THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

RESEARCH AND DEVELOPMENT TASK FORCE

The Critical Importance of Testbeds for National Security and Emergency Preparedness Research and Development

May 11, 2005

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At its fifth Research and Development Exchange (RDX) Workshop in March 2003, the President's National Security Telecommunications Advisory Committee (NSTAC) realized the need for a large-scale testbed to be used as an environment in which to test national security and emergency preparedness (NS/EP) systems ("systems" herein meaning telecommunications, networking and related information technology systems) and critical infrastructure dependencies on such systems. In October 2004, the President's NSTAC held its sixth RDX Workshop in Monterey, California. Participants again emphasized the critical importance of supporting research and development (R&D) initiatives addressing emerging communications technologies through modeling, simulation, and testbeds.

Historically, testbeds have been developed to test new service offerings with the period of time between the definition of a new offering and full deployment being considerable. In the current environment, testbeds must be forward looking, swiftly incorporating new technologies and services before such innovations are introduced on a broad scale. In the future, expenses and network complexities will continue to grow. However, these increasing costs could be mitigated by the benefits of developing joint, collaborative, distributed testbeds. Such shared environments could increase cost-efficiency and improve technical effectiveness of the results.

Experience indicates that the private sector will form collaborative, multi-organization testbeds where they enhance the potential for broad deployment of the technologies and significant economic payback is possible. Investment in collaboration to the same extent is far less likely for the significantly smaller return offered by NS/EP systems and related critical infrastructure dependencies. Moreover, normal competitive forces are likely to make collaboration on unique critical infrastructure protection (CIP) technologies more difficult. Finally, the R&D environment for NS/EP and CIP technologies is generally driven by Government investment. Careful targeting of such investment can leverage the contributions of industry and academia through improved collaboration that would not otherwise occur.

The task force examined several examples of large-scale testbeds, including the following:

- **Alliance for Telecommunications Industry Solutions.** The Alliance for Telecommunications Industry Solutions Internetwork Interoperability Test Coordination Committee coordinates service providers, vendors, and manufacturers of telecommunications equipment to develop test scenarios and scripts and to perform tests in a controlled "rainy day" environment.

- **Gigabit Testbed Initiative.** The Gigabit Testbed Initiative, a major coordinated effort by approximately 40 organizations funded by the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency, was used to explore and examine advance networking issues, research gigabit networks, and experiment in areas such as weather modeling, chemical dynamics, radiation oncology, and geophysics data exploration.

- **Idaho National Engineering and Environmental Laboratory.** The Idaho National Engineering and Environmental Laboratory supports the United States Department of Energy with three testbed initiatives, including the Critical Infrastructure Test Range to test complex power systems, a Wireless Testbed, and a Cyber Testbed.

- **Cyber Defense Technology Experimental Research Network.** The NSF and the Department of Homeland Security developed the Cyber Defense Technology Experimental Research Network to examine cyber attacks and develop defenses against worm attacks and viruses.

- **Moonv6.** The Moonv6 initiative is a testbed developed by the University of New Hampshire InterOperability Laboratory and the Army's Joint Interoperability Test Command to provide a network pilot for Internet Protocol version 6 deployment in North America. As of March 2004, all branches of the military, 26 equipment vendors, and four commercial service providers are also involved in the testbed.

- **Network for Earthquake Engineering Simulation.** The NSF created the Network for Earthquake Engineering Simulation—a shared network of facilities, tools, a data repository, and simulation software—to improve understanding of earthquakes and their effects.

To meet the needs of the affected communities, a joint, collaborative, distributed industry, Government, and academia pilot testbed could advance the current state of NS/EP and CIP integration activities. As the potential benefits of such a testbed touch so many departments and agencies, effective implementation will require oversight and direction from the Executive Office of the President. Accordingly, the task force recommends that the Government—

- Convene a Government sponsored NS/EP Testbed Workshop, hosted by an appropriate technical organization (e.g., National Institute of Standards and Technology), and attended by appropriate, representative stakeholders from industry, Government, and academia to:

  – Validate the need for and value of a national, joint, collaborative, large-scale, distributed testbed with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection and recovery dependencies;

  – Develop a small set of alternative approaches for the envisioned testbed that consider organization, membership, and operation and management, including startup, growth and continuing operations and the respective roles of government, academia and industry participants;

  – Determine whether the envisioned testbed should ultimately transition entirely to the private sector and, if it should, recommend under what conditions that could occur; and

  - Estimate startup and recurring costs for the envisioned testbed, including direct Government funding and indirect financial support (e.g., research grants).

