Testimony of

James F. Kurose, Ph.D.
Assistant Director
Computer and Information Science and Engineering Directorate

Before the
Subcommittee on Research and Technology

For the
Committee on Science, Space, and Technology
U.S. House of Representatives

January 27, 2015

The Expanding Cyber Threat

Good afternoon, Chairwoman, Ranking Member, and members of the Subcommittee. My name is Jim Kurose and I am the National Science Foundation (NSF) Assistant Director for the Computer and Information Science and Engineering Directorate.

As you know, NSF is dedicated to supporting fundamental research in all disciplines, advancing the progress of science and engineering, and educating the next generation of innovative leaders. I welcome this opportunity to highlight NSF's investments in cyber security research and education, including our efforts to work collaboratively with other government agencies and the private sector.

Investments in unclassified, fundamental, long-term research are critical to an effective national strategy for achieving a secure and trustworthy cyberspace. In 2011, NSF contributed to a National Science and Technology Council (NSTC) Strategic Plan titled *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*[1]. This plan identifies a broad, coordinated interagency research agenda that focuses on research that "changes the game," minimizes the misuses of cyber technology, bolsters education and training in cyber security, establishes a science of cyber security, and transitions promising research into practice. A major goal is to make cyberspace worthy of the public's trust.

[1] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

NSF's investments in cyber security are strongly aligned with this Strategic Plan. 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 promote connections between academia and industry; collectively, these activities will help to protect cyberspace, secure the Nation's critical infrastructure, and fuel job growth in the decades ahead.

Just as many powerful information technologies (IT) deployed today capitalize on fundamental research outcomes generated decades ago with NSF funding, NSF is bringing the problem-solving capabilities of the Nation's best and brightest minds to bear on the cyber security challenges of today and tomorrow. Let me share with you some examples of the important contributions made in recent years by the cyber security research community with both NSF and other federal support:

- Formal methods and software analyses that further the science of security and privacy via principled techniques for the specification, design and analysis of security mechanisms to secure software programs, and for formalizing and enforcing privacy and accountability in web- and cloud-based systems;
- Protections against vulnerabilities in hardware and product supply chains with new approaches for Trojan detection; protections against counterfeiting of integrated circuits and new tamper-resistant security primitives for hardware;
- Cryptographic schemes and cryptographic-based authentication that enable us to perform computations on encrypted data on untrusted platforms (e.g., on distributed "cloud" platforms);
- Breakthroughs in cryptographic program obfuscation that make it possible to mask the inner workings of a computer program, so that people can use the program without being able to figure out how it works;
- Clean-slate approaches and verifiable operating system kernels that protect traditional desktop and server operating systems and browsers, mobile devices, cloud-based systems, and applications;
- Secure network architectures designed to prevent and mitigate distributed denial-of-service attacks on the Internet, and jamming attacks in wireless communications;
- Identification and protection against security threats to Cyber-Physical Systems (CPS), which include critical infrastructure, via approaches for securing intelligent transportation systems, and anomaly detection in smart grids;
- Innovative machine learning and data mining approaches used in the development of defenses against spam suitable for social networks, and methods for detecting attacks, such as those involving credit card fraud;
- Differential privacy techniques that aim to provide actionable global, statistical information about sensitive data, while preserving the privacy of the users whose information is contained in the data set; and
- Usable security and privacy measures that explore ways to improve warning messages, privacy settings, security interfaces and primitives based on the how end users intuitively respond to such stimuli.

These research innovations and outcomes 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 critical infrastructure. Moreover, as I will describe later in my testimony, NSF is pioneering multi-disciplinary, collaborative research programs in cyber security across its directorates and with industry. For example, with the Semiconductor Research Corporation (SRC), NSF currently supports research into the design of secure and resilient semiconductors. With Intel Corporation, NSF invests in the security and privacy of cyber-physical systems, such as transportation systems and medical devices. In recent years, research

outcomes have led to the formation of numerous start-up companies in the IT sector and the take-up of new products and services that collectively bring innovative solutions to the marketplace and help to protect cyberspace.

The Cyber Security Challenge

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 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 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 critical infrastructure systems is frequently updated to improve functionality, availability, and/or performance. New systems introduce new vulnerabilities (unknowable in the lab) that need new defenses when put into practice.
- The environments in which our computing systems are rapidly developed and deployed, and the functionality that they provide are also not static. With entirely new computing models/platforms, like cloud and mobile computing, come new content and function, which in turn create new opportunities and incentives for attack and disruption.
- As the automation of complex system interdependencies comes to pervade our critical infrastructure, new kinds of cascading vulnerabilities can be accidentally created and subsequently discovered in these systems, including the electric power grid, automated transportation networks, and robotic medical systems.
- The sophistication of attackers is increasing as well as their sheer number and the specificity of their targets.
- As information and systems are increasingly connected, and are increasingly composed of software and hardware produced by global supply chains, the opportunities for malicious insiders to cause damage increases, and the risks of information leaks multiply.
- As more systems and data become accessible, information that was once low risk becomes high risk through correlation that was unimaginable only a few years ago.
- 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 positive behaviors are required. Security mechanisms that are not convenient will be circumvented; security mechanisms that are difficult to understand will be ignored or misinterpreted. Indeed, cyber security is a multi-dimensional challenge, requiring expertise in computer science, mathematics, economics, behavioral sciences, and education.

Emerging Threats

With the rapid pace of technological advancement, daily life is now intimately connected to the Internet. Key aspects of business operations, our financial systems, manufacturing supply chains, and military communications are tightly networked, integrating the economic, political, and social fabric of our global society. As I discussed previously, these interdependencies can lead to vulnerabilities and a wide range of threats that challenge the security, reliability, availability, and overall trustworthiness of all systems and resources rooted in information technology. Coupled with Internet adoption patterns,

we are witnessing a dramatic shift in the size, complexity, and diversity of cyber security attacks. Let me expand upon four key technology and adoption trends:

- The proliferation of mobile devices and wireless networks exposes new vulnerabilities;
- The protection of "cloud" infrastructure has become key to long-term adoption;
- Increasingly, cyber-enabled systems expand the scope of attacks to physical infrastructure, including critical infrastructure in domains such as manufacturing, energy production and consumption, healthcare, and transportation; and
- Social media platforms open new avenues for hackers.

