National Security Telecommunications Advisory Committee (NSTAC) Research and Development Workshop

"A Year Later: R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness"

The Honorable Richard M. Russell
Keynote Speaker

Associate Director
Office of Science and Technology Policy
Executive Office of the President

October 28, 2004
Monterey, CA

Thank you Guy for that kind introduction. I am pleased to be here with all of you today at the sixth meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) Research and Development Exchange.

Since its creation by President Ronald Reagan in September 1982 the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

The R&D exchange is an invaluable forum for information sharing between industry, Government, and academia.

Three years have passed since the attacks of September 11, 2001. And while the danger has not passed, America today is safer and stronger because of the actions taken by President Bush to protect our country.

This Administration has taken unprecedented efforts to protect America's critical infrastructure against the threat of terrorism.

Already, the President has led the largest reorganization of government in more than 50 years; strengthened our intelligence capabilities; expanded support for first responders and state homeland security efforts; and increased the protection of our transportation systems, borders, ports, and critical infrastructure. NS/EP telecommunications has benefited from these efforts.

I would like to start by acknowledging the work of the NSTAC Next Generation Networks Task Force (NGNTF). The NGNTF was formed to study the impact of next generation networks on NS/EP communications. They have defined three critical areas and will:

1. Agree upon a high-level description of the expected network environment or ecosystem of next generation networks and its interdependencies;

2. Examine NS/EP user requirements, end-to-end user requirements, end-to-end services, and the interfaces and accountability among network participants and network layers; and,

3. Analyze relevant user scenarios and expected cyber threats.

Just a few weeks ago the NGNTF leadership was kind enough to provide OSTP with a number of near term recommendations. The recommendations couldn't have come at a better time considering our heightened security concerns.

The NGNTF notes that networks are already converging to form the Next Generation Network. For example, service providers offering IP based telephony and high-speed Internet connections are now a mainstay of NS/EP communications.

Broadband availability is speeding this new era of IP based communications.

Earlier this year, President Bush announced support to expand access to high-speed Internet in every part of America. The President called for universal, affordable access for broadband technology by the year 2007 and wants to make sure we give Americans plenty of technology choices when it comes to purchasing broadband.

Broadband technology will enhance our Nation's economic competitiveness and will help improve the delivery of education and health care. Broadband provides

Americans with high-speed Internet access connections that improve the Nation's economic productivity and offer life-enhancing applications, such as distance learning, remote medical diagnostics, and the ability to work from home more effectively.

And it is important to note that broadband not only strengthens our economy, it also strengthens our NS/EP communications capabilities by providing new innovative means of communication.

The Bush Administration has implemented a wide range of policy directives to create economic incentives, remove regulatory barriers, and promote new technologies to help make broadband available.

The Administration supports the Federal Communications' Commission's (FCC) decision to free new fiber-to-the-home investments from legacy regulations.

Deregulating new ultra-fast broadband infrastructure is working. Earlier this month some of the Nation's largest telecommunications companies announced that they plan to at least double the speed of their fiber rollout.

On Apri1 26, 2004, the President signed an Executive Memorandum that implements Federal rights-of-way reforms to streamline the process for broadband providers to get access to Federal lands to build high-speed infrastructure.

The reforms will help to minimize burdens on industry by simplifying and standardizing the rights-of-way process across all relevant agencies, while allowing agencies to use their resources wisely.

Another example of expanded opportunities for NS/EP communications is in the area of Wi-Fi and Wi-Max. The administration has made unprecedented strides in balancing the commercial spectrum needs of critical government agencies (including Department of Defense, Department of Transportation, and Department of Homeland Security) and commercial interests.

The Administration has identified and is working to make available a large block of both licensed and unlicensed spectrum for commercial applications. This spectrum will help speed the rollout of advanced wireless services such as EVDO and existing wireless applications such as Wi-Fi and new broadband technologies such as Wi-Max.

EVDO, Wi-Fi and Wi-Max technologies can provide a range of new NS/EP services for Federal, State, and local officials.

All of these efforts are working. Broadband penetration has grown from seven million lines in December 2000 to twenty-eight million in December 2003. The FCC just opened the entire country to broadband over power lines. Intel just announced it is partnering to roll-out Wi-Max.

I think we can all agree that the future is now and we need to begin an earnest effort toward better understanding the new threats and vulnerabilities presented by our new converged network environment.

