Testimony of

Farnam Jahanian, Ph.D.
Assistant Director
Computer and Information Science and Engineering Directorate

Before the

Committee on Science, Space, and Technology
Subcommittee on Technology and Innovation
And the
Subcommittee on Research and Science Education
U.S. House of Representatives

May 25, 2011

Protecting Information in the Digital Age: Federal Cyber Security Research & Development Efforts

Good afternoon, Chairman Quayle and Chairman Brooks, Ranking Members Wu and Lipinski, and members of the Subcommittees. My name is Farnam Jahanian and I am the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

I welcome this opportunity to highlight NSF's investments in cyber security research and education. NSF aims to fund cyber security research at the frontiers of knowledge, to capitalize on the intellectual capacity of both young and experienced investigators in our Nation's academic and research institutions, and to partner with other U.S. government agencies and private sector and international organizations to meet the challenges of securing cyberspace. It is important to note that the many powerful information technologies (IT) deployed today around the world capitalize on fundamental research outcomes generated decades ago. An effective national strategy for achieving a cyberspace that is deemed “trustworthy” must include investments in fundamental, unclassified, long-term research. These investments will allow our society to continue to benefit from a robust, secure, dependable cyber infrastructure that supports all application sectors, including those on which our lives depend.

Allow me to share with you some examples of the important contributions made to date by the research community with both NSF and other Federal support. They include:

- Cryptographic schemes and cryptographic-based authentication, enabling today's Internet commerce, supporting secure digital signatures and online credit card transactions;
- Program analyses and verification techniques, enabling the early detection of software vulnerabilities and flaws, which can prevent cyber attacks, such as phishing, worms and botnets;
- New approaches to prevent and mitigate distributed denial of service attacks have helped secure Internet's underlying infrastructure;
- Approaches to identify exploitable flaws in cyber-enabled systems, including automotive control software and medical device software, that have alerted industry to the need for secure software and system development practices;
- Technology to detect and defeat "drive-by downloads" from malicious websites makes web browsing safer for the public;
- Innovative machine learning and data mining approaches used in spam filtering, and methods for detecting attacks, such as those involving credit card fraud;
- CAPTCHAs, the distorted text that only humans—not machines or bots—can decipher, to ensure that it is indeed a human, and not a bot, who is buying a ticket on-line or setting up an email account;
- Open source tools that enable rapid analysis of malware allow for quick detection and mitigation and new methods to study botnets reveal the structure of the underground economy, allowing investigators to make attribution and prevent future attacks from the same sources;
- Better understanding of how humans respond to software security warnings gives designers new models for designing usable and secure systems; and
- The underpinnings for fully homomorphic encryption, which means that we may eventually be able to perform encrypted computations on untrusted platforms (such as on a distributed "cloud" platform), just as today we can send encrypted communications over untrusted networks.

The research contributions listed above and other research outcomes and innovations developed with funding from NSF and other Federal partners are now being used by the private sector and government agencies to protect the nation's cyber infrastructure. Moreover, in recent years, NSF-funded research activities have led to the formation of start-up companies in the IT sector that bring innovative solutions and technologies to the marketplace, fueling job growth, and helping to protect cyber space. By promoting a healthy connection between academia and companies, NSF further enhances its research portfolio in trustworthy computing with foundational concepts and new ideas that are directly relevant to the commercial sector.

While the advances in cyber security research and development (R&D) are many, including those mentioned above, the Nation needs to continue its investments in long-term, game-changing research if our cyber systems are to be trustworthy. As you know, every day, we learn about more sophisticated and dangerous attacks. Why is the cyber security challenge so hard? The general answer is that attacks and defenses co-evolve: a system that was secure yesterday might no longer be secure tomorrow. More specific responses to this question include:

- The technology base of our systems is frequently updated to improve functionality, availability, and/or performance. New systems introduce new vulnerabilities that need new defenses.
- The settings in which our computing systems are deployed and the functionality they provide are not static. With new computing models/platforms, like cloud computing and smart phones, come new content and function, which in turn creates new incentives for attack and disruption.

- The sophistication of attackers is increasing as well as their sheer number and the specificity of their targets.
- Achieving system trustworthiness is not purely a technology problem. System developers, purchasers, operators and users all have a role to play in system security, and ways to incentivize them are required. Security mechanisms that are not convenient will be ignored or circumvented; security mechanisms that are difficult to understand will be ignored.
- Humans can be tricked into performing insecure actions or divulging confidential information through various ruses of clever adversaries.

