Statement of Dr. George O. Strawn
Director, National Coordination Office for
Networking and Information Technology Research and Development
to the Joint Meeting of the Subcommittee on Technology and Innovation
and the Subcommittee on Research and Science Education of the
Committee on Science, Space, and Technology
U.S. House of Representatives
May 25, 2011

Good morning. I am George Strawn, Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD). With my colleague, Dr. Farnam Jahanian of the National Science Foundation (NSF), I co-chair the NITRD Subcommittee of the National Science and Technology Council's (NSTC) Committee on Technology. I want to thank Chairman Brooks and Chairman Quayle, Ranking Members Lipinski and Wu, and members of the Subcommittees for the opportunity to come before you today to discuss protecting information in the digital age and NITRD's role in Federal efforts to improve cybersecurity.

The NITRD Program – now in its 20th year – provides a coordinated view of the Government's portfolio of unclassified investments in fundamental, long-term research and development (R&D) in advanced networking and information technology (IT), including cybersecurity and information assurance. All of the research reported in this portfolio is managed, selected, and funded by one or more of the 14 member agencies under their own individual appropriations. In addition to cybersecurity, the Program's current research areas are high-end computing, large-scale networking, human-computer interaction and information management, high-confidence software and systems, software design and productivity, and socioeconomic, education, and workforce implications of IT. Advances in these areas further our nation's goals for national defense and national security, economic competitiveness, energy and the environment, health care, and science and engineering leadership.

Response to the Committee Request

Your invitation to testify here today asked me to address five specific questions. But I would like to preface my comments with the general statement that the NITRD agencies strongly concur that improving the overall security of our cyber infrastructure – including computing systems, mobile devices, networks, digitally controlled critical infrastructures, and the vast quantities of information that now flow through cyberspace – is a critical national challenge. It is imperative that we successfully address this challenge, not only to strengthen our national security but also to sustain the technological leadership that drives our economic innovation, global competitiveness, and science and engineering preeminence, and supports our quality of life as Americans.

The 2010 strategic plan for NITRD developed by the Program's 14 member agencies (and now awaiting White House sign-off) describes "trust and confidence" in our

systems, networks, and information as one of three fundamental prerequisites for a bright U.S. future. The NITRD Plan states:

> "The perspective of the NITRD agencies is that one of the most significant tests of technological leadership in the years ahead will be the ability to engineer and build IT systems that inspire high levels of confidence because they function as intended – safely, securely, reliably, and cost-effectively. Fundamental research to ensure that digital networks, systems, devices, applications, and communications processes earn and deserve the trust and confidence of society thus constitutes an essential foundation for the Nation's future."

(1) Please provide a brief overview of the federal government's cybersecurity efforts and how research and development is integrated into those efforts;

The 14 NITRD member agencies and some two dozen other participating agencies represent the broad spectrum of Federal interests in networking and information technology R&D related to cybersecurity – such as national defense and intelligence capabilities; health records privacy and confidentiality; the security of the national power grid; the reliability and functionality of the air-traffic-control system; the integrity and persistence of scientific research data; and the maintenance of secure real-time communications systems in emergency response, weather forecasting, and the financial markets; and many other key national purposes. The role of the NITRD Program in advancing the Government's cybersecurity efforts is to identify the technologically hard but critical problems and coordinate effective research and development to address them.

The Program's framework of regular and ongoing interagency coordination enables the varied agencies to identify significant leverage, target common critical needs, avoid duplication of effort, maximize resource sharing, and partner in investments to pursue higher-level goals. Moreover, because NITRD research is performed in universities, Federal research centers and laboratories, Federally funded R&D centers, and in partnerships with private companies and nonprofit organizations across the country, continuous interaction, information exchange, and feedback takes place, providing new perspectives and insights to both Federal and private-sector stakeholders.

Initiatives #4 and 9 of the Comprehensive National Cybersecurity Initiative (CNCI) called for coordinating R&D efforts and developing enduring "leap-ahead" technology, strategies, and programs. The President's Cyberspace Policy Review builds on these goals to include developing a framework for research and development strategies that focus on game-changing technologies. The NITRD program has a key role in pursuing these goals. Research coordination has been strengthened through the establishment of a Cybersecurity and Information Assurance (CSIA) Senior Steering Group (SSG; made up of budget-level officials). The SSG, in close cooperation with the Special Cyber Operations Research and Engineering group (SCORE: convened by the Office of Science and Technology Policy and the Office of the Director of National Intelligence) enables effective coordination between the classified and unclassified Federal IT security R&D portfolios. This strong framework for coordination and the partnerships it has engendered

enabled a comprehensive response to the near- and mid-term action items of the Cyberspace Policy Review as described in my answer to question #2 below.