- Dependent on validation and supporting recommendations from the NS/EP Testbed Workshop, task and fund an appropriate Government organization with the mission to establish a national, joint, collaborative, large-scale, distributed testbed program with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection dependencies, including:

  - Identifying candidate member facilities, collaborating with participating members to develop methods to interconnect member facilities, generally administering test procedures, and monitoring the results;

  - Operating, to the extent feasible, on a fee-for-service and non-attribution basis, thereby encouraging participation by industry components;

  - Prioritizing NS/EP and related critical infrastructure dependencies use of the overall, distributed testbed facilities and allowing for secondary use for other collaborative testing purposes; and

  - Accounting for intellectual property rights and technology ownership.

1.0 INTRODUCTION

On March 13—14, 2003, the President's National Security Telecommunications Advisory Committee (NSTAC) held its fifth Research and Development Exchange (RDX) Workshop at the Georgia Tech Information Security Center at the Georgia Institute of Technology. The findings from the RDX Workshop included an expressed need to develop large-scale, distributed testbeds to examine national security and emergency preparedness (NS/EP) systems and related critical infrastructure dependencies. In October 2004, the President's NSTAC held its sixth RDX Workshop in Monterey, California. Participants again emphasized the critical importance of supporting research and development (R&D) initiatives addressing emerging communications technologies through modeling, simulation, and testbeds.

2.0 BENEFITS AND IMPACTS OF TESTBEDS

The R&D community is one of the Nation's greatest assets in combating evolving threats to its national security. In the constant search for new avenues to pursue R&D goals and improve NS/EP missions, testbeds have proven themselves to be a valuable and necessary tool. The accurate assessment of complex individual components, including a broad view of entire infrastructures, is essential to understanding the vulnerabilities and survivability of different systems. The current focus on critical infrastructure protection (CIP) and the interdependency of infrastructures has broadened the scope of NS/EP concerns to include the reliability of entire infrastructures, such as telecommunications, which are now considered a matter of national security. For this reason, R&D activities unique to NS/EP telecommunications should focus on those NS/EP services that currently afford priority, such as the Government Emergency Telecommunications Service (GETS), Special Routing Access Service (SRAS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS). The impact of the Next Generation Network (NGN) on these services and, more importantly, the assumption that there is a continuing need for these priority features in the NGN, should be a matter for further study.

Many systems that are integral to daily living, such as communications, power, water, and transportation, cannot be tested thoroughly in any other way than in a testbed model. Testbeds, which have traditionally been used for examining physical infrastructures, can also be implemented to assess cyber and network infrastructures and to study crisis management and response capabilities. As mechanisms that provide large-scale, real-world conditions in a controlled environment with user-controlled variables, testbeds serve as a primary model in achieving a better understanding of the vulnerabilities and survivability of systems that are relied upon everyday by everyone.

Historically, testbeds have been developed to test new service offerings with a considerable period of time between the definition of a new offering and full deployment. In the current environment, testbeds must be forward looking, swiftly incorporating new technologies and services before such innovations are introduced on a broad scale. In the future, expenses and network complexities will continue to grow. However, these increasing costs and complexities could be mitigated by the benefits of developing joint, collaborative, distributed testbeds. Such shared environments would reduce individual site complexities, increase cost-efficiency, and improve technical effectiveness.