Emerging Threats

The Internet plays a critical role in tightly integrating the economic, political, and social fabric of global society. These interdependencies leave the Nation vulnerable to a wide range of threats that challenge the security, reliability, availability, and overall trustworthiness of all information technology resources.

An evolution of means and motives. In retrospect, early threats, such as first-generation viruses and worms, while costly and dangerous, did not seriously challenge the availability or security of the Internet. In practice, many attackers simply engaged in acts of vandalism. Quickly, however, global Internet threats underwent a profound transformation -- from attacks designed solely to disable all or part of the Internet to those that specifically targeted people and organizations. Driven in large part by financial incentives, attackers learned that these systems offered a valuable resource, both in terms of the personal data they contained and as a resource that could be used for future attacks. Networks of these compromised machines, or botnets, have become the delivery platform of choice and fuel a variety of threats, such as SPAM, identity theft, phishing, and Distributed Denial of Service Attacks (DDoS).

These threats continue to evolve both in the motives of the attackers and the means they employ to achieve their goals. Today, exclusively economic motivations have given way to a wide range of goals, including the desire to project political will into cyber-space, such as the denial of service attacks that shadowed the clashes between Russia and Georgia over the region of South Ossetia in 2008, and the Ghostnet cyber spying operation that infiltrated the computers of embassies, foreign ministries, and the offices of the Dalai Lama in 2009. Both instances serve to highlight the scope of this problem and the difficulty in discovering the persons or nations that launched the attacks. With these changing motivations, attackers continue to innovate with new methods. Attacks continue to increase in size. They are more targeted, sophisticated, and stealthy. Furthermore, these attacks are more effective, propagating through high-level applications and through social engineering.

Future security challenges will follow Internet adoption patterns. While Internet threats are likely to continue along the trajectory outlined above, I believe new security challenges will emerge as attackers shadow Internet adoption patterns.

Mobile Internet use is growing quickly: it will become the predominant global Internet access method by 2014. Tens of thousands of applications available today support banking, ecommerce, highway navigation, health and wellbeing, and social networking, for example; the future will only bring more varied applications used in all facets of daily life. The current culture that encourages application downloading makes mobile devices especially vulnerable to malware. For example, in 2010, a smart phone weather application downloaded by mobile phone users demonstrated how a malicious attack could quickly co-opt a cohort of smart phones around the globe. Today, we lack the understanding and technology to enforce security policies in these situations.

Machine rooms and data centers have long been a mainstay of commercial information technology support. But new technology now enables the unprecedented aggregation of hardware and software, which is then provided in a comprehensive, highly-elastic service that we call "cloud computing." Cloud providers are adding infrastructure at a rapid rate to support this new model. These opportunities bring new risks. A new trust model is required. Users of cloud computing must place their trust in a third party that could well be sharing its resources with competitors and adversaries. Moreover, the cloud – because it concentrates value – is especially attractive to attackers. The ramifications of these changes require continued research and development; new approaches for protecting cloud infrastructure will be key to its long-term success. For more information on the strengths and weaknesses of cloud computing, see the NIST draft recommendations for information technology policy makers: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

The trend toward increasingly cyber-enabled systems, i.e., the integration of computation, communication, and control into physical systems, offers new challenges. Healthcare, education, and finance have been at risk of attack for a long time, and physical infrastructure – manufacturing, energy production, and transportation – are now at risk. Recent attacks demonstrate that even facilities not directly connected to the Internet can be targeted.

The Nation's researchers must start building systems whose trustworthiness derives from first principles, i.e., proven assumptions. To do that, NSF is formulating and developing a comprehensive research portfolio around a view of systems that are deemed *trustworthy*, i.e., systems that people can depend on day after day and year after year to operate correctly and safely – from our avionics, mass transit and automobile systems to medical devices operated remotely to save lives on battlefields. Included in this notion of trustworthiness are a number of critical concepts: *reliability* (does it work as intended?); *security* (how vulnerable is it to attack?); *privacy* (does it protect a person's information?); and *usability* (can a human easily use it?). Research needs to be game-changing and forward-looking; new policies and continued focus on cyber security education, public awareness and workforce development are critical to our success.

Given this summary of the emerging threats in cybersecurity and NSF's contributions to these challenges, let me now turn to the issues that were raised by the Subcommittees in the invitation to this hearing.

(1) Please provide a brief overview of the National Science Foundation's (NSF) cybersecurity activities and how research and development is integrated into your agency's mission.