The number of mobile devices has soared in the last several years; there are already more mobile devices connected to the Internet than tethered devices. By the year 2018, analysts expect the number of mobile-connected devices to be 10 billion, or nearly one and one-half times the world's population[2]. Mobile devices are increasingly characterized by their pervasiveness and connectedness: they have eclipsed traditional computers as points of entry to the Internet in an era of "always-on, always-connected" communications. Smartphones and tablets are able to access data in a wide variety of forms, from text messaging to web browsing to live applications ("apps") for streaming services, gaming, and beyond. Moreover, apps are taking advantage of a user's presence in time and space, and combined with other relevant data, are delivering targeted and tailored content and services. The result is a future that is increasingly smart and connected. Hundreds of thousands of applications available today support banking, e-commerce, 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, a recent study found that mobile device malware rates – reflecting the number of devices attacked but not infected – surged 75 percent from 2013 to 2014 alone, often through downloadable software masquerading as something else[3]. The natural desire to accomplish a task, whether business or pleasure, leads to clicking "yes" in response to online requests, which in turn enables further compromise of our systems. NSF-funded research is exploring solutions, including better understanding of the mobile app ecosystem, crowd-based advice for whether a mobile app has security or privacy risks, personality-driven user interfaces, and understanding how the brain intuitively senses messages.

Additionally, with cloud computing and the proliferation of mobile devices, an organization's information is no longer stored and accessed within its walls or perimeters. Information is frequently entirely created and stored in the "cloud." Systems and resources, including networks, hosts, storage, data centers and applications, are increasingly virtualized and distributed, and commonly under the control of the cloud service providers and the end-users themselves. Confidential information and intellectual property are increasingly flowing from back-end systems that the organization doesn't own or fully control, through networks that it doesn't own or control, to endpoints and end-users that it doesn't fully control. This evolution toward the cloud requires continued research and development; new approaches for protecting cloud infrastructure will be key to its long-term success. Side-channel attacks on cloud infrastructure, allowing an observer in the cloud to observe side effects of what other cloud users are doing, allow inferences that were not possible in pre-cloud environments. The National

[2] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html
[3] http://www.cnbc.com/id/102338872#.

Institute of Standards and Technology's definition of, and recommendations for, cloud computing[4] provide additional information. NSF investments in cloud computing security have been summarized in annual reports[5].

Computers are embedded everywhere, from the cash register in the coffee shop to sensors in highways, actuators in medical devices, and controls in manufacturing plants. As these systems are increasingly connected to the Internet, the threat landscape continues to evolve. The Target breach of 2013-2014 showed the risks of interconnected systems, with the initial compromise through an HVAC contractor[6]. Remote access to cash registers has been used to steal credit card numbers, as may have been the case in breaches affecting Home Depot[7] and over 1,000 other U.S. merchants[8]. As I will describe later in my testimony, NSF-funded researchers have demonstrated the ability to gain wireless access to a combination heart defibrillator and pacemaker, and are now working with colleagues in industry on security engineering of medical devices and implants.

Risks include privacy as well as security. Tire pressure sensors installed to help drivers avoid dangerous tire under- or over-inflation can be remotely identified, thus allowing a stalker to inconspicuously track movements of potential victims or allowing criminals to track undercover law enforcement officers around a city. Beyond computer virus infections that have disabled operating room computers, hospitals have been victim to breaches of patient records. Recent studies show that a large fraction of hospital equipment is vulnerable to computer attacks[9].

Deliberate and seemingly reasonable security measures can also backfire. GoGo Inflight, which provides WiFi access on airplanes, replaces digital certificates used to prove the identity of websites with its own certificates[10], allowing it to decrypt network traffic and prevent video streaming that would interfere with throughput for other passengers. As a side effect, however, sensitive email traffic could be decrypted before it leaves the airplane, and then re-encrypted, introducing risks for executives who are the most likely to use airplane wireless services. Attackers could employ the same strategy by placing open "hotspots" at coffee shops. While such a cyber threat is easily detectable and circumvented, it requires technical understanding by users who are used to clicking "yes" to messages.

In light of these challenges, the Nation's cyber security research community is key to enabling the design, implementation, and deployment of systems that are secure and trustworthy. NSF continues to formulate and develop 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.

Four principles guide NSF's investments in cyber security research:

---

[4] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[5] http://www.nsf.gov/pubs/2012/nsf12040/nsf12040.pdf
[6] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[7] http://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach/?_r=0
[8] http://www.hngn.com/articles/40068/20140823/cash-register-hack-affected-over-1-000-u-s-businesses.htm
[9] http://www.wired.com/2014/04/hospital-equipment-vulnerable/
[10] http://arstechnica.com/security/2015/01/gogo-issues-fake-https-certificate-to-users-visiting-youtube/

- Uncover and address the underlying cyber security research gaps by focusing on the root causes of cyber security challenges rather than just treating the symptoms;
- Develop a "science of security" based on enduring cyber security principles that will allow us to stay secure despite challenges in technology and the evolution of new threat environments;
- Approach cyber security as a multi-dimensional challenge, involving both the strengths of security technologies and the variability of human behavior; and
- Enable the "right science and engineering at the right scale" by casting a wide net that encourages more speculative research, and multiple perspectives including accelerating the transitioning of research results into practice.

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

(1) Provide an overview of the research the National Science Foundation (NSF) supports related to cyberinfrastructure, risk management, threat detection, identity management, and other issues related to cyber security.

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.

Cyber Security R&D Portfolio

NSF has been investing in cyber security research for many years. In FY 2014, NSF invested $158.28 million in unclassified, fundamental, long-term research in the science of trustworthiness and related trustworthy systems and technologies. Today, NSF's cyber security research portfolio includes projects addressing security from the microscopic level, detecting whether a silicon chip is a counterfeit or may contain a malicious circuit, to the macroscopic level, determining strategies for securing the next-generation electrical power grid and transportation network, as well as at the human level, studying online privacy and security behaviors of both adolescents and senior citizens, methods for leveraging personality differences to improve security behaviors, and understanding motivations for keeping systems patched. Fundamental research in cryptography, cryptographic protocol analysis, formal specification and verification techniques, static and dynamic program analysis, and security testing methods contribute to improved methods for building socio-technical systems that perform as intended, even in the face of threats. Research in calculating on encrypted data will allow for secure cloud computation; methods for executing encrypted software will provably prevent adversaries from reverse engineering software to find vulnerabilities that can be exploited. Research in secure programming languages and methodologies, and 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 smartphones, voting systems, medical devices, automotive systems, and other cyber-physical systems. New methods explore how to effectively communicate security and privacy information to users in ways that they can better understand, and offer approaches for blind users to receive useful but unobtrusive security information, since "pop up"

warnings are ineffective. Collaborations between computer scientists and social scientists continue to expand the scope of how we understand security problems and their solutions.