Experience indicates that the private sector will form collaborative, multi-organization, distributed testbeds where they enhance the potential for broad deployment of the tested technologies and significant economic payback is possible. Investment in collaboration to the same extent is far less likely for the significantly smaller return offered by technologies unique to NS/EP and CIP. For critical infrastructures, normal competitive forces are likely to make such collaboration more difficult. Finally, the R&D environment for technologies unique to NS/EP and CIP is generally driven by Government investment. Careful targeting of such investment can leverage the contributions of industry and academia through improved collaboration that would not otherwise occur.

2.1 Partnerships and Non-technical Impacts

Testbeds provide an arena for industry, Government, and academia, and other relevant communities to partner together in efforts to better understand the strengths and weaknesses of basic and advanced systems. These partnerships can lead to the expedited development of innovative technologies that benefit from the use of large-scale testbeds and further advance the impacts of those developing systems and networks tested on them. The development of the testbed serves as a catalyst for industry to develop and provide the needed technology. Technologies can then move more quickly from the R&D stages into practical applications in different systems and infrastructures.

Partnerships on this scale can also lead to increased cooperation between and among industry sectors and Government. A distributed, collaborative testbed can include efforts from dozens of different organizations representing universities, industry and national laboratories, computer companies, telecommunications companies, service and software providers, defense and security companies, hardware providers, energy companies, and many others. A primary derivative impact of this type of coordinated effort is better communication among different elements of the R&D community. Testbeds allow different elements of the R&D community to better appreciate and understand each other's problems and can lead to new concepts and practices in developing integrated solutions.

Another important benefit of industry, Government, and academia partnering in distributed testbed efforts is the funding structure, in which Government funding can be used to leverage a large investment from industry. The value of a strong industry/Government partnership cannot be overestimated in this regard. Services, operations, facilities, technologies, and real systems that industry can supply for a testbed might otherwise be unavailable, unaffordable, or infeasible for the R&D community. Likewise, industry participants in a testbed can learn from collaboration with Government and academic researchers and use the lessons learned for potential real-world applications.

This paper does not consider the effects of attribution. However, concerns about intellectual property rights and technology ownership continue to be topics of long-standing sensitivity and lively debate.

2.2 Technical Impacts

Testbeds by definition provide a controlled, science-based environment to analyze, test, and examine different approaches, outcomes, and results as they relate to technical components of a system or infrastructure. They can lead to the development of new and accelerated technologies. Developing a testbed that incorporates all levels of a system—from devices, components, software, application layers, to entire networks and infrastructures—provides the most beneficial mechanism to analyze problems and identify integrated solutions.

By combining different elements of the R&D community within an environment that demands innovative technologies and concepts, a testbed can lead to the emergence of new technologies and concepts into the marketplace and/or into NS/EP applications. Network management, transmission, switching, hosting, applications and support tools, software development, telecommunications and computer hardware, crisis management, and response capabilities are some of the technical areas that can be adequately examined in a testbed model. Nearly any variable or scenario imaginable can be incorporated into these components in a testbed, giving researchers an accurate depiction of real world impacts on a real system in a controlled environment.

As technology advances and industry introduces new services, the testbed must include these innovations. For example, services such as Voice over Internet Protocol and new protocol directions will continue to affect the overall behavior of the communications network, and as these technologies evolve, their NS/EP implications must continue to be explored.

2.3 Examples of Large-Scale Testbeds

Seven large-scale testbed models are considered below. However, no single testbed has been identified with the capacity to emulate the entire telecommunications and public network. Further, the cost and time to create such a testbed from "scratch" precludes the creation of a unique testbed. Therefore, a study of the performance of an interconnected set of facilities into a single, collaborative, distributed testbed should be able to conclude if such a set could serve the national purpose. The discussion below describes some of the testbeds known by the task force.

2.3.1 The Alliance for Telecommunications Industry Solutions Testbed

The Alliance for Telecommunications Industry Solutions (ATIS) Internetwork Interoperability Test Coordination (IITC) Committee was formed at the request of the Federal Communications Commission's Network Reliability Council (NRC), later re-charted as the Network Reliability and Interoperability Council, in 1996. The IITC Committee (and its predecessor, the Internetwork Interoperability Test Plan Committee, or IITP Committee) was formed in response to two reports issued by the NRC strongly urging the industry—service providers and manufacturers—to initiate broad-based programs to prevent service outages. The ATIS IITC Committee coordinates service providers and vendors and manufacturers of telecommunications equipment to develop test scenarios and scripts and to perform tests in a controlled "rainy day" environment. The Committee facilitates the exchange of information regarding the interoperability of networks and equipment (hardware and software) along with specific applications toward maintaining the highest standards of network reliability and integrity.

