Testimony of

Joan Ferrini-Mundy, Ph.D.
Assistant Director for Education and Human Resources
National Science Foundation

Before the
Subcommittee on Information Technology

for the
Committee on Oversight and Government Reform
U.S. House of Representatives

September 22, 2016

"Closing the Talent Gap in Federal Information Technology"

Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the Subcommittee. My name is Joan Ferrini-Mundy and I am the National Science Foundation's Assistant Director overseeing Education and Human Resources (EHR). I appreciate the opportunity to testify before you today.

The mission of NSF is "to promote the progress of science; to advance the national health, prosperity and welfare; [and] to secure the national defense…" NSF has a longstanding commitment to supporting research that drives scientific discovery, maintains America's global competitiveness, and builds the modern workforce that is critical for addressing the complex challenges that face the Nation. Within NSF, the mission of the EHR directorate is to provide the research foundation to develop a science, technology, engineering, and mathematics (STEM)-literate public and a diverse STEM workforce ready to lead science, engineering, and innovation for the future. Several NSF-supported programs have a key role in closing the talent gap in Federal information technology, and in the information technology (IT) workforce more generally. Here I highlight the NSF's CyberCorps®: Scholarship for Service (SFS) and Advanced Technological Education (ATE) programs in detail, and mention several other areas of investment that are critical to the development of the high-tech STEM workforce. I also will address NSF's contribution toward engaging, encouraging, and supporting a longer-term solution to the need for a larger and well-prepared Federal and national IT workforce of the future. Finally, I will briefly describe NSF's broader collaborations across the Federal government in the area of cybersecurity education.

The Cybersecurity Challenge and Preparation of Tomorrow's STEM Workforce

Advances in information technology (IT) have transformed all of our lives, enhancing our communications, expanding our capabilities, improving quality and personalization in a variety of sectors, and creating new economic and social opportunities. Every aspect of society has been transformed by the IT revolution, which is critical to national priorities in commerce, education, financial services, healthcare, manufacturing, and defense. Yet those same advances come with vulnerabilities: we hear all too often about cybersecurity breaches in government as well as major consumer companies, often impacting our own personal data. These incidents have increased a demand for cybersecurity professionals that far exceeds the supply. According to a report by the RAND Corporation in 2014[1], reports from numerous sources agree that there is a shortage of cybersecurity professionals and it is more pronounced for the federal government.

More broadly, as more recent innovations in IT such as machine learning, big data, artificial intelligence, sensor and instrumental technologies, the Internet of Things (IoT), and robotics shape daily life, education, and the workplace, NSF programs for the preparation of the computer science and STEM workforce play a key role in preparing the cybersecurity workforce of tomorrow, and also more generally a diverse STEM workforce that will be ready for leadership and innovation in data-rich and technology-enabled science, technology and engineering fields.

I will highlight briefly key programs at NSF for preparation of the cybersecurity workforce.

The CyberCorps®: Scholarship for Service Program

The CyberCorps®: Scholarship for Service (SFS)[2] program aims to develop a well-educated cybersecurity workforce for the government through engagement with educators (colleges and universities) and the target employers (government agencies). This program, originally named the Federal Cyber Service: SFS Program, was created as a result of a May 1998 Presidential Decision Directive (PDD-63)[3] 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[4], which included the Federal Cyber Services training and education initiative and the creation of a SFS program. More recently, *The Cybersecurity Enhancement Act of 2014* (Public Law No. 113-274) directed NSF, in coordination with the U.S. Office of Personnel Management (OPM) and the U.S. Department of Homeland Security (DHS), to continue the SFS program to recruit and educate 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.

The SFS program funds institutions of higher education, on the basis of their proposals to the NSF competitive merit review system, to develop and enhance cybersecurity education programs and curricula and to provide scholarships to undergraduate and graduate students in strong academic programs in cybersecurity. The institutions must present a clear proposal for why their program is of high quality for the preparation of cybersecurity professionals, at the level of the National Security Agency (NSA) and DHS National Centers of Academic Excellence criteria. The students receiving scholarships must be U.S. citizens or lawful permanent residents of the US and must be able to meet the

[1] http://www.rand.org/pubs/research_reports/RR430.html
[2] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991
[3] http://fas.org/irp/offdocs/pdd/pdd-63.htm
[4] https://fas.org/irp/offdocs/pdd/CIP-plan.pdf

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 agencies and students in forging good matches, the NSF program requires a summer internship at a Federal agency. NSF also partners with OPM to host an annual job fair for SFS students and prospective Federal employers.