That is why this year's R&D Exchange is so important.

The theme for this year's R&D exchange is "A Year Later: R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness".

The aim is to examine progress made since the last R&D exchange and consider the new challenges we face. This morning I want to share with you a few of the success stories since the last R&D exchange and present some of the ideas and plans we have for the future.

Let me start first with the overall Federal R&D budget...it is a good news story.

With the President's FY 2005 budget, total R&D investment during this Administration's first term will be increased 44% to a record $132 billion in 2005 as compared to $91 billion in 2005 as compared to $91 billion in FY 2001. That equates to increases of nearly 10% each year, significantly outpacing the FY 2005 overall "non-security" discretionary spending growth of 0.5%.

Science and technology drive economic growth. They help improve our health care, enhance our quality of life, and play an important role in securing the homeland and winning the war on terrorism. These increases reflect the Administration's appreciation of the importance of a strong national R&D enterprise for our current and future prosperity.

The President's FY 2005 budget request commits 13.5% of total discretionary outlays to R&D, the highest level in 37 years. Not since 1968, during the Apollo program, have we seen an investment in research and development of this magnitude. Of this amount, the budget commits 5.7% of total discretionary outlays to non-defense R&D, the third highest level in 25 years.

Let me highlight a few examples of ongoing Federal communication R&D. I think it will showcase the importance of the work and the large number of agencies involved.

At the National Communications System:

- The NCS developed a route diversity methodology that enables federal agencies to rapidly and accurately evaluate their existing communications infrastructure. Route diversity is communications routing between two points over physically disparate paths.

- The NCS is continuing to develop and refine telecommunications dependency models to determine the impact of Internet disruptions on selected critical infrastructures.

- Over the past year, Wireless Priority Service (WPS) has grown from one nationwide GSM carrier to four; from 3,000 users to over 11,000, and development has begun on CDMA platforms allowing Verizon Wireless and Sprint PCS to join the existing GSM carriers in offering WPS by the end of 2005.

Technology insertion within the wireless industry continues at a rate that requires ongoing research and planning for migration of existing WPS capabilities to 3rd Generation communications technologies.

As the wireless world merges with 3G architectures, NCS is developing research and development programs to include:

- Development of specific Industry Requirements for inclusion of WPS functionality within Universal Mobile Telecommunications System (UMTS)

- Development of Next Generation Network prototypes supporting WPS capabilities with NS/EP Voice Over IP (VoIP) applications, and

- Development of a wireless access framework for IP-based integrated voice and data NS/EP capabilities.

- The NCS is also working on an effort that will lead to assuring current NS/EP services, such as GETS, SRAS, WPS, and others, are available in the next generation networks.

At the Department of Commerce:

- DOC is conducting studies to develop tools that will improve the movement and communication of people within structures under emergency situations.

- They are also developing cyber security standards and guidelines.

At the Department of Defense:

- DoD has created the capability to link real-time intelligence threat information with the identification of potentially threatened critical infrastructure.

- They have delivered advances in the cyber arena in the critical realm of autonomous software agent technology including multi-agent system interoperability and cognitive agent architecture.

- They are also working on unmanned sensors that perform ad-hoc networking for autonomous self-healing routing and that provide network security including authentication, data integrity, and privacy.

- DoD is also developing realistic models of blast effects in urban and rural settings to forecast various impacts including limitations in movement of people and vehicles. This is particularly important to telecommunication restoration following a major incident.

At the Department of Energy:

- DOE has established a Critical Infrastructure Test Range, which includes a multi-laboratory National Supervisory Control and Data Acquisition (SCADA) Test Bed to investigate cyber vulnerabilities and evaluate technologies to protect existing process control systems as well as security enhancements for new systems.

At the Department of Homeland Security:

- DHS has produced an initial version of a fully integrated modeling, simulation and analysis system for use by National and regional leaders with decision support and planning capability across all 14 critical infrastructure sectors including telecommunications.

- DHS has also completed an analysis of how to protect SCADA systems and is establishing a virtual National Cyber Security R&D Center.

At the Department of Justice:

- DoJ has completed a study on the real cost and consequences of insider threats. The study included multiple industries and the impacts and losses associated with this type of attack.