Across NSF's portfolio of cyber security research, about a third of the investments are in projects that involve one to two faculty researchers and one to two graduate students, and another are in projects that involve small teams of researchers, including graduate students. Here are some specific examples of the kinds of foundational research projects that small teams of researchers are pursuing, and their intended broader significance:

- Integrated circuits used in all forms of electronics are subject to counterfeits, which may violate intellectual property laws, be less reliable, or even dangerous. This research develops mechanisms that can tell if a chip is new or used, and discern genuine from counterfeit chips in a method similar to a car's Vehicle Identification Number (VIN) and odometer.
- Internet traffic can be redirected through alternate locations, akin to redirecting vehicles through a neighborhood by posting "Detour" signs. This technique has been used for potentially nefarious purposes, including a 2013 attack that sent U.S. Internet traffic through a foreign country. Ongoing research is developing new methods to improve the ability to detect such redirections and characterize their extent, frequency, and impact, and share summary reports with network operators, emergency response teams, law enforcement, and policy makers.
- Voting systems must meet a wide range of requirements, including cost, accuracy, resilience against attack, auditability, and usability by all citizens who are infrequent voters. An NSF award in collaboration with the government of Travis County, TX, seeks to create voting systems that can address all of these needs simultaneously, building on the past decade of research on risks to voting technology.
- Biometric approaches, such as fingerprinting and iris recognition, hold tremendous promise to prove identity to computer systems, but still have significant limitations, including susceptibility to "spoofing." An NSF-funded research team is seeking to advance our knowledge of security and accuracy of "multi-biometric" systems by inventing, evaluating, and applying innovative methods and tools to combine highly accurate static traits, such as iris patterns, with novel traits based on the dynamics of eye movements that cannot be spoofed. These techniques do not require new hardware, and can be used for other purposes beyond identification such as discerning fatigue or concussion.
- When a photograph is shared online through social media, the person sharing the photo (usually the photographer) makes decisions about who can see it, rather than the people whose images are in the photo. Ongoing research aims to address technical methods for allowing people to control how privacy protections can protect their images.

Beyond single-investigator and team awards, NSF also invests in center-scale activities. Since 2012, the Secure and Trustworthy Computing program has funded seven center-scale projects called "frontiers," representing far-reaching explorations motivated by deep scientific questions and grand challenge problems in security, privacy, encryption, cloud computing, and healthcare systems, to name a few:

- *Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives* at the University of California at San Diego, University of California at Berkeley, and George Mason University (2012) – This research tackles the technical and economic elements of Internet security: how the motivations and interactions of attackers, defenders and users shape the threats we face, how they evolve over time and how they can best be addressed. This research has the potential to

dramatically benefit society by undermining entire cybercrime ecosystems by, for example, disrupting underground activities, infrastructure and social networks.

- *Privacy Tools for Sharing Research Data* at Harvard University (2012) – A multi-disciplinary team of researchers is developing tools and policies to aid in the collection, analysis and sharing of data in cyberspace, while protecting individual privacy. The ideas and tools developed in this project will have a significant broad impact on society since the issues addressed in the work arise in many other important domains, including public health and electronic commerce.
- *Enabling Trustworthy Cybersystems for Health and Wellness* at Dartmouth University, the University of Illinois at Urbana-Champaign, Johns Hopkins University, and University of Michigan at Ann Arbor (2013) – This interdisciplinary center investigates ways to provide trustworthy information systems for health and wellness in the context of sensitive information and health-related tasks being increasingly pushed into mobile devices and cloud-based services. In the long term, this project will help create mobile health systems that can be trusted by individual citizens to protect their privacy and by health professionals to ensure data integrity and security.
- *Rethinking Security in the Era of Cloud Computing* at the University of North Carolina at Chapel Hill, Stony Brook University, Duke University, North Carolina State University, and University of Wisconsin at Madison (2013) – This project explores ways of improving security of data and services in the cloud by addressing key challenges like secure transport, authorization, user and software authentication and security monitoring. This project challenges the common perception that the cloud decreases security for its customers, and instead envisions new opportunities for improving the security of data and services by moving them to the cloud.
- *Towards Effective Web Privacy Notice and Choice: A Multi-disciplinary Perspective* at Carnegie Mellon University, Fordham University, and Stanford University (2013) – This project explores ways to improve the usability of privacy policies by developing scalable technologies to semi-automatically extract key privacy policy features from website privacy policies, and presenting these features to users in an easy-to-digest format akin to nutrition labels on food products. This research will enable Internet users to make informed privacy decisions as they contemplate interacting with different websites.
- *Center for Encrypted Functionalities* at the University of California at Los Angeles, Stanford University, Columbia University, University of Texas at Austin, and Johns Hopkins University (2014) – This project explores new encryption methods to make a computer program, and not just its output, invisible to an outside observer, while preserving its functionality – a process known as program obfuscation. Members of this team recently discovered the first mathematically sound approach to encrypting functionalities – a breakthrough could reshape the way we think about security and computation.
- *Modular Approach to Cloud Security* at Boston University, the Massachusetts Institute of Technology, University of Connecticut, and Northeastern University (2014) – This project aims to investigate, design and test a modular approach to cyber security for cloud systems, with the aim of addressing the question of how the security of the system as a whole can be derived from the security of its components. The project has the potential to transform the way we build and reason about information systems with meaningful multi-layered security.

NSF aims to provide high-level visibility to grand challenge research areas in cyber security by enabling such center-scale activities that bring together interdisciplinary expertise from multiple institutions to focus in-depth on topics of national importance.

Cyber Security Programs

The discussion above focused on the different scales of NSF-funded cyber security research. Let me now take a programmatic view of these activities. The National Science Foundation funds a broad range of activities to advance cyber security research, develop a well-educated and capable workforce, and to keep all citizens informed and aware. FY 2015 investments in these activities include $126 million in the Secure and Trustworthy Cyberspace (SaTC) program, led by the Directorate for Computer and Information Science and Engineering (CISE) in partnership with the Directorates for Education and Human Resources (EHR), Engineering, Mathematical and Physical Sciences, and Social, Behavioral, and Economic Sciences. Currently, there are over 670 Secure and Trustworthy Cyberspace awards that are active, including 175 new research projects in 35 states that were funded in FY 2014 alone.

To provide some context about NSF's Secure and Trustworthy Cyberspace program, since FY 2012[11], this program has sought to secure the Nation's cyberspace by addressing two perspectives within the multi-dimensional cyber security 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, and 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. Research that contributes to the design of incentives, markets, or institutions to reduce either the likelihood of cyber-attack or the negative consequences of cyber-attack are especially encouraged, as are projects that examine incentives and motivations of individuals.

In FY 2013, the Secure and Trustworthy Cyberspace program began addressing a third perspective on *cyber security education,* with the goal to promote innovation, development, and assessment of new learning opportunities and to create and sustain an unrivaled cyber security workforce capable of developing secure cyberinfrastructure components and systems, as well as to raise the awareness of cyber security challenges to a more general population.

In FY 2015, the Secure and Trustworthy Cyberspace program has started explicitly addressing a fourth perspective, *Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS)*, with the goal 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), as I will describe later in my testimony.