The SFS program aims for a 100 percent placement rate in government cybersecurity-related positions. The placement rates for the 2013 and 2014 graduating classes were 97 percent and 95 percent, respectively. The placements for the 2015 graduating class are not yet complete but at present 92 percent have been placed. The overall placement rate of SFS graduates in government is 94 percent. As of August 2016, there were 62 active SFS institutions, 2909 scholarship recipients, 2213 graduates and 612 current students. 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 (CIA), and U.S. Department of Justice (DOJ), along with state, local, and tribal governments.

The programmatic aspects of SFS represent forward-looking thinking in terms of what are the most effective means of preparation for cybersecurity professionals. As part of a broad education including computer science, SFS-funded programs incorporate emphases on data science, computer systems architecture, analytics and algorithms, statistics, engineering, social and behavioral sciences, and business and information science.

I would like to highlight the fact that the University of Texas at San Antonio (UTSA) successfully competed for an NSF SFS award, and over the course of six years, UTSA has provided scholarships to support 22 cybersecurity students. Of the students who have graduated from UTSA, all are reported to continue to be employed by the Federal government with the exception of two who deferred their government service commitment in order to obtain graduate degrees. UTSA is a Hispanic-Serving Institution (HSI) with more than 58 percent of its students coming from groups underrepresented in higher education. UTSA is just one example of how the SFS program is helping to increase the pool of well-prepared cybersecurity professionals for the Nation by recruiting students, including those from underrepresented groups, into cybersecurity and information technology careers.

Other established SFS projects are in place throughout the nation. For example, the SFS project at the New Mexico Institute of Mining and Technology provides practical, hands-on applications of cybersecurity coordinated among several academic departments. Research projects are integrated into advanced courses to enhance problem-solving skills. An underlying curriculum principle is to integrate cybersecurity context into all core computer science and engineering and IT courses.

At Carnegie Mellon University, which offers master's level work in cybersecurity, the SFS project features cutting-edge project-based coursework and requires a course in ethics and a project in cybersecurity. The SFS project at the University of Arizona recruits students from throughout the state, with a particular emphasis on recruiting and retaining underrepresented minorities. The project is cross-disciplinary and supports cybersecurity in its broadest definition, including information assurance, network security, information security risk management, and security management practices. The project contributes to meaningful curriculum development that can serve as a model for other programs.

At California State University, San Bernardino, most SFS students are first-generation minority students, transferring from community colleges, often from low-income and disadvantaged backgrounds. This project places great emphasis on ensuring that this diverse student cohort (50 percent Hispanic and 43 percent female) learns the skills required for them to successfully obtain and retain professional employment. Representatives of the program have mentored leaders of other institutions regarding the best practices in recruiting for diversity, placement strategies, leveraging university resources, and project management.

An additional thrust for SFS was put forward earlier this year. The President's Cybersecurity National Action Plan[5] proposes a CyberCorps Reserve program so that SFS alumni may be available over the course of their careers to help the Federal government respond to cybersecurity challenges. The NSF role, as proposed in the President's Fiscal Year (FY) 2017 Budget Request, would be to invest in "the expansion of the SFS program to lay the groundwork for SFS program alumni to be available over the course of their careers to serve the federal government's response to cybersecurity challenges." NSF is participating in a multi-agency effort led by the Office of Management and Budget (OMB) and OPM, along with DHS, the U.S. Department of Defense (DOD), and the U.S. Department of Energy (DOE), to develop models for rapid deployment of cybersecurity teams in crisis situations.

A second emphasis of the SFS program is expansion of the capacity of the U.S. higher education enterprise to prepare cybersecurity professionals who are highly qualified for a changing future. These efforts include research on the teaching and learning of cybersecurity, done in connection with the development of curricula, the integration of cybersecurity topics into relevant degree programs, and the design of virtual learning laboratories. In addition NSF supports strengthening partnerships between government and relevant employment sectors to effectively integrate applied research experiences into cybersecurity degree programs, and to integrate data science and other emerging topics into cybersecurity curricula.

