affecting a significant region of the country. These response efforts ranged from ensuring the survival of enduring constitutional government, support to military operations, and providing federal disaster assistance. Some of these efforts are accomplished in close coordination with FEMA's Office of National Security Coordination.

In recognition of the fact that more than 95 percent of government telecommunications traffic traverses the public switched telephone network, E.O. 12472 also directed the NCS to "serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning," a principle of public-private collaboration that HSPD-7 calls for all critical infrastructure sectors.

B. *NCS Responsibilities Relative to EMP*

Part 215 of Title 47, Chapter II, of the Code of Federal Regulations (C.F.R.) establishes NCS, as the focal point within the Federal government for all EMP technical data and studies concerning telecommunications. The purposes underlying this designation were to centralize dissemination of data and the results of studies concerning the telecommunications effects of EMP and protective measures among Federal agencies and avoid duplication of research efforts.

III. NCS ACTIVITES RELATIVE TO TELECOMMUNICATIONS ELECTROMAGNETIC DISRUPTIVE EFFECTS (TEDE) FROM NUCLEAR EMP AND OTHER SOURCES

Emerging from the tactical and strategic concerns of the Cold War, analyses of potential sources of electromagnetic disruption of telecommunications services have historically focused most sharply on the effects produced by the electromagnetic pulse emanating from the detonation of a nuclear device by a hostile nation-state. For example, in a 1985 special report to the President, the National Security Telecommunications Advisory Committee (NSTAC) provided its analysis of the vulnerability of the telecommunications infrastructure to High Altitude EMP (HEMP).

Yet, while nuclear EMP remains the only mechanism to effect widespread electromagnetic disruption to telecommunications – for example, the 2004 EMP Commission notes impacts covering a geographic area 2800 km in diameter – it is important to recognize that the advance of

technology has yielded many more tools capable of producing similar telecommunications electromagnetic disruptive effects (TEDE) on a more limited, but nevertheless significant, scale. Such tools are, as a general matter, often less costly than are those necessary to create an EMP. Accordingly, consonant with its NS/EP telecommunications mission, NCS has expanded its analytical activities to encompass the full range of TEDE sources including, but not limited to, EMP.

With respect to EMP specifically, the NCS has, over the ensuing two decades since the NSTAC Report, conducted numerous studies, simulations, and tests of various elements of the telecommunications infrastructure to electromagnetic interference from a nuclear EMP. These tests, conducted in the late 1980s and into the 1990s, subjected the major telecommunications switching system components to electromagnetic radiation simulating an EMP. The information derived from these tests was used by the equipment manufacturers to implement vulnerability mitigating changes in the design of the switching systems.

Just last year, the NCS also actively participated in the congressionally-chartered *Commission to Assess the Threat from High Altitude Electromagnetic Pulse* (the "2004 EMP Commission") that examined and evaluated the state of the EMP threat at present and looking 15 years into the foreseeable future. The Commission's Report, delivered last July, concludes that EMP presents a less significant direct threat to telecommunications than it does to the National Power grid but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the nation's telecommunications systems in the region exposed to EMP (which could include most of the United States). The NCS concurs with this assessment.

Notably, the Commission focused on many high altitude effects from EMP, but did not delve into the threats from source region EMP, system-generated EMP, trapped radiation, and other sources of TEDE such as directed radio frequency (RF) energy weapons, which could be developed and used by terrorists against the telecommunications infrastructure. As noted above, NCS considers this to be an important area for future consideration and action. NCS' efforts relative to the potential threat posed by such other sources of TEDE fall into the following three categories:

(1) evaluating the vulnerability of the telecommunications infrastructure to the full range of electromagnetic disruptive effects;

(2) identifying measures to mitigate these effects and providing timely information to the nation on the vulnerabilities and the mitigation measures; and

(3) initiating programs that provide connectivity assurance in the event of disruption such as facility hardening and Telecommunications Services Priority (TSP) service.

As a part of its vulnerability assessment activities, the NCS participated in the congressionally-mandated "Live Fire" exercise in 2000. "Live Fire" tested military communications equipment vulnerabilities to electromagnetic disruption; however, because much of the equipment used by the military corresponds to the commercial-off-the-shelf (COTS) equipment used in the civilian telecommunications infrastructure nationally, NCS' participation in this effort facilitated tests of equipment and systems common to the Internet .

Some of our efforts have included tests, simulations and analysis to assess the vulnerability to TEDE of:

?? High frequency Two-Way radio systems

?? Public Service Radio Systems

- ?? Public Telecommunications Network Switches (4E, 5E, DMS-100)
- ?? Public Telecommunications Network Buildings and Facilities
- ?? Satellite teleports
- ?? Signaling, Control and Data Acquisition systems (SCADA)
- ?? Internet edge equipments (routers, small computers)
- ?? Internet core equipments (Switching Systems)

At present, NCS is initiating an effort to evaluate the impact of TEDE from various modalities on a large backbone router.

IV. UNDERSTANDING THE THREAT BEYOND TEDE

As noted above, the NCS is responsible for assessing all threats to the national telecommunications infrastructure. Accordingly, recognizing communication's pivotal role in deterring and/or recovering from an attack, the NCS does not look at EMP or other sources of TEDE in a vacuum, but rather in the larger context of the full range of potential threats to the telecommunications infrastructure.

In the 1980s, government and industry focused their attention on the potential destruction and damage a major first strike could generate. As the Cold War threat abated, interest turned to other potential threats, including attacks in cyberspace, weapons of mass destruction, and terrorist acts. In the dynamic threat environment of today, it remains important for industry and government to assess potential threats to the national telecommunications infrastructure. In addition to EMP and TEDE, the NCS is involved with assessing other potential vulnerabilities of the infrastructure, such as:

- ?? Submarine Cable Landings
- ?? Telecom hotels
- ?? Convergence of the traditional telecommunication network with IP-based systems

Studies, modeling and simulation, and testing in these areas, as well as those involving potential EMP,, cyber, and/or physical attacks, alone or in combination with each other, will enable us to develop a fuller picture of the risk landscape as we build tools and programs to manage the risk to the nation's communications system.

Finally, as a part of the interim National Infrastructure Protection Plan (NIPP) recently released by DHS, the NCS serves as the Sector Specific Agency (SSA) for the telecommunications sector. In this lead role IAIP and NCS support and facilitate the organization of the sector to strengthen significantly the collaborative effort to identify vulnerabilities and develop mitigation strategies both within the sector as well as across sectors.

Although new, this activity is key to our ability to develop and refine cross-sector risk mitigation strategies as we work to address the risks posed by EMP and other sources of TEDE.

V. CONCLUSION

The NCS is responsible for assessing and mitigating vulnerabilities to the national telecommunications infrastructure. Accordingly, recognizing communication's pivotal role in deterring and/or recovering from an attack, the NCS has developed a vulnerability mitigation approach that is designed to address the entire spectrum of potential disruptions to the nation's telecommunications and ensure critical communications will be possible under all conditions.

The existence of EMP effects has been known since the 1940's and we have tested thoroughly our current generation of core telecommunications switches and have determined that there is minimal EMP effect on these switches. Furthermore, most of our core communications assets are in large, very well constructed facilities which provide a measure of shielding. This situation will evolve as we move to next generation networks (NGN) but we are monitoring this network evolution by testing critical components of the NGN and leveraging DoD testing.

In moving forward, the NCS has a proven history of preparing for and responding to all types of threats, founded in its ability to develop effective tools and programs combined with a trusted working relationship with industry to continually improve the hardness and survivability of the nation’s communications network.

This concludes my prepared statement. I would be happy to answer any questions you may have at this time.