Beyond these four perspectives, the Secure and Trustworthy Cyberspace program 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

[11] NSF has been investing in cyber security research for many years, including through the Trusted Computing (FY 2002-2003), Cyber Trust (FY 2004-2008), and Trustworthy Computing (FY 2009-2011) programs. Beginning in FY 2012, the Secure and Trustworthy Cyberspace program has aligned NSF's investments with the 2011 federal Strategic Plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. Since 2002, NSF has issued over 1,700 cyber security awards.

operational environment. Such efforts can result in fielded capabilities and innovations of direct benefit to networks, systems, and environments supporting NSF science and engineering research and education communities. Areas of emphasis for these "transition to practice" investments have included malware detection and prevention, situational understanding, data assurance, risk analysis, and software assurance.

In addition to the Secure and Trustworthy Cyberspace 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 sciences, cyber-physical systems, smart health and wellbeing, future internet architectures, networking technology and systems, information integration and informatics; the social, behavioral, and economic sciences, including an understanding of market forces and social/cognitive factors associated with developing secure, trustworthy systems; engineering, including the development of advanced cyber security algorithms that can integrate with hardware architectures to improve the security of the Nation's critical communications, electric power, health, and financial information systems; and the mathematical and physical sciences, including the foundations of cryptographic, statistical, topological, and graph-based methods and algorithms, as well as risk analysis and assessments to address challenges in cyber security.

NSF's support of cyber security research includes a focus on privacy. In FY 2014, NSF invested about $25 million to support privacy research as an extension of security, including exploring basic privacy constructs and their application in many areas of information technology. NSF's privacy support is largely driven bottom-up by research proposals from the academic research community.

Indeed, across its cyber security research and development programs, 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, long-term, often interdisciplinary or multi-disciplinary ideas, which are evaluated by the best researchers through the merit review process. This process, which supports the vast majority of unclassified cyber security research in the U.S., has led to innovative and transformative results, some of which I have previously described in my testimony.

(2) Why is NSF supported research important to individuals and industry?

(3) What impact does NSF research have on the cyber-industry, including critical infrastructure?

Allow me to answer these two questions below.

As part of its cyber security investments, NSF promotes partnerships between academia and industry. These are critical to a healthy trustworthy computing ecosystem. They enable discoveries to transition out of the lab and into the field as threats and solutions co-evolve over time. And they ensure U.S. leadership, economic growth, and a skilled workforce.

Specifically, NSF envisions a thriving research community that will address major technological challenges for the next generation of devices and systems, including the security and trustworthiness of these devices and systems. As part of this effort, NSF supports fundamental research underlying device and component technologies, power, controls, computation, networking, communications and cyber technologies. NSF supports the integration and networking of intelligent systems principles at the nano-, micro-, and macro-scales for a variety of application domains spanning healthcare, homeland security,

disaster mitigation, energy, telecommunications, environment, transportation, manufacturing, and other systems-related areas.

NSF has therefore worked closely with the Semiconductor Research Corporation (SRC), the world's leading technology research consortium consisting of member companies and university research programs across the globe, in the area of hardware security. Through the Secure, Trustworthy, Assured, and Resilient Semiconductors and Systems (STARSS) perspective within the Secure and Trustworthy Cyberspace program, NSF and SRC are funding innovations in hardware security and facilitating close collaborations between academic researchers and industry.

Computing processors meet a huge range of needs, from leading-edge processors that are the "brains" behind critically-important systems and infrastructure, including networking and communications, electric power grids, finance, military, and aerospace systems, to smaller embedded processors, sensors, and other electronic components that provide "smart" functionality and connectivity in a variety of applications, such as automotive braking and airbag systems, personal healthcare, industrial controls, and the rapidly growing list of connected devices often called the "Internet of Things" (IoT). The wide range of devices and applications together with the exponential growth of the number of connected "things" has made security and trustworthiness a prime concern.

Design and manufacture of today's complex hardware systems requires many steps and involves the work of hundreds of engineers, typically distributed across multiple locations and organizations worldwide. Today, semiconductor circuits and systems are designed so as to make it feasible or easier to verify, manufacture and test during subsequent steps. However, what is needed is an understanding of how to design for assurance, with the objective of decreasing the likelihood of unintended behavior or access, increasing resistance and resilience to tampering and counterfeiting, and improving the ability to provide authentication in the field. Designing for assurance requires new strategies for architecture and specification, and tools for synthesis, physical design, test, and verification, especially at the stages of design in which formal methods are currently weak or absent. It is imperative to develop a theoretical basis for hardware security in order to design systems that are free of vulnerability and that are assured and resilient against attacks, even vulnerabilities and attacks that are not (yet) known. Through our partnership, NSF and SRC jointly funded nine projects in FY 2014 spanning these areas, with additional awards anticipated in FY 2015.

NSF is also partnering with Intel Corporation in the area of cyber-physical systems, security and privacy. The national and economic security of the U.S. depends on the reliable function of critical infrastructure. This infrastructure is rapidly being advanced through the integration of information and communication technologies, leading to cyber-physical systems. Advances in CPS will enable capability, adaptability, scalability, and usability that will far exceed the simple embedded systems of today. CPS technologies will transform the way people interact with engineered systems – just as the Internet has transformed the way people interact with information. New smart CPS will drive innovation and competition in sectors such as food and agriculture, energy, different modes of transportation including air and automobiles, building design and automation, healthcare and medical implants, and advanced manufacturing.

Cyber-physical systems are subject to threats stemming from increasing reliance on computer and communication technologies. Cyber security threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, public safety, and health at risk.

The goal of our partnership with Intel is to foster novel, transformative, multidisciplinary approaches that ensure the security of current and emerging cyber-physical systems, taking into consideration the unique challenges present in this environment relative to other domains with cyber security concerns. These challenges arise from the non-reversible nature of the interactions of CPS with the physical world; the scale of deployment; the federated nature of numerous infrastructures; the deep embedding and long projected lifetimes of CPS components; the interaction of CPS with users at different scales, degrees of control, and expertise levels; the economic and policy constraints under which such systems must often operate; and the sensing and collection of information related to a large spectrum of everyday human activities. The first set of joint NSF/Intel awards are planned for FY 2015.

NSF has also invested in two active Industry/University Cooperative Research Centers (I/UCRCs), which feature high-quality, industrially relevant fundamental research, strong industrial support of and collaboration in research and education, and direct transfer of university-developed ideas, research results, and technology to U.S. industry to improve its competitive posture in world markets. I/UCRCs, in general, are a great investment in the future. Across the I/UCRC program, over 2,000 students were supported in 2014, with 649 attaining their degrees, including 185 students who were hired directly by industrial members of their I/UCRCs. On average, I/UCRCs saw a six to one leveraging of NSF funds in 2014. The two cyber security-related centers are:

- *CITeR: Center for Identification Technology Research (Biometrics)* at Clarkson University, the University of Arizona, West Virginia University, University of Buffalo, and Michigan State University – CITeR aims to advance understanding in biometrics and credibility assessment central to realization of next generation identification management systems necessary for private sector and government applications. CITeR's research includes iris, fingerprint, face, voice, and gait 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 application areas, ranging from driver's licenses to passports and visas, for example.
- *S2ERC: Security and Software Engineering* at Ball State University, Iowa State University, Virginia Tech, and Georgetown University – S2ERC investigates integrated methods of engineering practical software systems that are able to meet emerging security requirements. This goal is important 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. Recent S2ERC research projects have focused on software design, metrics, testing, and reliability in the face of intrusion detection, ad-hoc network security, wireless security, attack-tolerant systems, and trustworthiness in cloud and mobile applications.