The National Science Foundation funds a broad range of activities to advance cybersecurity research, develop a well-educated and capable workforce, and to keep all citizens informed and aware. Investments in these activities include the Trustworthy Computing program in the Directorate for Computer and Information Science and Engineering, the Scholarships for Service program in the Directorate for Education and Human Resources, the TRUST Science and Technology Center, and many related research projects across Engineering, Mathematical and Physical Sciences, and Office of Cyberinfrastructure programs. As stated in its organic act, NSF's mission is "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…" Support for basic and applied research is integral to NSF's mission. NSF also supports development activities beyond the stage of research prototypes through its Small Business Innovative Research (SBIR) and Small Business Technology Transfer (STTR) programs and in its support of science and engineering computing infrastructure through its Office of Cyberinfrastructure.

Cybersecurity Research

NSF has been investing in cyber security research for many years. In FY 2011, NSF will invest almost $117 million in fundamental research in the science of trustworthiness and related trustworthy systems and technologies. Approximately one half of this $117 million is allocated to the cross-cutting Trustworthy Computing program, which in FY 2011 is funded at a level of $55 million dollars. Currently, there are about 500 projects that are active. About a third of these projects includes more than one faculty researcher and all include graduate students. Active awards in the Trustworthy Computing program include $1.2M for support of 19 post-doctoral students as well. In addition to the Trustworthy Computing program, NSF continues to make cyber security investments in the core scientific sub-disciplines of the computing and information sciences, including the foundations of algorithms and information and communications, cyber physical systems, smart health and wellbeing, future internet architectures, networking technology and systems, information integration and informatics, and in the social and economic implications of developing secure, trustworthy systems.

NSF continues to cast a wide net and let the best ideas surface, rather than pursuing a prescriptive research agenda. It engages the cyber security research community in developing new fundamental ideas, which are then evaluated by the best researchers through the peer review process. This process, which supports the vast majority of unclassified cyber security research in the United States, has led to innovative and transformative results. Today, NSF's cyber security research portfolio includes projects addressing security from the microscopic level, detecting whether a silicon chip may contain a malicious circuit, to the macroscopic level, determining strategies for securing the next generation electrical power grid, as well as at the human level, studying online privacy and security behaviors of both adolescents and senior citizens. Fundamental research in cryptography, cryptographic protocol analysis, formal specification and verification techniques, static and dynamic program analysis, security testing methods, all contribute to improved methods for building systems that perform as intended, even in the face of threats. Research in secure programming languages and methodologies, in securing operating systems and especially the virtualization mechanisms and hypervisors on which much of the security of cloud computing architectures depends is also prominent in NSF's portfolio. NSF's researchers are investigating novel methods for detecting when security measures have failed, when intrusions have occurred, and when information may have been altered or stolen. NSF's portfolio includes projects studying security in human-centric systems and in a variety of web application contexts as well as in smart phones, medical devices, and automotive systems.

Aside from single investigator and team awards, NSF also invests in center-scale activities. In FY 2012, NSF will provide the eighth year of funding for the *Team for Research in Ubiquitous Secure Technology* (TRUST) Science and Technology Center (STC). This center, which includes University of California (UC), Berkeley, Carnegie Mellon University, Cornell University, San Jose State University, Stanford University, and Vanderbilt University and many industrial partners, is focused on the development of cybersecurity science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the Nation's critical infrastructure by addressing the technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.

Since 2004, the Trustworthy Computing program has funded four centers. All of these centers are coming to an end this year or next:

- *Trustworthy Cyber Infrastructure for the Power Grid* led by University of Illinois Urbana-Champaign, now transitioned to Department of Energy (DoE) and Department of Homeland Security (DHS) for continued funding

This research creates infrastructure technology that will convey critical information to grid system operators despite partially successful cyber attacks and accidental failures. Security and trust validation techniques are developed that can quantify the trustworthiness of a proposed design with respect to critical properties. An interactive simulator created by the project will allow users to experiment with new power grid cyber-infrastructure design approaches.

- *Cybertrust Center for Internet Epidemiology and Defenses* led by UC San Diego and UC Berkeley

Understanding the scope and emergent behavior of Internet-scale worms seen in the wild constitutes a new science termed *Internet epidemiology*. To gain visibility into pathogens propagating across the global Internet, the Center has developed and operated an Internet pathogen detection service of unprecedented scale. With this service, the Center has demonstrated the speed and coverage over which such pathogens can spread, and has developed mechanisms for deriving "signatures" of a worm's activity and disseminating these to worm suppression devices deployed throughout the global network.