Because the SFS program is a part of the larger cybersecurity ecosystem, SFS collaborates to stimulate the development of the cybersecurity workforce of the future. SFS supports "Inspiring the Next Generation of Cyber Stars" ("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. In the summer of 2016, 120 camps at 68 institutions spanning 33 states, plus the District of Columbia and Puerto Rico) engaged about 4,000 students and about 800 K-12 teachers, with support from NSF and NSA.

The SFS program actively seeks to promote greater diversity in the cybersecurity workforce. As one strategy, the program has supported partnerships between majority institutions with strong cybersecurity programs and minority-serving institutions. For example, the University of North Carolina at Charlotte collaborates with two Historically Black Colleges and Universities (HBCUs), North Carolina A&T State University and Johnson C. Smith University, to support students earning bachelor's, master's, and doctoral degrees in cybersecurity. In 2013, NSF funded the launch of the annual Women in Cybersecurity Conference in 2013, an activity now supported by Facebook, Fidelity Investments, IBM,

[5] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

and many other industry, government, and academic partners. Since 2014, the Women in Cybersecurity Conference has maintained a continuing effort to recruit, retain, and advance women in cybersecurity. It brings together women (students, faculty, researchers, and professionals) in cybersecurity from academia and industry to share knowledge, experience, networking, and mentoring on an annual basis. Beyond the annual conference, Women in Cybersecurity has become a community of engagement, encouragement and support for women in the cybersecurity field.

Advanced Technological Education

NSF's Advanced Technological Education (ATE)[6] program addresses the need for IT and cybersecurity personnel at a different educational level and in a different way than SFS. With an emphasis on two-year colleges, ATE focuses on the education of technicians for the high-technology fields that drive our Nation's economy, including information technology and cybersecurity. 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.

ATE 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; research on the improvement of the preparation of the technology workforce, and other related activities.

The ATE program funds large, comprehensive Centers of Excellence, as well as smaller-scale, more focused projects. These efforts may have either a national or a regional focus. The following are the program's major awards supporting cybersecurity education:

Advanced Cyberforensics Education (ACE) Consortium (www.cyberace.org) (Florida) involves over a dozen institutions across Florida, Georgia, South Carolina, and North Carolina. The primary goals are to develop and disseminate cyberforensics curricula, provide professional development for faculty members, and create interest in cybersecurity among high school students.

Cyber Security Education Consortium (CSEC; www.cseconline.net/2014/) (Oklahoma) is a regional center that involves over 40 two-year academic institutions in eight states (Oklahoma, Arkansas, Colorado, Kansas, Louisiana, Missouri, Tennessee, and Texas). Over 100 faculty members offer courses based on CSEC's core information assurance and forensics curriculum, which encompasses information assurance principles, secure electronic commerce, network security, enterprise security management, and digital forensics. Particular emphases are automation and control systems security and mobile-device security.

Center for Systems Security and Information Assurance (CSSIA; www.cssia.org) (Illinois) focuses on providing faculty development and a cutting-edge virtual teaching and learning environment for cybersecurity. CSSIA's Faculty Development Academy has offered courses and workshops (both face-to-face and online) for thousands of educators. CSSIA's virtual teaching and learning environment has been adopted by several hundred educational institutions and is also used extensively for cybersecurity student competitions. CSSIA also leads several initiatives that encourage minorities, women, and veterans to pursue careers in cybersecurity.

[6] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5464

CyberWatch West (CWW; www.cyberwatchwest.org) (Washington) is a regional ATE center that focuses on cybersecurity education and workforce development in 14 Western states. Activities include providing model curricula, offering workshops for faculty, facilitating student participation in intercollegiate cyber defense competitions, and mentoring community colleges that aim to achieve designation as a National Center of Academic Excellence in Cyber Defense – 2-Year Education (CAE-2Y).

National CyberWatch Center (NCC; www.nationalcyberwatch.org) (Maryland) cultivates collaborations among educational institutions, businesses, government agencies, and professional organizations to grow and strengthen cybersecurity education programs and the cybersecurity workforce. NCC's network includes over 200 two-year and four-year institutions in almost all 50 states. Key initiatives include developing and updating cybersecurity degree and certificate programs in cyber defense, network forensics, network security administration, secure software development, and systems security administration; mapping curricula to federal and industry knowledge-and-skill standards, job roles, and professional certifications; and creating model transfer pathways that allow students to move between two-year and four-year degree programs.