Beyond these academic/industry collaborations, a critical aspect of the SaTC program for all research projects is the Transition to Practice, or TTP, option, which supports proposed research activities and ideas whose outcomes at the end of the award are capable of being implemented, applied, experimentally used, or deployed in an operational environment. Transitioning research into practice, whether in research programs, commercial products, or use in government agencies shortens the time from ideas to practical solutions.

NSF is also co-funding "Innovation Transitions" (InTrans) awards with industry partners for cyber security research teams at the point of completing their center-scale projects, with the goals of continuing the long-term vision and objectives of the project team, maturing and deploying successful research and innovation results in industry, and facilitating the transition of the innovations to support from industrial sponsors with the potential to develop new technologies.

NSF-funded cyber security research has also led to the formation of numerous start-up companies in the IT sector and the take-up of new products and services, all of which bring innovative solutions to the marketplace, spurring job growth and helping to protect cyberspace. NSF has supported these start-ups through specific programs, including:

- The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs stimulate technological innovation in the private sector by strengthening the role of small business concerns in meeting federal research and development needs, increasing the commercial application of federally supported research results, and fostering and encouraging participation by socially and economically disadvantaged and women-owned small businesses. Outcomes of several NSF-funded cyber security research projects have led to NSF SBIR and STTR grants.
- The NSF Innovation Corps™ (I-Corps™) is a public-private partnership that teaches grantees to identify valuable product opportunities that emerge from academic research, and offers entrepreneurship training to student participants. Since the inception of the NSF Innovation Corps™ program in 2011, a number of I-Corps™ Teams in the cyber security domain have participated in the I-Corps™ curriculum.

Finally, a number of NSF-funded researchers, particularly those working in larger, inter- or multidisciplinary teams, collaborate closely with industry to deepen and extend the outcomes of their research activities. For example, NSF-funded researchers at the University of California at San Diego and University of Washington have demonstrated the ability to remotely take over automotive control systems[12]. 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 (SAE) and the United States Council for Automotive Research (USCAR) have partnered with the researchers to stand up efforts focused on automotive security research[13]. Automotive manufacturers have also started dedicating significant resources to security[14].

Similarly, NSF-funded researchers at the University of Michigan, University of Massachusetts Amherst, and University of Washington were able to gain wireless access to a combination heart defibrillator and pacemaker, reprogramming it to shut it down and to deliver jolts of electricity that could have potentially been fatal if the device had been implanted in a person. This research team is now collaborating with industry, including the Medical Device Innovation, Safety, and Security (MDISS) Consortium, Association for the Advancement of Medical Instrumentation (AAMI), and specific biomedical device companies, including Medtronic, Philips Healthcare, Siemens Healthcare, and Welch Allyn, to prevent illegal or unauthorized hacking of devices that have wireless capabilities. For each of the last two years, this NSF-funded research team has also held a Medical Device Security Workshop[15,16] to bring together solution-oriented experts in medical device manufacturing and computer security to meet and discuss effective ways to improve information security and inform Food and Drug Administration (FDA) guidelines on cyber security. Additionally, the research team has created a

[12] http://www.nytimes.com/2011/03/10/business/10hack.html
[13] http://www.autosec.org/faq.html
[14] http://www.caranddriver.com/features/can-your-car-be-hacked-feature
[15] http://secure-medicine.org/workshop/2014
[16] http://secure-medicine.org/workshop/2013

traveling classroom for medical device manufacturers, and has provided private on-site security engineering education and training to over 500 employees from a half-dozen major medical device manufacturers. We expect such academic/industry collaborations to continue to grow as new cyber security challenges and results emerge.

Education and Workforce Development

NSF's investments in cyber security 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.

Supporting the Next Generation of Cyber Security Researchers

In recent years, through the Research Experiences for Undergraduates (REU) program, NSF has supported several REU Sites based on independent proposals that seek to initiate and conduct projects that engage a number of undergraduate students in research. REU Sites must have a well-defined common focus, based in a single discipline or spanning interdisciplinary or multi-disciplinary research opportunities with a coherent intellectual theme, which enables a cohort experience for students. Each REU Site typically supports 8 to 12 undergraduate students each summer, including housing and stipend support, with each student involved in a specific project guided by a faculty mentor. REU Sites are an important means for extending high-quality research environments and mentoring to diverse groups of students. NSF's investments in REU Sites focused on cyber security and information assurance include:

- *Trustable Computing Systems Security Research and Education* at the University of Connecticut;
- *Information Assurance and Security* at Dakota State University;
- *Undergraduates Engaged in Cyber Security Research* at the University of Maryland;
- *Site for Extensive and Collaborative Undergraduate Research Experience (SECURE)* at the University of Nebraska at Omaha;
- *Multidisciplinary Information Assurance and Security* at Purdue University; and
- *Digital Forensics Research in Rhode Island* at the University of Rhode Island.

Over the years, the Secure and Trustworthy Cyberspace program has supplemented its awards by providing small amounts of additional funding to researchers to bring undergraduates into their labs throughout the school year through the REU program. This program gives many undergraduate students their first hands-on experiences with real science and engineering research projects. In addition, through the REU mechanism, the Secure and Trustworthy Cyberspace program has supplemented awards to provide research experiences for teachers in computer science and engineering, as well as for U.S. veterans who wish to engage in meaningful research experiences, as recommended by the April 2009 report of an NSF-funded workshop on *Veterans' Education for Engineering and Science*[17].

[17] http://www.nsf.gov/eng/eec/VeteranEducation.pdf

The Secure and Trustworthy Cyberspace program has provided awards to support travel and accommodations for students who wish to attend premier research conferences and workshops in information assurance and cyber security. Each award provides funding for 10 to 20 full-time students attending accredited institutions, who in turn can attend conferences and workshops to present their research, learn about advances in the field, and meet prospective colleagues and collaborators. SaTC student travel grant awardees encourage women and other underrepresented minorities to apply for these funds.

The Secure and Trustworthy Cyberspace program has also funded 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.