More than 14 test phases have been conducted under the auspices of the IITC Committee. Tests accomplished during these phases used interconnected manufacturers' and service providers' laboratory facilities to execute the test plans. Tests conducted during this time include Common Channel Signaling, Local Number Portability, and Year 2000.

Recently, the Committee proposed the creation of an innovative testing network termed the Public Network Assurance (PNAS) Network. The PNAS Network would incorporate Quality Assurance Sites, which most service providers and manufacturers already operate as part of their International Organization for Standardization 9000 certification process. Members of the PNAS Network would permanently interconnect their test facilities. This interconnection would afford participants the capability to perform tests in a multi-technology network environment without each participant having to individually implement the necessary technologies, such as circuit switched, Internet Protocol, and wireless, in-house. As a consequence, each PNAS Network member would be providing the technologies with which that member was most familiar, using already purchased and operating test equipment. Involvement in the PNAS Network would permit each contributor to leverage his or her company's own internal knowledge of a technology in support of a testing program employing multiple technologies. Furthermore, each member would benefit through the sharing of the test results.

The PNAS Network would provide a suitable setting for the conduct of tests involving NS/EP scenarios. The multiple technologies available within the network would allow the testing, in a single interconnected network, of numerous types of network impairment or failure conditions likely to be experienced during an NS/EP event. Various types of network traffic and traffic patterns could be introduced into the simulated network. The effect on the traffic and the performance of the simulated network would be monitored, and the results reported. If properly configured, the PNAS Network could be used to verify the results obtained from computer-based network congestion or network failure simulations—information that could prove invaluable for predicting the response of the public and government-operated networks under extremely stressful conditions encountered during an NS/EP event. To date, discussions on the PNAS Network have been conducted only within the IITC Committee and, as such, the proposal has not been presented to or endorsed by ATIS or its Board of Directors.

2.3.2 The Gigabit Testbed Initiative

The Gigabit Testbed Initiative, a major coordinated effort by approximately 40 organizations funded by the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency, began in 1990. The Corporation for National Research Initiatives led the project, in coordination with participating organizations and the United States (U.S.) Government.

Five testbeds were established across the country as part of the Gigabit Testbed Initiative, and the testbeds were used, over the course of several years, to explore and examine advanced networking issues, research gigabit networks, and experiment in areas such as weather modeling, chemical dynamics, radiation oncology, and geophysics data exploration. Funding from the Government totaled about $20 million during 5 years, primarily to fund university research efforts. Industry participants contributed facilities, equipment, and personnel, valued at exponentially greater than the Government contribution, but at no cost to the project.

The lack of an available high-speed network proved, at the time, to be a hurdle to the project. However, development of such networks and equipment was already under way at several companies, and the Gigabit Testbed Initiative helped accelerate their deployment. Additionally, as a result of the project, two researchers from Carnegie-Mellon University started a local-area Asynchronous Transfer Mode (ATM) company that led to the emergence of high-speed local area networking capabilities and products. In direct response to the needs of the testbed, industry participants developed new software technologies that were deployed into the marketplace. The Gigabit Testbed Initiative also led to the development of high-speed network initiatives in three states. BellSouth and GTE[1] formed the North Carolina Information Highway and provided an ATM/Synchronous Optical Network throughout the state. The New York Network Exchange created an experimental network in New York, and Pacific Bell founded the California Research and Education Network.[2] As a result of the Gigabit Testbed Initiative, the defense and intelligence communities were able to use gigabit networking technology earlier than they anticipated for experimental networks and global-scale systems.