- *Situational Awareness for Everyone* led by Carnegie Mellon University and University of North Carolina, Chapel Hill

This center focuses on how to make both users and organizations more aware of their cybersecurity situation – the risks they face and how they can deal with them in practice. For organizations, the center has developed tools and techniques focused on network security awareness and management. Some of these tools are now operating in California's inter-campus network as well as Berkeley's and Carnegie Mellon's internal campus networks; industry is also showing concrete interest. The center has also focused on educating children and adults, reaching children through a novel game that educates users about security issues and tailors its behavior for the age and background of the player. It has been tested in Pittsburgh regional school districts and is now available on the Internet.

- ACCURATE led by Johns Hopkins University

The voting system integrity problem is a paradigmatic hard cyber trust problem, requiring trustworthy system architectures, security, integrity, privacy, anonymity, high assurance, and human-machine interfaces. Voting systems must preserve a voter's privacy and anonymity, while also being auditable and transparent. This center has generated new understanding of voting systems and has participated in the California Secretary of State's "Top to Bottom Review" of voting systems.

NSF has also invested in two active industry/university cooperative research centers:

- CITeR: Center for Identification Technology Research (Biometrics) at West Virginia University and the University of Arizona

CITeR focuses on identification of people that includes iris, fingerprint and face recognition and will significantly enhance the research database available for the disciplines involved with security biometrics technologies. Research is needed in large-scale, fully-automated, distributed systems in several applications, ranging from drivers license to passports and visas, for example.

- S2ERC: Security and Software Engineering at Ball State and other universities

S2ERC investigates integrated methods of engineering practical software systems that are able to meet emerging security requirements. This goal is of great importance to both industry and government in order for them to confidently deploy real-world software systems that meet their mission goals in the face of a broad range of security attacks. Participants in S2ERC include Ball State University, DePaul University, Indiana University- Purdue University Fort Wayne, Indiana University – Purdue University Indianapolis, Iowa State University, James Madison University, Pennsylvania State University, Purdue University, University of Illinois at Chicago, University of West Florida, Virginia Polytechnic Institute and State University, and West Virginia University.

Cybersecurity Education

Investments in cybersecurity research are accompanied by investments in cyber-security education and workforce development. Research undertaken in academia not only engages some of our nation's best and brightest researchers, but because these researchers are also teachers, new generations of students are exposed to the latest thinking from the people who understand it best. And when these students graduate and move into the workplace, they will bring this knowledge and understanding with them. Moreover, faculty members in this dual role of researchers and teachers have incentives to write textbooks and prepare other teaching materials that allow dissemination of their work to a wide audience, including teachers and students nationwide.

Over the years, the Trustworthy Computing program has supplemented its awards by giving small amounts of additional funding to researchers who were willing to bring undergraduates into their labs through the Research Experiences for Undergraduates (REU) program. This program gives many undergraduate students their first hands-on experiences with real science and engineering research projects. In addition, the Trustworthy Computing program has funded up and coming young investigators through the CAREER program that offers NSF's most prestigious awards in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations.

	FY08	FY09	FY10	FY11
TC CAREER awards	15	19	15	17
TC REUs	29	58	23	41

The NSF Directorate for Education and Human Resources (EHR) has focused on increasing the number of professionals with degrees in cybersecurity. An overwhelming majority of these EHR developed

professionals were supported by the **Federal Cyber Service: Scholarship for Service (SFS)** and **Advanced Technological Education (ATE)** programs.

The SFS program seeks to increase the number of qualified students entering the field of cybersecurity and to increase the capacity of United States higher education enterprise to produce cybersecurity professionals. The SFS program is an interagency program administered by NSF in collaboration with the Office of Personnel Management (OPM), the Department of Homeland Security (DHS), and the National Security Agency (NSA), among other agencies. SFS was established as a result of a January 2000 Presidential Executive Order that defined the National Plan for Information Systems Protection. The SFS program supports two tracks.

The first track, the **SFS Scholarship Track,** provides funding to colleges and universities to award scholarships to students in the information assurance and computer security fields. A recipient must be a U.S. citizen, a full-time student within two years of graduation, demonstrate academic talent, meet selection criteria for Federal employment, be willing to undergo a background investigation for security clearance and must agree to work for at least two years in the Federal government. To date, the SFS program has provided scholarships to 1400 students with 1100 of them successfully placed in the Federal government. The SFS graduates were employed by more than 30 Federal agencies, including National Security Agency, Department of Homeland Security, Central Intelligence Agency, and Department of Justice.

From 2007 to 2010, twenty-eight awards were made totaling $46.75 million dollars. Currently, SFS Scholarships are offered at 34 institutions, with the largest enrollments at the University of Tulsa, Carnegie Mellon University, Mississippi State, and University of North Carolina.