(2) Describe your office's role in meeting the objectives outlined in the near-term and mid-term action plans included in the Cyberspace Policy Review, detail past progress and future plans for meeting the objectives outlined in the review;

While individual members of the NITRD community are likely to be involved in multiple elements of the near- and mid-term action plans, I would like to focus on three of these in which NITRD, supported by the NCO, has a prominent role:

Near-term Action Plan #9: Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community with access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

Over the last two years, NITRD's CSIA IWG and SSG have engaged in an intensive round of public discussions, brainstorming, and thorough technical examinations of cybersecurity issues in order to develop just such a game-changing R&D framework. The result is the soon-to-be-released Federal cybersecurity R&D strategic plan, "*Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*." The strategic plan provides game-changing themes to direct R&D efforts towards understanding the underlying root causes of known current threats with the goal of disrupting the status quo with radically different approaches. The four themes serve as a framework to unify cybersecurity R&D activities. The themes are: Designed-In Security (DIS), Tailored Trustworthy Spaces (TTS), Moving Target (MT), and Cyber Economic Incentives (CEI), with focus areas on wireless mobile networks in the TTS theme and nature-inspired solutions and a deep understanding of cyberspace in the MT theme.

The process of building the R&D strategic plan began with a Leap-Ahead Initiative, developed by the White House Office of Science and Technology Policy (OSTP) and the CSIA SSG. The initiative solicited public inputs and received more than 200 responses on ideas for how to change the cybersecurity landscape. These ideas were distilled into five fundamentally game-changing concepts in cybersecurity and provided as inputs to the National Cyber Leap Year Summit held August 17-19, 2009, in Arlington, Virginia. The summit gathered innovators from the academic and commercial sectors to explore these concepts. The outcomes of the summit were distilled into the three game-changing R&D themes. In FY 2010, the themes were provided as inputs to the Administration's cybersecurity R&D agenda and introduced to the research community as strategies for public-private actions to secure the Nation's digital future. Since the Summit, as the understanding of cyberspace has evolved, a new theme – Designed-In Security (DIS) – has been added to the Federal cybersecurity R&D plan. The next phase in this effort will be to develop, with private-sector input, a roadmap to implement the strategic plan.

An important new strategic thrust introduced in the Federal cybersecurity R&D plan is to develop a science of security. A science of security is needed to ground research efforts and would have the potential of producing hypotheses subject to experimental validation and universal concepts that are predictive and transcend specific systems, attacks, and defenses. Within 10 years, the aim is to develop a scientific framework that applies to real-world settings and provides explanatory value. The CSIA agencies are working with private-sector stakeholders to identify real-world data sets that can be used for research experimentation and testing without compromising privacy or proprietary and sensitive information.

Mid-term Action Plan #3: Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.

The portfolio of research and development activities sponsored by the NITRD agencies constitutes this country's only full-spectrum IT R&D enterprise, and thus these activities represent a unique resource for seeding U.S. innovation of all kinds. In addition, NITRD funding represents the single largest source of support for the education and training of new generations not only of U.S. IT research leaders but of IT entrepreneurs and technical experts in many fields of endeavor. Our Nation's investments in this NITRD portfolio in general, and in its cybersecurity-related components in particular, have increased along with the critical roles that these technologies play in our information age economy. NITRD agencies now support multiple NCO-coordinated activities impacting research and development, education, and workforce readiness for cybersecurity and the protection of our Nation's critical infrastructure and its entire economy. Nevertheless, all recognize that the challenge remains large and growing.

Mid-term Action Plan #11: Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.

The forthcoming Federal cybersecurity R&D plan specifically addresses the need to accelerate the transition of R&D to practice. It states that an explicit, coordinated process that transitions the fruits of research into practice is essential if Federal cybersecurity R&D investments are to have significant, long-lasting impact. As part of the transition to practice activities, the Federal cybersecurity research community plans to participate in activities related to technology discovery; test and evaluation; and transition, adoption, and commercialization. Planned activities in technology discovery include, for example, participation in the Information Technology Security Entrepreneurs' Forum (ITSEF) and Defense Venture Catalyst Initiative (DeVenCI). In test and evaluation, NITRD agencies plan to leverage available operational and next-generation networked environments to support experimental deployment, test, and evaluation of novel security technologies in realistic settings in both public- and private-sector environments. For transition, adoption, and commercialization, NITRD agencies plan to participate in the System Integrator Forum (SIF) and Small Business Innovative Research (SBIR) Conferences.

As part of their activities to engage with the cybersecurity research community, senior Federal agency cybersecurity officials are presenting the framework for R&D strategies and themes articulated in the strategic plan to researchers attending the annual IEEE Security and Privacy Symposium, May 22-25, 2011 in Oakland, California.

I would like to note here that the transition to practice is also being addressed by NITRD's Large Scale Networking (LSN) agencies. They have developed an innovative network-performance monitoring technology called perfSONAR, which provides network managers with unprecedented capabilities to evaluate how well their networks are functioning, to find problems, and to recognize anomalies in network security. The LSN agencies are now working with private-sector networks and international research network partners to implement deployment of this powerful new tool. The LSN teams, JET (Joint Engineering Team) and MAGIC (Middleware and Grid Infrastructure Coordination), are also closely involved in transition to practice through their testing and implementation in advanced research networks of security-enhancing technologies such as federated identity management, IPv6, and DNSSec.