2.3.3 Idaho National Engineering and Environmental Laboratory

The Idaho National Engineering and Environmental Laboratory (INEEL), created in 1949, is a national laboratory that supports the U.S. Department of Energy (DOE). INEEL is operated for the DOE by Bechtel BWXT Idaho, LLC., which is composed of Bechtel National, Inc., BWX Technologies Co., and a consortium of eight regional universities known as the Inland Northwest Research Alliance.

The INEEL infrastructure is home to the Critical Infrastructure Test Range, which includes complex power systems, isolated power grids, numerous communications systems including a developing wireless testbed, command and control capabilities, information systems including a site-wide fiber system, numerous safeguards and security systems, transportation systems, power plants and supporting facilities, and medical and emergency response facilities. The 890-square-mile facility is a high-tech, critical infrastructure model that originally began as a testbed for nuclear reactors, and it now hosts testbeds ranging from nuclear waste treatment to wireless technologies.

The INEEL and Bechtel Telecommunications have established the Bechtel/INEEL Wireless Testbed, offering large-scale, independent, end-to-end testing of next generation wired, and wireless, communications infrastructure. The testing includes 3rd Generation/4th Generation cellular, land mobile radios, and wireless local area network systems.[3] The INEEL is also working with the National Communications System, the Department of Homeland Security (DHS), the Department of Defense (DOD), and other agencies to identify and assess testing needs for interoperability, standards verification, priority signaling, and other critical infrastructure concerns. With the construction and incorporation of three cell towers within existing communications infrastructure, potential areas of testing could also include the emergency power capabilities at base stations and survivability and vulnerabilities of 911 systems.

[1] GTE is now part of Verizon Communications.

[2] Corporation for National Research Initiatives. "The Gigabit Testbed Initiative," December 1996. http://www.cnri.reston.va.us/gigafr/

[3] Gatens, Kathy. "INEEL and Bechtel Telecom Collaborate on Wireless Testbed," June 2003. http://www.inel.gov/featurestories/06-03wireless.shtml

The INEEL also includes a Cyber Testbed that can support training, troubleshooting, equipment testing, production simulations, network software testing, new release upgrade testing, and beta testing. The testbed has different workstations to test different network hardware configurations, including different software systems. At any time, the systems can be configured to run real-time, real-world variables or technologies without any threat of impacting the mainstream user population. In addition, the Cyber Testbed conducts research in information assurance, intrusion protection, information forensics, and system recovery.

2.3.4 Cyber Defense Technology Experimental Research Network

The NSF, in conjunction with the DHS, developed the Cyber Defense Technology Experimental Research (DETER) Network in October 2003. The DETER is a large-scale, cyber testbed that will be used to examine cyber attacks and develop defenses against worm attacks and viruses. Researchers at the University of California, Berkeley, are partnering with the University of Southern California's Information Sciences Institute to develop the DETER network testbed.

This particular testbed arose from the need to model the detailed and heterogeneous nature of the Internet.[4] It will simulate the composition and operation of the entire Internet, including routers, hubs, and end users' computer desktops. In addition, the Pennsylvania State University, University of California, Davis, Purdue University, and the International Computer Science Institute were awarded funds to develop scenarios for testing and evaluating proposed defense systems.[5]

2.3.5 Moonv6

The Moonv6 initiative is a testbed developed to provide a network pilot for Internet Protocol version 6 (IPv6) deployment in Northern America. The University of New Hampshire InterOperability Laboratory (UNH-IOL) and the Army's Joint Interoperability Test Command collaborated on the project when it began in October 2003. As of March 2004, all branches of the military, 26 equipment vendors, and four commercial service providers were also involved in the testbed.[6]

Currently, Internet Protocol version 4 (IPv4) is used in Northern America; however, it is not known as a secure protocol, and the address space is limited. Therefore, IPv6 has been developed with much larger address space, better security, and other operational advantages. The Moonv6 testbed has been developed to provide a real-world environment to test vendor equipment. The network includes more than 80 servers and covers eight military, academic, and commercial sites from New Hampshire to California. The Moonv6 initiative is a key element in DOD plans to move its networks from IPv4 to IPv6 during then next 5 years.[7]

The Moonv6 testbed is being deployed in multiple phases. Phase one was completed in October 2003, when the network was linked to several academic and military sites to demonstrate the

[4] Yang, Sarah. UC BerkeleyNews. "NSF awards $5.46 million to UC Berkley and USC to build testbed for cyber war games," 15 October 2003.