Calendar Years	SFS Graduates
2002	9
2003	75
2004	152
2005	179
2006	172
2007	157
2008	121
2009	86
2010	116
Total	1067

Students enrolled FY2007-10	
University of Tulsa	107
Carnegie Mellon University	75
Mississippi State	48
University of North Carolina	46
Naval Postgraduate School	44
Idaho State University	42
Syracuse University	35
New Mexico Tech	31
Stoney Brook University	31
Polytechnic University of NY	30
AFIT	28
North Carolina A&T	28
George Washington University	27
Iowa State University	26
Georgia Tech	22
Johns Hopkins University	22

Agency Placement FY 2007-10	
National Security Agency	105
US Navy	51
Department Of Defense	28
Mitre Corporation	27
US Army	26
US Air Force	22
Central Intelligence Agency	19
Sandia Laboratory	19
Department Of Treasury	18
Department Of Commerce	17
Department Of Justice	17
Department Of Homeland Security	13
Federal Reserve System	13
Software Engineering Institute	12
Other	90
Total	477

The second track, the **SFS Capacity Building Track,** provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals. Examples of projects include: developing faculty expertise in information cybersecurity, creating learning materials and strategies, outreach activities, or other innovative and creative projects, which lead to an increase in the national cyber security workforce. Proposing organizations must demonstrate expertise in cybersecurity education or research. From 2007 to 2010, twenty-four awards were made totaling $5.73 million dollars and covering every region of the country.

With an emphasis on two-year colleges, **the Advanced Technological Education (ATE) program** focuses on the education of technicians for the high-technology fields, including cybersecurity. Activities may have either a national or a regional focus, but not a purely local one. The ATE program supports projects, centers, and targeted research in technician education. Currently, there are 14 active ATE awards in

cybersecurity for a total of $17.1M, including $3M awarded in FY10. Three of these projects have been funded under the Regional ATE Center track, providing $3M for four years for each of the centers.

- **CyberWatch** (Maryland) **-** The CyberWatch Center is headquartered at Prince George's Community College. The mission of the center is to "increase the quantity and quality of the cybersecurity workforce." It sponsors a K-12 program, college-level model programs and courses, lab resources, articulation agreements, and resources for faculty development. CyberWatch has 50 institutional members, including 35 community colleges and 15 universities from 20 states. More than 1800 students were enrolled in cybersecurity courses at partnering community colleges in 2009.

- **Center for Systems Security and Information Assurance (CSSIA)** (Illinois) **-** The CSSIA center has developed an associate's degree program in information technology security, and is providing professional development opportunities and curricular materials. CSSIA has 8 institutional members, including 6 community colleges and 2 universities from 5 states – Illinois, Indiana, Michigan, Minnesota, and Wisconsin. Their community college partner institutions enrolled more than 1400 students in cybersecurity courses in 2009.

- **Cyber Security Education Consortium (CSEC)** (Oklahoma) **-** The CSEC center is "dedicated to building a cybersecurity workforce who will play a critical role in implementing the national strategy to secure cyberspace." The center provides regional training workshops as well as internships in SCADA security and digital forensics. CSEC has 45 institutional members, including 42 community colleges and 3 universities from 8 states -- Arkansas, Colorado, Kansas, Louisiana, Missouri, Oklahoma, Tennessee, and Texas. Almost 2000 students enrolled in cybersecurity courses at partnering community colleges in 2009.

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

NSF supported the development of the Cyberspace Policy Review, providing the task force that prepared the review with direct access to an extensive group of academic cyber security researchers. The Cyberspace Policy Review Near-Term Action Plan lists ten items and the Mid-Term Action Plan lists fourteen. The actions most concerned with NSF's mission are discussed below.

Near-term Action Plan #9 calls for (a) *developing a framework for research and development strategies that focus on game-changing technologies that can enhance the trustworthiness of the digital infrastructure* and (b) *providing the research community with access to event data to facilitate developing tools, testing theories, and identifying workable solutions*.

(a) Specifically, over the past two years, NSF has participated in a set of activities designed to develop research themes related to game-changing technologies, including the announcement of three such themes last year: Moving Target, intended to raise the costs for attackers; Tailored Trustworthy Spaces, intended to support the creation of trustworthy computing environments that can respond to a range of trust requirements; and Cyber Economic Incentives, intended to help understand how to motivate adoption of trustworthy technologies. NSF has collaborated with its partner agencies in publicizing these themes to the research community and has incorporated them into related research solicitations. In the succeeding year, NSF has participated actively in a working group organized under the

Networking Information Technology R&D (NITRD) program's Cyber security and Information Insurance (CSIA) Interagency Working Group (IWG) to develop a strategic plan for the Federal cyber security research and development program. This plan is expected to be released officially before the end of May.