(3) Please discuss how cybersecurity research and development and education and workforce activities across the federal agencies are coordinated and implemented through the NITRD National Coordinating Office;

NITRD activities are supported by the NCO, which provides logistics as well as expert technical coordinators to support the operations of the Subcommittee and an evolving collection of working groups (such as the CSIA IWG) in which the agencies participate to coordinate their own research and development activities and to plan and oversee joint activities when appropriate. They regularly share plans and developments, host workshops, author papers, and interact with the academic and private sectors as a means of defining and operating the most effective programs of research and development attainable in their subject areas.

The following snapshot examples illustrate how such interagency collaboration can lead to substantially better results in research and development as well as education:

- Partnership for Cyberspace Innovation – a partnership of NIST, the Science and Technology Directorate of DHS, and the Financial Services Sector Coordinating Council (FSSCC), with the goal of speeding the commercialization of cybersecurity research innovations that support our Nation's critical infrastructures. This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures such as online health services, the Smart Grid, water, and transportation.
- Middleware And Grid Infrastructure Coordination (MAGIC) Team – a partnership of agencies and Federal laboratories including ANL, DHS, DOE/SC, FNAL, LANL, LBL, NASA, NIH, NIST, NOAA, NSF, PNNL, and UCAR, and their industry partners, which improves the Nation's cybersecurity and privacy environment through research, development, and promotion of Identity Management best practices, standards, and community outreach.

- Joint Engineering Team (JET) – a partnership of agency and research networks including DoD, DOE, NASA, NSF, Internet2, and National Lambda Rail that seeks to improve performance as well as security by coordinating networking testbeds (for optical, cloud, architecture, and networking research) and promoting the deployment in advanced networks of more secure technologies such as IPv6 and DNSSec.
- National Initiative for Cybersecurity Education (NICE) – a partnership led by NIST and including DHS, DoD, NSF, ED, OPM, NSA, DOJ, NSA, ODNI, and others, with the goal of establishing an operational, sustainable, and continually improving cybersecurity education program to foster sound cyber practices that will enhance the Nation's security.
- The SEW-Education subgroup of the NITRD SEW Coordinating Group, with a focus on raising the national profile of computing-related knowledge through fundamental changes in K-12 computer science education. This new group, one of whose co-chairs leads the NIST cybersecurity education initiative, is a participant in the NICE program and is now developing its plan of action.

As Director of the NCO for NITRD, it is always a pleasure for me to describe how, by facilitating the collaborative efforts of representatives from many agencies – by arranging meetings and teleconferences, hosting/supporting workshops and conferences, preparing "zero-th" drafts of brainstorming documents, communicating regularly with NITRD participants, and the like – the NCO helps empower the collective intelligence of the NITRD community to accomplish together far more than any single agency could on its own. I believe the NITRD model of cooperation among very disparate agencies truly works, and has led to significant improvements in research and development as well as strategic planning and for cybersecurity.

(4) Please provide feedback on H.R. 4061, the Cybersecurity Enhancement Act of 2009, from the 111th Congress as it pertains to your office by commenting on the merits of that bill and any areas that you see room for improvement or changes; and

As is described above, the NITRD Program currently supports an extensive process of coordination and planning across the Federal agencies involved in research and development. This process has led to the development of the Federal cybersecurity R&D strategic plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, which defines a set of interrelated priorities for the agencies of the U.S. government that conduct or sponsor R&D in cybersecurity. This plan aligns well with the planning objectives noted in H.R. 4061, and is to be followed by coordinated development of a roadmap of steps guiding its implementation. In this process, NITRD and its agency members have hosted workshops for the exchange of information with academia and the private sector and have requested comments from a wide range of stakeholders including the public. NITRD member agencies are beginning to use language and direction from this coordinated plan in agency research and development activities. We greatly appreciate the interest of the Committee and the Subcommittees represented here today and share your commitment to research and

development for better cybersecurity. We look forward to continuing to work closely with you on this shared goal with or without any additional legislation.

(5) How would the Administration's proposed legislation impact the NITRD program and the Nation's cybersecurity research and development, education, and workforce needs?

The proposed legislation directly promotes greater cybersecurity research and development, education, and workforce needs as one of five parts of its basic approach as outlined in SEC 243 (b). The same section promotes the development and implementation of technical capabilities in support of national cybersecurity goals. Many such technical capabilities of the future will represent the practical implementations of the results of ongoing Federal research and development coordinated in the NITRD Program.

The legislation also calls for research and development in cybersecurity in SEC 243 (c) as an important component of a multifaceted program to foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting Federal systems and critical information infrastructure, including comprehensive protective capabilities and other technological solutions. Such research and development will be essential not only to better meet existing threats, but to provide the technical and scientific foundation for capabilities to meet emerging threats and developments. The coordination of such research and development, and the transition to practice of its successful results, are key components of the NITRD contributions to improving cybersecurity. The proposed legislation for cybersecurity research and development, as outlined in Sections 243 (c) and (d), thus is consistent and aligns with the R&D coordination in which the NITRD Program engages.