[5] DFI International. Homeland Security: Update. "Biz/Gov Cooperation on Cyber Security," 20 November 2003.

[6] Cavazos, Jessy. "Moonv6: A Small Step for Man, A Giant Leap for Mankind," Frost & Sullivan, 11 March 2004. http://www.testandmeasurement.frost.com/prod/servlet/market-insight-top.pag?docid=11032689&ctxixpLink=FcmCtx1&ctxixpLabel=FcmCtx2

[7] Jackson, William. Government Computer News. "Moonv6 Testing to Continue," 9 December 2003, http://www.gcn.com/vol1_no1/daily-updates/24375-1.html>

network abilities. During this time, tests were successful for the File Transfer Protocol, hypertext Transfer Protocol (HTTP), Secure HTTP, Telnet, and Domain Name System applications. Phase two testing was completed in March 2004, where network routing protocols, applications, security, and transition mechanisms were successfully tested. Besides DOD, phase two participants included the North American IPv6 Task Force, the UNH-IOL, the Internet2 Consortium, and carriers AT&T Virtual Private Network Services, France Telecom R&D, and NTT DoCoMo of Japan. In November 2004, sixteen vendors participated in the third round of interoperability tests on Moonv6. The latest tests focused on voice, wireless, firewalls and a host of advanced network and application-layer tests.[8]

2.3.6 Network for Earthquake Engineering Simulation

The George E. Brown, Jr. Network for Earthquake Engineering Simulation (NEES) is a major research equipment and facility construction program of the NSF Engineering Directorate. NEES advances earthquake engineering research through the integration of experimentation, theory, data, and model-based simulation. The shared national network includes 15 large-scale advanced experimentation laboratories at major universities across the Nation and integrates those facilities with collaborative tools, a central data repository, and earthquake simulation software bridged together by the high-speed Internet2 NEESgrid. The laboratories fall into five general categories: shake tables, tsunami wave basin, geotechnical centrifuges, field experimentation and monitoring, and large-scale laboratory experimentation.

The NEESgrid is a communications web that facilitates integration of diverse components and allows off-site researchers to collaborate and interact in real time with any of the networked sites. This pioneering cyber infrastructure connects earthquake engineering researchers throughout the United States and the world. Integrating real-life and computational simulations, NEESgrid software brings together various components to share knowledge and enables researchers to breach traditional disciplinary and geographical barriers to design innovative, safer civil infrastructure.[9]

The goal of the NEES project is to provide a national network of geographically distributed, shared-use, next-generation experimental research equipment sites, which will give researchers the tools to learn how earthquakes and tsunamis impact the buildings, bridges, utility systems and other critical components of today's society and develop better and more cost-effective ways of mitigating earthquake damage. This research might also be applied to help prevent infrastructure damage from other natural disasters and terrorism. The network enables participation from a broader earthquake engineering community, including educators, students, practitioners, and public sector organizations and individuals, who will have access to the equipment, data, models, and software from NEES. The development phase was completed in 2004 and NEES will be operational until 2014.

2.3.7 Institute for Telecommunication Sciences

The Institute for Telecommunication Sciences (ITS) is the research and engineering arm of the National Telecommunications and Information Administration (NTIA) of the Department of

[8] Moon v6 Network Project. "November Test Set Observations and Results," November 2006
http://www.moonv6.com/Moonv6-Nov2004.pdf

[9] Chamot, Josh. National Science Foundation Website. "Network for Earthquake Engineering Simulation: A Special Report"

Commerce. Activities at the Institute are undertaken through a combination of programs sponsored by the Department of Commerce and other Federal agencies, and through cooperative research agreements with the private sector. Other major sponsors include the National Institute of Science and Technology (NIST) Office of Law Enforcement Standards, DHS, the Department of Transportation, the National Weather Service, and the U.S. Coast Guard. Cooperative research with telecommunication companies and manufacturers supports technology transfer and commercialization of telecommunications products and services, which are major goals of the Department of Commerce. ITS has cooperative R&D agreements with large established companies as well as small, start-up companies. Partnerships such as these enhance synergies between entrepreneurial ventures and broad national goals.