At the Department of Transportation:

- DoT initiated Adaptive Quarantine research project to ensure that FAA is prepared to preempt active, passive, novel, insider and outsider cyber attacks against safety-critical and mission support networks and systems.

- DoT is also proceeding with a renewed examination of the security and control of highways, bridges, tunnels and reducing the risk of the highway system being used as a means to deliver an attack. As so many of our nations telecommunications pathways follow public right of ways, this research is very useful.

Finally, at the National Science Foundation:

- NSF has a variety of research projects that range from blast impacts, to physical infrastructure models for systems and structures, applications of nano- and biotechnology in protective materials and devices, social dynamics of terrorism, cybertrust and cybersecurity, new architectures for secure and resilient cyber and physical infrastructure systems, integrated computational and information resource development, and sensor networks.

- NSF is also investigating collaborative knowledge environments for the management of dynamic information, knowledge discovery; information extraction and fusion.

All these department and agency efforts, plus many others, directly or indirectly support NS/EP communications and the four aspects of trustworthiness (cyber security and software, human factors, physical security, and integration) that were raised in the last R&D exchange.

I'd like to now share with you what we, within the Federal government, believe to be the critical areas deserving special attention in the coming months and years.

The topics I am about to discuss were identified through the interagency R&D coordinating process under the President's National Science and Technology Council (NSTC) Infrastructure Subcommittee.

The topics are based on threat information and discussions with industry representatives, infrastructure owners and operators, and government officials. We believe these nine areas will contribute to a stronger NS/EP posture for the Nation.

1. **Detection and sensor systems and related integration needs.** We must have the systems and tools to detect and sense what is occurring or even being planned or considered. We need to develop advanced detection and interconnected sensor

systems for intuitive monitoring and rapid assessment of the condition of NS/EP communications and to identify approaching threats;

2. **Protection of assets and prevention of successful attacks against them.** We must have the systems, tools, methods and permissions to protect assets and NS/EP communications critical to the Nation. We need to develop effective protection of communication assets and prevent successful attacks against them with economically sustainable and operationally seamless measures;

3. **Security of entry portals and access to assets.** We must prevent unauthorized access to important places and systems. We need to develop smarter, more advanced security techniques for physical and cyber entry portals and access points.

4. **Insider threats.** We must address the dangerous situation of a trusted party who has passed all our controls, is inside our key assets and decides to betray that trust. We need to develop new methods to rapidly detect malicious behavior, track access to sensitive resources, and prevent actions damaging to NS/EP communications.

5. **Analysis and decision support systems.** We must have tools that can analyze complex and difficult problems and support our decision making in the most integrated and informed way possible. We need to develop analysis and decision support methods to provide a sound basis for setting infrastructure protection priorities;

6. **Response, recovery, and reconstitution.** If we do have a critical event, we need to be prepared to deal with the situation from initial response to final replacement of the lost asset or capability. We need to advance the response, recovery, and reconstitution capabilities for NS/EP physical and cyber networks, more rapidly restore the services they provide, and reconstitute the flow of communications;

7. **New and emerging threats and vulnerabilities.** We must recognize that there are new capabilities being developed by adversaries not previously considered or for which we may have insufficient knowledge and protection.

We need to anticipate and target new and emerging threats and deal with the new vulnerabilities that will be created as technology evolves and we shift emphasis and investments to higher levels of security.

8. **Advanced infrastructure architectures and system designs.** We must build new systems that do not have the faults or limitations of past systems and technologies that were created at a time when security was not as serious an issue.

We need to provide advanced NS/EP physical and communication architectures and networked system designs that are inherently more secure; and finally

9. **Human and social issues.** We must recognize the human assets are also elements of critical infrastructure. We need R&D on the best means to deal with the human-technology interface.

The areas I have described will likely require continuing work over many years. We also recognize that the results of research cannot simply be tossed over the wall with the hope that solutions will be automatically picked up by industry. We will need to work collaboratively to establish improved processes for

technology transfer and diffusion of federally funded technology and intellectual property into commercial products and services.

Before closing I would like to take a moment to express my sincere appreciation to the NSTAC for the many contributions it has made over the years to improve our national security posture. Your knowledge and expertise are invaluable to the President and the Nation.

A successful R&D agenda for NS/EP communications will require support, knowledge and contribution from almost every office in government and from you. I appreciate your help.

I look forward to taking your questions.