	FY 2012	FY 2013	FY 2014
SaTC CAREER awards	14	13	9
SaTC REU Sites and Supplements	34	32	42
SaTC conference student travel awards	11	15	15

Nurturing and Growing the Cyber Security PI Community

Additionally, the Secure and Trustworthy Cyberspace program has sought to broaden the cyber security research community, which is critical to facilitating advances in the field. For example, in FY 2013 and FY 2014, the program organized and held Aspiring SaTC Principal Investigators (PIs) workshops that sought to educate potential cyber security researchers on the priorities of the program and components of successful research projects. NSF plans to continue to use this approach to bring new researchers with a broad set of talents and interests into the SaTC PI community.

The program has also held biennial meetings of all its PIs, including most recently in FY 2013 and FY 2015. These meetings have sought to bring PIs together with representatives from academe, industry, and government, with the goals of understanding progress and identifying emerging research challenges; fostering collaboration and coordination among PIs, both within and across specific science and engineering disciplines; sharing experiences and learning from others' experiences in transitioning research into practice; and understanding strategies and methods for improving education, recruitment, and career development in cyber security.

Training for Cyber Security Professionals

Beyond the growth of the cyber security research and education community, the NSF Directorate for Education and Human Resources (EHR) has focused on increasing the number of professionals with degrees in cyber security. An overwhelming majority of these EHR-developed professionals were supported by the CyberCorps®: Scholarship for Service (SFS) and/or Advanced Technological Education (ATE) programs.

The SFS program provides funding to colleges and universities for scholarships and capacity building to increase the number of qualified students entering the fields of information assurance and cyber security and to increase the capacity of the higher education enterprise to produce professionals in those fields. 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 Cybersecurity Enhancement Act of 2014 (Public Law No. 113-274) directs NSF, in coordination with 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 cyber security mission for Federal, State, local, and tribal governments. The SFS program supports two tracks.

The Scholarship Track provides funds to colleges and universities to award scholarships to students in support of their education in areas relevant to cyber security. In return for their scholarships, recipients must agree to work after graduation for the federal government or, subject to approval from NSF, for a state, local, or tribal government in a position related to cyber security for a period equal to the length of the scholarship.

During the scholarship period, the students will participate in meaningful summer internships. Doctoral students may be allowed to replace their summer internship with a research activity following a recommendation from their academic advisor and approval of NSF.

To be eligible for consideration for an SFS scholarship, a student must be a U.S. citizen, be within two to three years of graduation in a coherent formal bachelor's, master's, or doctoral program focused on cyber security at an awardee institution, and be able to meet selection criteria for federal employment. Each proposing institution must provide a description of its selection criteria and process, and must submit their lists of candidates for SFS scholarships to OPM for final eligibility confirmation.

Through the end of FY 2014, the SFS program has provided scholarships to more than 2,300 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, and state, local, and tribal governments, including the National Security Agency, Department of Homeland Security, Central Intelligence Agency, and Department of Justice.

Graduating Class	
2002	9
2003	75
2004	153
2005	179
2006	172
2007	158
2008	122
2009	86
2010	121
2011	116
2012	175
2013	171
Jan-Sept 2014	170
Total	***1707***

Top 15 Universities (Students Enrolled FY 2009-2014)	
University of Tulsa	98
Carnegie Mellon University	72
Mississippi State University	60
California State University, San Bernardino	58
Northeastern University	42
University of North Carolina at Charlotte	42
Naval Postgraduate School	41
NYU - Polytechnic	40
Idaho State University	39
University of Illinois at Urbana Champaign	38
Air Force Institute of Technology	36
North Carolina A & T State University	35
Dakota State University	34
University of Nebraska at Omaha	28
University of Texas at Dallas	28
Other 38 universities	523
Total	***1240***

Placement FY 2009-14	
National Security Agency	120
US Navy	66
Mitre Corporation	53
Department of Homeland Security	50
Federal Reserve System	35
State, Local, & Tribal	34
Sandia Laboratory	32
Department of Defense	31
Software Engineering Institute	28
Central Intelligence Agency	27
US Air Force	23
US Army	23
Department of Treasury	21
Department of Justice	20
Lincoln Laboratory	20
Other	129
Total	***712***

The Capacity Track, provides funds to colleges and universities to expand existing educational opportunities and resources in cyber security and increase in the ability of the United States higher education enterprise to produce cyber security professionals. Examples of projects include: conducting research on the teaching and learning of cyber security, including research on materials, methods and small-scale interventions; establishing curricula recommendations for new courses, degree programs, and educational pathways with plans for wide adoption nationally; evaluating teaching and learning effectiveness of cyber security curricular programs and courses; integrating cyber security topics into computer science, information technology, engineering and other existing degree programs with plans for pervasive adoption; developing virtual laboratories to promote collaboration and resource sharing in cyber security education; strengthening partnerships between institutions of higher education, government, and relevant employment sectors leading to improved models for the integration of applied research experiences into cyber security degree programs; and evaluating the effectiveness of cyber security competitions and other outreach and retention activities.

From FY 2011 through FY 2014, the SFS program has made 117 awards totaling over $145 million 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 that drive our Nation's economy, including cyber security. The program involves partnerships between academic institutions and industry to promote improvement in the education of science and engineering technicians at the undergraduate

and secondary school levels. The ATE program supports curriculum development; professional development of college faculty and secondary school teachers; career pathways to two-year colleges from secondary schools and from two-year colleges to four-year institutions; and other activities. Another goal is articulation between two-year and four-year programs for K-12 prospective science, technology, engineering, and mathematics (STEM) teachers who focus on technological education.

The ATE program supports projects, centers, and targeted research on technician education. Activities may have either a national or a regional focus, but not a purely local one. A project or center is expected to communicate a realistic vision for sustainability and a plan for achievement. It is expected that at least some aspects of both centers and projects will be sustained or institutionalized past the period of award funding. Being sustainable means that a project or center has developed a product or service that the host institution, its partners, and its target audiences want continued.