ITS expertise includes areas such as radio research fundamentals and spectrum measurement, communication systems and networks, standards development, wireless voice/data systems and emerging technologies, audio and video quality research, and electromagnetic modeling and analysis. The Table Mountain Field Site and Radio Quiet Zone is a unique 1800-acre radio research facility north of Boulder, Colorado. The site is designated as a Radio Quiet Zone where the magnitude of strong external signals is restricted to minimize radio frequency (RF) interference to sensitive research projects.

Several testbeds within ITS provide for the advancement of telecommunications technologies, including next generation hybrid (wireless/wireline) networks. An 802.11 testbed allows for a common network for research in the areas of wireless networks and wireless network access technologies. ITS has set up multiple long-range outdoor links to explore the impact of environmental factors on communications over 802.11 based carriers. The links consist of 1, 10, and 11 mile distances. This testbed utilizes no proprietary technology, but is based on commercial off the shelf (COTS) equipment. A high gain directional antenna is employed at each of the links to provide the required directionality and gain. The experimental installation is capable of providing information about the RF characteristics of the channel as well as multiple packet network parameters. For non real-time transmission control protocol (TCP) networks, this includes throughput measurements and for real-time transmissions measurements like delay, jitter, and instantaneous packet loss are available. The Advanced Antenna Testbed (ATB) is a multi-channel test facility based on ITS digital sampling channel probe technology. The ATB provides common reference sites for evaluating next-generation antenna systems. Additionally, the Interoperability Research Laboratory provides a test capability for measuring the performance of Project 25 land-mobile radio systems that comply with Telecommunications Industry Association (TIA) 102 and TIA-603 series of standards.

3.0 TESTBED FINDINGS

For several years, the NSTAC, via its R&D Task Force, has worked to ensure NS/EP functions and capabilities are embedded in the Nation’s telecommunications infrastructure. The concept of an NS/EP-specific testbed was first raised at the NSTAC’s 1998 RDX Workshop at Purdue University in West Lafayette, Indiana, when participants emphasized the need for the development of joint or virtual “neutral party” testbeds that would allow all organizations—industry, Government, academia, or others—to test products in realistic environments. At the 1999 RDX Workshop at the University of Tulsa in Tulsa, Oklahoma, participants discussed the need to develop better testing and evaluation mechanisms to reduce the vulnerabilities of the telecommunications network introduced by malicious software. At the 2003 RDX Workshop in Atlanta, Georgia, participants noted that integration efforts were not progressing as quickly as they should and again discussed specific mechanisms and strategies to accelerate the transition and integration of innovative R&D to build trusted tools and systems to support future NS/EP telecommunications infrastructures and applications. Consensus from the participants indicated a need for rapid prototyping and the development of testbeds to study the need and feasibility of integrating NS/EP-related systems into the evolving telecommunications network.

Most recently, at the 2004 RDX Workshop in Monterey, California, participants focused on the need for concerted telecommunications R&D initiatives that would address the complex realities associated with the transition to a converged network. In his keynote address, Mr. Richard Russell, Associate Director of Technology, Office of Science and Technology Policy (OSTP), highlighted examples of Federal programs and initiatives at many of the departments and agencies that support NS/EP telecommunications, including the Department of Transportation's adaptive quarantine research project, and the DOE's multi-laboratory supervisory control and data acquisition (SCADA) testbed. Additionally, Workshop participants indicated that it was critically important to understand interdependencies, associated threats, and correlated points of failure across critical infrastructures. Among their findings, they discussed several overriding issues for the R&D community, including new modeling and testing strategies for emerging technologies and the need for additional testbeds.

