Testimony of

Jeremy Epstein
Lead Program Director
Secure and Trustworthy Cyberspace (SaTC)

Before the

Committee on Commerce, Science, and Transportation
U.S. Senate

September 3, 2015

"Confronting the Challenge of Cybersecurity"

Good afternoon, Chairman Thune, and members of the Committee. My name is Jeremy Epstein and I am the National Science Foundation (NSF) Lead Program Director for the Secure and Trustworthy Cyberspace (SaTC) program within the Computer and Information Science and Engineering (CISE) Directorate.

NSF's mission is "to promote the progress of science; to advance the national health, prosperity, and welfare; [and] to secure the national defense…". NSF's goals – discovery, learning, research infrastructure and stewardship – provide an integrated strategy to advance the frontiers of knowledge, cultivate a world-class, broadly inclusive science and engineering workforce, build the nation's research capability through investments in advanced instrumentation and facilities, and support excellence in science and engineering research and education. I welcome this opportunity to highlight NSF's investments in cybersecurity research and education.

The Cybersecurity Challenge

While the advances in cybersecurity research and development (R&D) are many, the Nation must continue its investments in game-changing research if our cyber systems are to be trustworthy now and in the future. As you know, every day, we learn about more sophisticated and dangerous attacks. Why is the cybersecurity challenge so hard? In general, it's hard because attacks and defenses evolve together: a system that was secure yesterday might no longer be secure tomorrow.

NSF is uniquely positioned to address both today's cyber challenges as well as the threats of the future, because NSF invests in discoveries, as well as the discoverers who enable fundamental scientific advances and technologies.

Cyber Security Research Programs

NSF 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. A major NSF activity is the SaTC program, led by CISE in partnership with the Directorates for Education and Human Resources (EHR), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral, and Economic Sciences (SBE), and funded at $126 million in FY 2015. Currently, there are over 670 active Secure and Trustworthy Cyberspace awards.

NSF's SaTC program builds on predecessor programs begun in 2002 and seeks to secure the Nation's cyberspace by addressing four perspectives within the multi-dimensional cybersecurity problem space:

- *Trustworthy computing systems*, with goals to provide the basis for designing, building, and operating a cyberinfrastructure with improved resistance and improved resilience to attack that can be tailored to meet a wide range of technical and policy requirements, including both privacy and accountability.
- *Social, behavioral and economic sciences*, with goals to understand, predict, and explain prevention, attack and/or defense behaviors and contribute to developing strategies for remediation.
- *Cybersecurity education,* with goals to promote innovation, development, and assessment of new learning opportunities and to help prepare and sustain an unrivaled cybersecurity workforce capable of developing secure cyberinfrastructure components and systems, as well as to raise the awareness of cybersecurity challenges to a more general population.
- *Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS)*, with goals to develop strategies, techniques, and tools that avoid and mitigate hardware vulnerabilities and lead to semiconductors and systems that are resistant and resilient to attack or tampering. STARSS is a joint effort of NSF and the Semiconductor Research Corporation (SRC), a consortium of leading technology companies.

The SaTC program further aims to address the challenge of moving from research to capability. The program supports research activities whose outcomes are capable of being implemented, applied, experimentally used, or deployed in an operational environment. Areas of emphasis for these "transition to practice" investments have included malware detection and prevention, situational understanding, data assurance, risk analysis, and software assurance.

For example, NSF-funded researchers have demonstrated the ability to remotely take over automotive control systems[1]. The researchers found that, because many of today's cars contain cellular connections and Bluetooth wireless technology, it is possible for a hacker working from a remote location to take control of various features – like the car locks and brakes – as well as to track the vehicle's location, eavesdrop on its passenger cabin, and steal vehicle data. The researchers are now working with the automotive industry to develop new methods for assuring the safety and security of on-board electronics. Both the Society for Automotive Engineers and the United States Council for Automotive Research have partnered with the researchers to initiate efforts focused on automotive security research[2]. Automotive manufacturers have also started dedicating significant resources to security[3].