Of 17 active ATE awards, four are focused on cyber security, including a national center, a resource center, and two regional centers:

- *National CyberWatch Center* (Maryland) – This center, originally established in 2005 at Prince George's Community College and re-funded as a national center in 2012, leads collaborative efforts to increase the quantity and quality of the cyber security workforce by advancing cyber security education. The center comprises over 50 two-year schools, over 50 four-year institutions in 33 states, over 30 industry partners, three government partners, six public school systems, and two non-profit organizations. It pursues curriculum development, faculty professional development, and K-12 initiatives. It is estimated that over 11,000 students have been impacted by the National CyberWatch Center's faculty development.
- *National Resource Center for Systems Security and Information Assurance (CSSIA)* (Illinois) – Originally established in 2003, this center, based at Moraine Valley Community College, seeks to support: innovative faculty development; expansion of comprehensive cyber competitions at the higher education and minority levels; development and expansive distribution of high-quality cyber security lab content; and remote virtualization content delivery and innovative virtualization lab environments. CSSIA has mentored, established, and expanded cyber security degree and certification programs at hundreds of institutions in over 30 states. In 2013 alone, 1,191 students participated in CSSIA-sponsored cyber security competitions.
- *Cyber Security Education Consortium (CSEC)* (Oklahoma) – Based at the University of Tulsa, this center is a partnership of community colleges and career and technology centers in eight states in the central U.S. CSEC has established cyber security certificate and degree programs at 49 two-year program sites in eight states, and signed over 120 articulation agreements that provide students with advanced placement, dual enrollment, or cyber security course credit at two- and four-year institutions. Since 2004, over 1,300 CSEC students have completed certificate programs in cyber security; over 800 others have received associate degrees; and over 200 others have attained bachelor's degrees in cyber security. In the 2013-14 academic year, CSEC had 2,337 security-related student enrollments.
- *CyberWatch West* (Washington) – The overarching goal of CyberWatch West is to strengthen the cyber security workforce in California and the Pacific Northwest. To accomplish this goal, CyberWatch West is concentrating on the following four major areas: (1) student activities, including meaningful internships and a cyber-defense league with weekly virtual exercises; (2) assistance in curriculum development based on recognized standards and creation of cyber security pathways from community colleges to four-year institutions; (3) a faculty development and mentor program to help infuse cyber security concepts into coursework; (4) outreach and partnership with regional

community colleges, universities, high schools, and industry to determine and assist with regional needs in cyber security education. CyberWatch West consists of 44 academic partners, plus three high-schools and 19 industry and government partners, and has an active enrollment of nearly 1,000 students, including a large minority student population.

In addition, there is an ATE large project entitled *Advanced Cyberforensics Education Consortium (ACE)* based at Daytona University (Florida), with 15 college partners in four states. ACE provides students with high-quality, hands-on educational experiences to increase marketability in the cyber security/forensics sectors of business and government. Since its establishment in January 2013, over 300 college students have completed at least one of the four core courses.

NSF has also supported several university pilots on cyber security education and secure programming. These pilots included the New Jersey Cyber Center project and New Jersey Governor's Cup; a Purdue University-led collaborative project linking student research teams with real-word projects mentored by technical directors at the National Security Agency; and an innovative competition at the University of Maryland to build secure systems.

Additionally, NSF continues to co-lead with the U.S. Department of Education the Formal Cybersecurity Education Component of the National Initiative for Cybersecurity Education (NICE). The goal of NICE is to establish an operational, sustainable and continually improving cyber security education program for the Nation to use sound cyber practices that will enhance the Nation's security. The National Institute of Standards and Technology (NIST) is leading the NICE initiative in collaboration with other federal departments and agencies, including NSF, to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability. NSF's involvement in the Formal Cybersecurity Education Component aims to bolster formal cyber security education programs encompassing kindergarten through twelfth grade, 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.

Collaboration Across the Federal Government

Finally, it is essential to describe the National Science Foundation's close coordination and collaboration with other federal agencies pursuing cyber security research and development activities.

Cyber Security R&D Strategic Plan

As mentioned earlier, in 2011, the National Science and Technology Council (NSTC), with the cooperation of NSF, put forward a strategic plan titled *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*[18]. As noted in the Strategic Plan, three important principles guided its development, and NSF's approach to cyber security is aligned with these:

- The research must aim at underlying cyber security deficiencies and focus on root causes of vulnerabilities – that is, we need to understand and address the causes of cyber security problems as opposed to just treating their symptoms.
- The Strategic Plan must channel expertise and resources from a wide range of disciplines and sectors. Cyber security is a multi-dimensional challenge, involving both the strength of security technologies and variability of human behavior. Therefore, solutions will depend not only on

[18] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

expertise in mathematics, computer science, and electrical engineering, but also in biology, economics, and other social and behavioral sciences.
- Cyber security principles must be enduring, allowing us to stay secure despite changes in technologies and in the threat environment. Whether we use desktop computers, tablets, mobile phones, control systems, Internet-enabled household appliances, or other cyberspace-enabled devices yet to be invented, we must be able to maintain and fulfill our trust requirements to ensure our continued security and safety.

The Plan specifies four strategic thrusts to organize activities and drive progress in cyber security R&D across the federal government:

- Inducing Change – Utilizing game-changing themes to direct efforts towards understanding the underlying root causes of known current threats with the goal of disrupting the status quo with radically different approaches to improve the security of the critical cyber systems and infrastructure that serve society.
- Developing Scientific Foundations – Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cyber security through adoption of a systematic, rigorous, and disciplined scientific approach. Promotes the discovery of laws, hypothesis testing, repeatable experimental designs, standardized data-gathering methods, metrics, common terminology, and critical analysis that engenders reproducible results and rationally based conclusions.
- Maximizing Research Impact – Catalyzing integration across the game-changing R&D themes, cooperation between governmental and private-sector communities, collaboration across international borders, and strengthened linkages to other national priorities, such as health IT and Smart Grid.
- Accelerating Transition to Practice – Focusing efforts to ensure adoption and implementation of the powerful new technologies and strategies that emerge from the research themes, and the activities to build a scientific foundation so as to create measurable improvements in the cyber security landscape.

Finally, rather than focusing on specific technical problems and solutions, the Strategic Plan articulates desired end-states and capabilities, thereby inviting a diversity of approaches and encouraging innovation across disciplines and sectors. The research themes that are prioritized in the Plan and worthy of further inquiry include:

- The science of cyber security will develop the underlying fundamental principles that allow for the adoption of a more scientific approach to building, maintaining, and using trustworthy systems.
- The designed-in security theme focuses on developing capabilities to design and evolve high-assurance systems resistant to cyber-attacks, whose assurance properties can be verified. Such development capabilities offer the path to dramatic increases in the security and safety of software systems.
- Moving target defense research aspires to elude attackers through diverse, shifting, and increasingly complex cyber techniques and mechanisms.
- The tailored trustworthy spaces theme supports research into varying trustworthy space policies and services that are context specific with the aim to create flexible, distributed trust environments.

- The cyber economic incentives theme focuses on research at the interstices of the economic and computer sciences to achieve secure practices through market mechanisms and behavioral incentives.