(b) NSF has also actively promoted research access to event data. Although NSF itself does not possess any datasets appropriate for this purpose, it convened a workshop on cyber security data for experimentation in August 2010 that brought companies and organizations that possess such data together with members of the research community who would like to study the data. Several companies have agreed to make data available on their premises, and NSF has invited its researchers to request supplementary funds to support visits to data repositories that are not available for remote access.

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.

As already described above, NSF supports a broad range of cyber security research; in FY2011 NSF will invest almost $117 million in this area; approximately half of this is in the Trustworthy Computing program. The balance of NSF's cyber security investments are made in the many core scientific sub-disciplines of the computing and information sciences. In addition to single and multiple-investigator research grants, NSF has funded a Science and Technology Center, four Center-Scale Activities, and Industry/University Cooperative Research Centers. Education is embedded in virtually all of these research grants through the training of graduate students, many of whom will join the industry or university workforce in cyber security research. NSF CAREER awards, among NSF's most prestigious grants, carry specific requirements for integration of research and education. Cyber security research funds also support the Research Experience for Undergraduates (REU) program to grow student interest in cyber security research. The Scholarships for Service (SFS) program ($52.5 million from 2007-2010) provides tuition scholarships for students enrolled in cyber security programs at a wide range of institutions across the nation in exchange for a commitment to a period of service in a government post following graduation. A component of the SFS program is also devoted to building additional teaching capacity through curriculum and faculty development. The Advanced Technological Education (ATE) program supports cyber security education in fourteen projects.

Mid-Term Action Plan #4: Develop a strategy to expand and train the workforce, including attracting and retaining cyber security expertise in the Federal government.

As described earlier, NSF's Scholarships for Service program, including capacity building grants to support expansion of the educational resources available to train students in cyber security, is a fundamental part of the national strategy to train and expand the workforce in this key area; scholarships under this program carry a commitment for service in the Federal government. Last fall, NSF sponsored a Summit on Education in Secure Software to help identify how to teach students to write programs that cannot easily be subverted. NSF is also participating in the National Initiative for Cyber security Education (NICE) as co-lead with the Department of Education for Formal Cyber security Education. This activity encompasses development of education programs for K-12, higher education, vocational and other discipline-related programs in order to help provide a pipeline of skilled workers for private sector and government.

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

NSF's Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs aim to support the transition of successful research projects into the marketplace. These programs have funded several projects related to cyber security in recent years. Of the current active projects, eight have direct linkage to cyber security; these have been awarded about $4.5M to date.

CISE also participates in the Grant Opportunities for Academic Liaison with Industry (GOALI) program, which aims to promote academic-industry partnerships on high risk, transformational research projects. CISE plans to supplement its regular Advisory Committee with a new panel of industry leaders to further promote the adoption of research results by industry.

CISE also encourages academic industry partnerships. For example, as mentioned above, the NSF Team for Research in Ubiquitous Security Technology (TRUST) Science and Technology Center works with a number of industry partners who 1) help define the Center's strategic intent and research and education priorities through the Center's External Advisory Board, and 2) interact directly with faculty and students on individual research projects. Industry partners include Broadcom, Cisco, eBay, Google, HP, IBM, Intel, Juniper, Microsoft, Oracle/Sun, Qualcom, Raytheon, Symantec, United Technologies, and Yahoo. CISE has similar active engagement with industry across its portfolio, including in four Trustworthy Computing Centers and two Industry & University Cooperative Research Centers.

The following areas –as stated in the Cyberspace Policy Review– are not directly addressable by NSF; however, the Trustworthy Computing Program has invested in foundational research that can facilitate progress.

Mid-Term Action Plan #8: Develop mechanisms for cyber security-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
Example research areas include methods for specifying and enforcing privacy policies, applying new cryptographic schemes to support access control, developing techniques for anonymizing sensitive data, and secure multiparty computation techniques.

Mid-Term Action Plan #9: Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
Example research areas include communication patterns during emergencies; efficient, robust mesh networks that can operate through disasters; and network architectures for first-responder communications.

Mid-Term Action Plan #13: Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy
Example research areas include biometrics, cryptographic means for securing identities, and access management based on identity and experience.