[1] http://www.nytimes.com/2011/03/10/business/10hack.html
[2] http://www.autosec.org/faq.html
[3] http://www.caranddriver.com/features/can-your-car-be-hacked-feature

NSF-funded researchers supported by the SaTC program use testbeds such as the Cyber Defense Technology Experimental Research (DETER) Network, originally developed with NSF funding and now supported by the Department of Homeland Security (DHS) and the Remotely Accessible Virtualized Environment (RAVE) Lab, which was also developed with NSF funding and is specifically focused on cybersecurity education. As directed by *The Cybersecurity Enhancement Act of 2014*, NSF is working to identify what other testbeds are needed for cybersecurity research in the future. NSF appreciates the Committee's awareness of the national need for robust cybersecurity testbeds.

Cybersecurity Education and Training Programs

The NSF Directorate for Education and Human Resources seeks to develop a well-prepared cybersecurity workforce of the future in large part through the CyberCorps®: Scholarship for Service (SFS) program.

SFS was created as a result of a May 1998 Presidential Decision Directive, which described a strategy for cooperative efforts by the government and the private sector to protect physical and cyber-based systems. In January 2000, a Presidential Executive Order defined the National Plan for Information Systems Protection, which included the Federal Cyber Services (FCS) training and education initiative and the creation of a SFS program. *The Cybersecurity Enhancement Act of 2014* directs NSF, in coordination with the U.S. Office of Personnel Management (OPM) and DHS, to continue the SFS program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments. We recognize the Chairman and the Committee's work on this legislation and appreciate the strong support for the SFS program.

The SFS program funds institutions of higher education to support undergraduate and graduate students in academic programs in cybersecurity. The students must be U.S. citizens or lawful permanent residents of the U.S., and must be able to meet the eligibility and selection criteria for government employment. Students can be supported on scholarships for up to three years, and in return, they agree to take government cybersecurity positions for the same duration as their scholarships. The government agencies eligible for job placement include federal, state, local, or tribal governments. To assist both the agencies and the students in good matches, NSF partners with OPM to run an annual job fair. In addition to OPM, NSF also partners with DHS and the National Security Agency (NSA) on the SFS program.

A second emphasis of the SFS program is expansion of the U.S. higher education enterprise to produce cybersecurity professionals through a variety of efforts. These include research on the teaching and learning of cybersecurity, development of curricula, integrating cybersecurity topics into relevant degree programs, developing virtual laboratories, strengthening partnerships between government and relevant employment sectors to better integrate applied research experiences into cybersecurity degree programs, and integrating data science into cybersecurity curricula.

From FY 2011 through FY 2014, the SFS program made 117 awards throughout the U.S., totaling over $145 million. As of early August 2015, the SFS program has provided scholarships to more than 2,400 students and graduated more than 1,700, including 22 percent with bachelor's degrees, 76 percent with master's degrees, and two percent with doctoral degrees. Of these graduates, 93 percent have been successfully placed in the Federal government. SFS scholarship recipients have been placed in internships and full-time positions in more than 140 federal departments, agencies, and branches, including the NSA, DHS, Central Intelligence Agency, and Department of Justice, along with state, local, and tribal governments.

The SFS program has recently embarked on a new activity, Inspiring the Next Generation of Cyber Stars (or GenCyber) summer camps, to seed the interest of young people in this exciting and exploding new field, to help them learn about cybersecurity, and to learn how skills in this area could pay off for them in the future. These overnight and day camps are available to students and teachers at the K-12 level at no expense to them; funding is provided by NSF and NSA. A pilot project for cybersecurity summer camps in 2014 stimulated such great interest that the GenCyber program expanded in 2015, supporting 43 camps held on 29 university campuses in 19 states with more than 1,400 participants.