As prescribed in the findings from the previous RDX Workshops, including the most recent, a pressing need exists to develop large-scale NS/EP-related, distributed testbeds. This will require significant integration and partnering between industry, Government, and the academic R&D communities. The challenge will be to create an environment that attracts the operations elements of industry to provide resources and assets, including people, access to real systems, and funding to conduct tests in collaborative and innovative research projects, pilots, and testbeds. Because of the unique nature of requirements to assign some NS/EP services priority within the NGN, Government must be willing to absorb the cost of this R&D, including the interconnection of the distributed testbeds and the expense of using lab resources of the participants. For NS/EP unique technologies, Government must also assume the cost of standards development, feature development by the vendors, and service implementation and on-going operation and administration by the telecommunication service providers. Since Government controls the customer base for such services, it is impossible for industry to develop a persuasive business case for these services given that they will not have broad marketability. Developing an R&D strategy for large-scale testbeds that includes public and private stakeholders and uses participation from different sectors will enable critical NS/EP needs and requirements to be tested and properly integrated into the telecommunications network. Additionally, as the potential benefits of a distributed testbed touch so many departments and agencies within the Federal Government, effective implementation will require oversight and direction from the Executive Office of the President (EOP).

4.0 RECOMMENDATIONS

To meet the needs of the NS/EP community, a joint, collaborative industry, Government, and academia pilot testbed could advance the current state of NS/EP integration activities. As the potential benefits of such a testbed touch so many departments and agencies, effective implementation will require oversight and direction from the EOP. Accordingly, the task force recommends that the Government —

- Convene a Government sponsored NS/EP Testbed Workshop, hosted by an appropriate technical organization (e.g., NIST), and attended by appropriate, representative stakeholders from industry, Government, and academia to:

  - Validate the need for and value of a national, joint, collaborative, large-scale, distributed testbed with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection and recovery dependencies;

  - Develop a small set of alternative approaches for the envisioned testbed that consider organization, membership, and operation and management, including startup, growth and continuing operations and the respective roles of Government, academia and industry participants;

  - Determine whether the envisioned testbed should ultimately transition entirely to the private sector and, if it should, recommend under what conditions that could occur; and

  - Estimate startup and recurring costs for the envisioned testbed, including direct Government funding and indirect financial support (e.g., research grants).

- Dependent on affirmation and supporting recommendations from the NS/EP Testbed Workshop, task and fund an appropriate government organization with the mission to establish a national, joint, collaborative, large-scale, distributed testbed program with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection dependencies, including:

  - Identifying candidate member facilities, collaborating with participating members to develop methods to interconnect member facilities, generally administering test procedures, and monitoring the results;

  - Operating, to the extent feasible, on a fee-for-service and non-attribution basis, thereby encouraging participation by industry components;

  - Prioritizing NS/EP and critical infrastructure use of the overall testbed facilities and allowing for secondary use for other collaborative testing purposes; and

  - Accounting for intellectual property rights and technology ownership.

APPENDIX A

TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Computer Sciences Corporation	Mr. Guy Copeland, Chair
Nortel	Dr. John Edwards, Vice Chair
Science Applications International Corporation	Mr. Hank Kluepfel, Vice Chair
BellSouth	Mr. David Barron
The Boeing Company	Mr. Robert Steele
Lucent Technologies	Mr. Kevin Kelly
Motorola	Dr. Robert Kubik
Microsoft Corporation	Mr. Ted Tanner
Qwest Communications	Mr. Jon Lofstedt
SBC Communications Inc.	Ms. Rosemary Leffler
VeriSign, Inc.	Mr. Michael Aisenberg
Verizon Communications	Mr. James Bean

OTHER PARTICIPANTS

Georgia Tech University	Dr. Seymour Goodman
Lucent Technologies	Mr. Frank Cantarelli

GOVERNMENT PARTICIPANTS

Department of Homeland Security, Science and Technology Directorate	Dr. Simon Szykman
Department of Homeland Security, Office of the Manager, National Communications System	Ms. DeJuan Price