(3) Please discuss how cybersecurity research and development, education and workforce training, and standards development are coordinated with other relevant agencies;

NSF coordinates its cyber security research and planning activities with other Federal agencies, including the Departments of Defense (DoD) and Homeland Security (DHS) and the agencies of the Intelligence Community, through the following "mission-bridging" activities:

- NSF plays a leadership role in the interagency Networking and Information Technology Research and Development (NITRD) Program. The National Science and Technology Council's NITRD Sub-Committee, of which I am co-chair, has played a prominent role in the coordination of the Federal government's cyber security research investments.
- In January 2008, President Bush initiated the Comprehensive National Cybersecurity Initiative (CNCI). The current Administration supports and has continued efforts on this initiative. One of the goals of the CNCI is to develop "leap-ahead" technologies that would achieve orders-of-magnitude improvements in cybersecurity. Based on this directive, a NITRD Senior Steering Group (SSG) for Cybersecurity R&D was established to provide a responsive and robust conduit for cybersecurity R&D information across the policy, fiscal, and research levels of the Government. The SSG is composed of senior representatives of agencies with national cybersecurity leadership positions, including: DoD, ODNI, DHS, NSA, NSF, NIST, OSTP, and OMB. A principal responsibility of the SSG is to define, coordinate, and recommend strategic Federal R&D objectives in cybersecurity, and to communicate research needs and proposed budget priorities to policy makers and budget officials, including recommendations to OSTP, OMB, and the Joint Inter-Agency Cyber Task Force (JIACTF). One of CISE's Division Directors is the co-chair of this group.
- The NITRD CyberSecurity and Information Assurance Interagency Working Group (CSIA IWG) coordinates cyber security and information assurance research and development across the thirteen member agencies, including DoD, the Department of Energy (DOE) and the National Security Agency (NSA).
- To facilitate cross conversation between classified and unclassified programs in the Federal government, a coordinating group called Special Cyber Operations Research and Engineering (SCORE) was established, which includes members from the SSG. NSF research is reported in this forum. In the past year, SCORE has organized a series of workshops questioning some commonly held assumptions about technical approaches to cybersecurity; NSF investigators have been active participants.
- Under the auspices of the NITRD program and the CSIA SSG and IWG, NSF and the other member agencies have co-funded and co-sponsored a number of workshops:
    - Science of Security Workshop, co-funded by NSF, NSA, and IARPA (November 16-18, 2008): To discuss the foundations of making security into a science.
    - Usability, Security, Privacy Workshop, hosted by the National Academies' Computer Science and Telecommunications Board (July 21-22, 2009): To advance the study of usability and ways to embed usability considerations into the research, design and development of secure systems.
    - Workshop on Clean-Slate Security Architectures, co-funded by NSF and DARPA (July 28, 2009): To frame a new security architecture that could be the basis of clean-slate networks.
    - Workshop on Security Research for the Financial Infrastructure, co-supported by Treasury, DHS and NSF (October 28-29, 2009): To gain a better understanding of the

security problems faced by the financial sector and how the research community might help solve those problems.
    - Workshop on Cyber Security Data for Experimentation (August 26-27, 2010): To explore options for research access to event data.
    - Summit on Education in Secure Software (October 18-19, 2010): To develop a comprehensive agenda focused on the challenges of secure software education.
    - NSF Workshop on the Future of Trustworthy Computing (October 27-29, 2010): To provide context and direction for researchers interested in Trustworthy Computing.
    - NSF/Microsoft Research Workshop on Usable Verification (November 15-16, 2010): To stimulate advances in the usability of tools for formal verification.
    - Workshop on Fundamental Research Challenges for Trustworthy Biometrics (November 8-9, 2010): To identify underlying biometrics research challenges.
- A number of projects have received their seed or beginning funding at NSF and then have been picked up by other agencies as they see the value of applying basic research to their mission challenges. NSF has also encouraged its researchers to take advantage of research assets created by its partner agencies. For example,
    - NSF funded the Trustworthy Cyber Infrastructure for the Power Grid Center at UIUC; it has now transitioned to DoE/DHS for continued funding.
    - NSF funded the DETER testbed in its early years; it is now wholly funded by DHS.
    - NSF encourages its Principal Investigator (PI) community to use the data available from the DHS-funded PREDICT repository to validate and test their ideas.