I would like to highlight the fact that Dakota State University (DSU) has successfully competed for an NSF award to develop greater capacity for cybersecurity education, and for two scholarship grants to support cybersecurity students. Of the students who were awarded scholarships in the cybersecurity program at DSU, about half have graduated and all have been placed in government cybersecurity jobs; half are still in school; and a new cohort of scholarship holders is anticipated in the fall of 2015. In addition, DSU ran two GenCyber camps in 2015, one for high school students entering grades 10-12, and one for girls entering grades 8-12. You have heard additional detail about NSF-funded cybersecurity activities at DSU from other witnesses here today.

Strategic Planning Across the Federal Government

Finally, NSF closely coordinates its activities with other federal agencies and collaborates with them in pursuing cybersecurity research and education activities. In 2011, the National Science and Technology Council (NSTC), with the cooperation of NSF, developed a strategic plan titled *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*[4]. This plan has guided coordination across the federal government. As you know, the 2014 Cybersecurity Enhancement Act called for an updated R&D strategic plan. NSF is playing a key role in developing the revision of the strategic plan. Recognizing the changes in the threats to the national economy and security posed by cyber attacks, the revised strategy will expand on the 2011 report, with increased focus on areas including privacy, security of the Internet of Things and Cyber-Physical Systems, and an increased breadth of the understanding of human-centric aspects (social, behavioral, cultural, and psychological) of cybersecurity. Without deep awareness of the latter dimensions, a purely technological solution to cybersecurity is likely to fail.

Coordination Across the Federal Government

NSF coordinates its cybersecurity research and planning activities with other federal agencies, including the Department of Defense (DoD) and DHS, and the agencies of the intelligence community, through various "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 Subcommittee, of which NSF is co-chair, has played a prominent role in coordinating the federal government's cybersecurity research investments.
- A NITRD Senior Steering Group (SSG) for Cyber Security and Information Assurance R&D (CSIA R&D)[5] 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: NSF, DoD,

[4] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[5] https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_Information_Assurance_Research_and_Development_Senior_Steering_Group_%28CSIA_R%26D_SSG%29

the Office of the Director of National Intelligence (ODNI), DHS, NSA, the National Institute of Standards and Technology (NIST), the Office of Science and Technology Policy, and the Office of Management and Budget. 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.

- To facilitate conversation among classified and unclassified programs in the federal government, a coordinating group called Special Cyber Operations Research and Engineering (SCORE) was established. SCORE includes members from the CSIA R&D Senior Steering Group. NSF research, which is non-classified, is reported in this forum.
- On the education front, NSF is an active participant and contributor in the NIST-led National Initiative for Cybersecurity Education (NICE). NSF's involvement aims to bolster formal cybersecurity education programs encompassing K-12, higher education, and vocational programs, with a focus on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for the private sector and government.

Conclusions

Our Nation must continue to invest in long-term, fundamental, and game-changing research if our cyber systems are to remain trustworthy in the future. NSF's interdisciplinary research and education portfolios are contributing to a next-generation workforce that is increasingly cyber-aware, armed with the knowledge that it needs to protect against cyber attacks. With robust, sustained support for cybersecurity research and education in both the executive and legislative branches, as well as partnerships such as those on display here at Dakota State University, NSF contributes to the protection of our national security and the enhancement of our economic prosperity. This concludes my remarks. I would be happy to answer any questions at this time.

Biographical Sketch

Mr. Jeremy Epstein is the Lead Program Director for the National Science Foundation's (NSF) Secure and Trustworthy Cyberspace (SaTC) program, the federal government's flagship fundamental cybersecurity research program. In addition to SaTC, he leads the Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII) and co-leads the NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy (CPS-Security) within NSF's CISE Directorate. Jeremy's research areas include software security and voting systems security. He is associate editor-in-chief of the IEEE Security & Privacy Magazine; founder of the Applied Computer Security Associates (ACSA) Scholarships for Women Studying Information Security (SWSIS); the IEEE representative to the NIST Technical Guidelines Development Committee which writes voting systems standards; and a senior member of IEEE and ACM. He holds an M.S. in computer sciences from Purdue University and a B.S. from the New Mexico Institute of Mining and Technology.