Coordination Across the Government

Beyond the Strategic Plan, 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 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 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 Cyber Security Initiative (CNCI)[19]. 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 cyber security.
- Based on this directive, a NITRD Senior Steering Group (SSG) for Cyber Security and Information Assurance R&D (CSIA R&D)[20] was established to provide a responsive and robust conduit for cyber security R&D information across the policy, fiscal, and research levels of the government. The SSG is composed of senior representatives of agencies with national cyber security leadership positions, including: DoD, Office of the Director of National Intelligence (ODNI), DHS, NSA, NSF, NIST, Office of Science and Technology Policy, and Office of Management and Budget. A principal responsibility of the SSG is to define, coordinate, and recommend strategic federal R&D objectives in cyber security, and to communicate research needs and proposed budget priorities to policy makers and budget officials. One of CISE's Division Directors is the co-chair of this group.
- The NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)[21] coordinates cyber security and information assurance research and development across the member agencies, including DoD, the Department of Energy and the National Security Agency, which focus on research and development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems.
- 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. SCORE, which includes members from the CSIA R&D SSG and IWG, is intended to work in parallel to the CSIA R&D IWG. NSF research is reported in this forum.
- 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 several workshops, including in FY 2014:

[19] http://www.nitrd.gov/subcommittee/csiacyberlink.html

[20] https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_Information_Assurance_Research_and_Development_Senior_Steering_Group_%28CSIA_R%26D_SSG%29

[21] https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_and_Information_Assurance_Interagency_Working_Group_(CSIA_IWG)

- A "Science of Cyber Security" workshop that considered specific foundational problems (e.g., metrics, fundamental results, evidence-based research, and protection of critical infrastructure); and
- A "Cyber Security 2025" workshop that sought to catalyze a community-wide discussion to review progress relative to the federal strategic plan and to envision long-term research agendas for the field.

- In February 2014, NSF convened a workshop with participation from across the federal government as well as academe and the private sector to generate actionable ideas that could potentially be pursued or adopted by cyber security researchers, policymakers, or practitioners to advance cyber security. The recommendations that emerged from the workshop are grouped into three categories – technology, policy, and leadership – and are described in detail in the final report[22].
- Through NITRD, NSF and the DHS Science and Technology Directorate have worked together to identify and co-fund emerging security technologies that will transition into operational use in both the private sector and government. The first example of this collaboration is the ShellOS project at the University of North Carolina at Chapel Hill[23], which identifies malware in email attachments more rapidly and accurately than commercial products, and stops such malware attacks before users can download the infected attachments.

An Increasing Emphasis on Privacy R&D

Through the CSIA R&D SSG, NSF is supporting the development of a National Privacy Research Strategy (NPRS) that will establish objectives and prioritization guidance for federally-funded privacy research, provide a framework for coordinating R&D in privacy-enhancing technologies, and encourage multi-disciplinary research that recognizes the responsibilities of the government and needs of society, and that enhances opportunities for innovation in the digital realm. As part of this effort, the CSIA R&D SSG published a Request for Information in September 2014[24]. On the basis of this input[25], the CSIA R&D SSG is convening a cross-sector workshop in February 2015 to surface key privacy perspectives, needs, and challenges that should be considered in forming a privacy research strategy; to gain a better understanding of what objectives should guide federal privacy research; and to examine prospective research themes that might be used to organize and prioritize federal research in privacy. The workshop, which will span government, commercial, individual, and societal perspectives, aims to decompose privacy into areas where goals for privacy research could be established; create a framework that links privacy research objectives into a coherent picture; and formulate research objectives in ways that invite a variety of contributions and approaches from many disciplines. The National Privacy Research Strategy follows a review by the National Coordination Office (NCO) on privacy research activities pursued by agencies in NITRD that sought to understand what research is taking place and to begin exploring a multi-agency research agenda in the foundations of privacy[26].

Conclusions

My testimony today has emphasized that the pace and scope of today's cyber threats pose grand challenges to our national critical infrastructure, and that NSF has been making, and continues to make,

[22] http://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf
[23] https://www.usenix.org/legacy/event/sec11/tech/full_papers/Snow.pdf
[24] https://federalregister.gov/a/2014-22239
[25] https://www.nitrd.gov/cybersecurity/nationalprivacyresearchstrategy.aspx
[26] https://www.nitrd.gov/Pubs/Report_on_Privacy_Research_within_NITRD.pdf

significant investments across multiple directorates in foundational and multi-disciplinary cyber security research, resulting in important advances over the years as well as identifying fundamentally new research directions and creating opportunities for the future. Indeed, our Nation needs to continue to invest in long-term, fundamental and game-changing research if our cyber systems are to remain trustworthy in the future. I have also described how 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. I have discussed how NSF partners with industry and other government agencies to address cyber threats and to advance cyber security R&D. I appreciate the opportunity to have this dialogue with members of this Subcommittee 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

JAMES F. KUROSE

James F. Kurose is the National Science Foundation Assistant Director for the Computer and Information Science and Engineering (CISE) Directorate. Prior to joining NSF, he was a Distinguished Professor in the School of Computer Science at the University of Massachusetts Amherst, where he led research projects on computer network protocols and architecture, network measurement, sensor networks, multimedia communication, and modeling and performance evaluation. Dr. Kurose also currently serves as co-chair of the Networking and Information Technology Research and Development (NITRD) Subcommittee of the National Science and Technology Council (NSTC) Committee on Technology, providing overall coordination for the IT R&D activities of 18 federal government agencies and offices.

At NSF, Dr. Kurose guides the CISE directorate in its mission to advance the Nation's leadership in computer and information science and engineering through its support for fundamental and transformative research, as well as the development and use of cyberinfrastructure across the science and engineering enterprise. These activities are critical to ensuring economic competitiveness and achieving national priorities. With a budget of nearly $900 million, CISE supports ambitious long-term research and innovation, advanced cyberinfrastructure to enable and accelerate discovery and innovation across all disciplines, 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 three decades at the University of Massachusetts Amherst, Dr. Kurose served in a number of administrative roles including chair of the Department of Computer Science, interim dean and executive associate dean of the College of Natural Sciences, and senior faculty advisor to the Vice Chancellor for Research and Engagement. He has been a visiting scientist at IBM Research, INRIA, Institut EURECOM, the University of Paris, the Laboratory for Information, Network and Communication Sciences, and Technicolor Research Labs. He helped found and lead the Commonwealth Information Technology Initiative and the Massachusetts Green High Performance Computing Center.

He has served as editor-in-chief of the Institute of Electrical and Electronics Engineers (IEEE) *Transactions on Communications* and was the founding editor-in-chief of the *IEEE/ACM* (Association for Computing Machinery) *Transactions on Networking.* With Keith Ross, he coauthored the textbook, *Computer Networking: A Top-Down Approach,* which is in its sixth edition.

Dr. Kurose has received recognition for his research, including the IEEE Infocom Achievement Award and the ACM Sigcomm Test of Time award. He has also been recognized for his educational activities, receiving the IEEE/CS Taylor Booth Education medal and the Massachusetts Telecommunication Council Workforce Development Leader of the Year award.

Dr. Kurose has served on a variety of advisory boards, including on the CISE advisory committee and the Board of Directors for the Computing Research Association.

Dr. Kurose holds a Bachelor of Arts degree in physics from Wesleyan University, and a Master of Science and a Ph.D. in computer science from Columbia University. He is a fellow of the IEEE and ACM.