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

The Cyber Security Research and Development Act of 2002 has been an important asset in stimulating innovative research and development. NSF's activities are well-aligned with the provisions of the existing Act and its proposed enhancement. NSF has been working with the National Coordinating Office (NCO) on a national strategy for research and development, which is one of the key points in the new draft legislation. The addition of usability and social and behavioral factors as areas of research interest is consistent with the path that NSF is currently pursuing, as is the focus on fostering curriculum development on principles and techniques of designing secure software. Calling out investments in center-scale activities is also consistent with the importance that NSF places on funding centers to create visibility and activity around important national challenges. As mentioned above, NSF actively encourages interaction across government, academic, and commercial sectors. CISE plans to supplement its regular Advisory Committee with a new panel of industry leaders to further promote the adoption of research results by industry. In summary, NSF's investments in cybersecurity research, education and workforce development are consistent with the provisions of H.R. 4061.

(5) How would the Administration's proposed cybersecurity legislation impact NSF's cyber security activities?

The National Science Foundation is the Nation's premier agency for advancing fundamental research and education in science and engineering. NSF's mission is to "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…"

The Administration's proposal is offering a carefully tailored and measured approach that relies on private sector innovation. This proposal will enable cyber infrastructure owners and operators to adopt new strategies and techniques to deal with cyber threats. NSF's R&D investments enable scientific discovery and engineering advances that continuously fuel that innovation.

Conclusions

In my testimony today, I've tried to show that the pace and scope of today's cyber threats pose grand challenges to our national critical infrastructure. I have outlined the investments in NSF's cyber security research and education portfolio, which show progress and significant advances over the years. Nonetheless, the Nation needs to invest in long-term, fundamental and game-changing research if our cybersystems are to remain secure in the future. I have indicated NSF's role in addressing the Near- and Mid-Term Action Plans included in the Cyberspace Policy Review and have detailed our progress in meeting those objectives. I have also discussed how NSF partners with other agencies and have given examples of many cross-agency activities. Finally, I have provided feedback on H.R. 4061, The Cybersecruity Enhancement Act of 2009, as well as on the Administration's proposed cybersecurity legislation. I appreciate the opportunity to have this dialogue with members of your Subcommittees on these very important topics. With robust sustained support for cyber security research and development in both the executive and legislative branches, there is a unique opportunity to protect our national security and enhance our economic prosperity for decades to come. This concludes my remarks. I would be happy to answer any questions at this time.

Biographical Sketch

FARNAM JAHANIAN

Farnam Jahanian is the Assistant Director of the Computer and Information Science and Engineering (CISE) Directorate at the National Science Foundation. Prior to joining NSF, he held the Edward S. Davidson Collegiate Professorship in Electrical Engineering and Computer Science at the University of Michigan, where he served as Chair for Computer Science and Engineering from 2007 – 2011 and as Director of Software Systems Laboratory from 1997 – 2000. Dr. Jahanian also serves as co-chair of the Networking and Information Technology Research and Development (NITRD) Subcommittee of the NSTC Committee on Technology, providing overall coordination for activities of 14 government agencies.

At CISE, Dr. Jahanian guides the directorate in its mission to uphold the nation's leadership in computer and information science and engineering through its support for fundamental and transformative advances that are a key driver of economic competitiveness and crucial to achieving our major national priorities. With a budget of approximately $618 million, CISE supports ambitious long-term research and innovation, the creation of cutting-edge facilities and tools, broad interdisciplinary collaborations, and education and training of the next generation of computer scientists and information technology professionals with skills essential to success in the increasingly competitive, global market.

Over the last two decades at the University of Michigan, Dr. Jahanian led several large-scale research projects that studied the growth and scalability of the Internet infrastructure and which ultimately transformed how cyber threats are addressed by Internet Service Providers. His work on Internet routing stability and convergence has been highly influential within both the network research and the Internet operational communities. This work was recently recognized with an ACM SIGCOMM Test of Time Award in 2008. His research on Internet infrastructure security formed the basis for the successful Internet security services company Arbor Networks, which he co-founded in 2001. He served as Chairman of Arbor Networks until its acquisition by Tektronix Communications, a division of Danaher Corporation, in 2010.

The author of over 100 published research papers, Dr. Jahanian has served on dozens of national advisory boards and government panels. He has received numerous awards for his research, teaching, and technology commercialization activities. He has been an active advocate for economic development efforts over the last decade, working with entrepreneurs, and frequently lecturing on how basic research can be uniquely central to an innovation ecosystem that drives economic growth and global competitiveness. In 2009, he was named Distinguished University Innovator at the University of Michigan.

Dr. Jahanian holds a master's degree and a Ph.D. in Computer Science from the University of Texas at Austin. He is a Fellow of the *American Association for the Advancement of Science (AAAS), the Association for Computing Machinery (ACM), and the Institute of Electrical and Electronic Engineers (IEEE).*