Other Programs for the Preparation of Cybersecurity and IT Professionals

In addition to SFS and ATE, NSF hosts other programs that are intended to, in part, support the development of the IT and STEM workforce. One of these is the Research Experiences for Undergraduates (REU)[7] program, which offers intensive summer research experiences to nearly 5,000 college and university students every year in all of the fields of STEM supported by NSF—including computer science broadly and cybersecurity specifically. In cybersecurity alone, over a dozen NSF-funded REU Sites currently prepare students with research skills that will enable them to pursue graduate school or employment in areas spanning the security of critical infrastructure; security of mobile devices, wireless networks, cyber-physical systems, cloud computing, e-commerce, and software; privacy; and digital forensics.

Two other programs important to workforce development are funded with H-1B Visa Receipts. The Scholarships for STEM (S-STEM) program[8] supports undergraduates with high financial need to pursue STEM careers, and the Innovative Technology Experiences for Students and Teachers (ITEST)[9] provides support to engage K-12 students and teachers in experiences to prepare students to consider STEM and IT career options. Within both programs are examples of outstanding projects focused on preparation of cybersecurity professionals. For example, the ITEST program supports an award to excite girls about IT through after-school and summer programs, and a project to study the effectiveness of a career academy on information technology education. S-STEM supports a project at Capitol Technology University (Laurel, Maryland) for place-bound community college graduates so that they can complete a bachelor's degree at a distance, making it possible for them to join the cybersecurity workforce. Recruitment of new students focuses on minorities and first-generation college students who might not otherwise complete a bachelor's degree.

[7] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5517&from=fund
[8] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5257
[9] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5467

Developing a Computer-Literate Workforce and Society for the Future

Providing access to computer science (CS) education is a critical step to ensure our Nation remains competitive in the global economy and strengthens its overall cybersecurity. Educators and business leaders across the country are increasingly recognizing that CS is a "new basic" skill, necessary for economic opportunity and social mobility. CS is also an active and applied field of STEM learning that allows students to engage in hands-on, real-world interaction with key mathematics, science, and engineering principles. It gives students opportunities to be producers in the digital economy, not just consumers, and to be active participants and active citizens in our technology-driven world. The related computational thinking skills, relevant to many disciplines and careers, are increasingly included in education programs. Those include breaking a large problem into smaller ones, recognizing how new problems relate to ones that have already been solved, setting aside details of a problem that are less important, and identifying and refining the steps needed to reach a solution.

However, wide access to CS education is limited, and there are disparities even for those who do have access to these courses. For example, of the fewer than 10 percent of all high schools that offered any Advanced Placement® CS courses in 2015, only 22 percent of those who took the corresponding AP exam were girls, and only 13 percent were African-American or Latino.

Since 2008, NSF has led the "CS 10K" effort, funding researchers to develop rigorous and engaging curricula with the goal of preparing 10,000 teachers to teach computer science in 10,000 schools across the Nation. NSF is dedicated to broadening the participation of individuals in all fields of STEM, including CS. NSF has supported the research needed to establish best practices for engaging and retaining diverse student populations so that all students have the opportunity to see computer science as engaging, personally relevant and empowering. Through these efforts, NSF-funded projects are building an evidence-based foundation for K-12 CS education and an ecosystem of curricula, course materials, assessments, scalable models of professional development and online support networks and resources for teachers. In addition, The College Board, with funding from NSF, has launched a new Advanced Placement® (AP) computer science course called Computer Science Principles (CS Principles)[10] that is intended to explore the creative aspects of computing and increase the number and diversity of students entering the field. The first exam is scheduled to be administered in spring 2017, and hundreds of schools and colleges across the U.S. are already piloting the course. NSF is now sponsoring the development of an AP CS Principles course with an emphasis on cybersecurity.

NSF's investments in CS 10K since 2008 laid the groundwork for the Computer Science for All Initiative[11] announced in January 2016. As the lead Federal agency for building the research knowledge base for CS education, NSF has committed $120 million over the next five years to CS for All, in order to accelerate ongoing efforts to enable rigorous and engaging CS education in schools across the Nation. Those funds will support continued research and evaluation related to prototyping of instructional materials, scalable and sustainable professional development models, approaches to pre-service preparation for CS teachers, and teacher resources at the K-12 grade levels. NSF also will collaborate with the private sector to support high school CS teachers: as part of its million investments, NSF will pilot and expand professional development approaches in CS to additional schools across the U.S., with additional funding from industry that will enable teachers to attend these pilot programs. Infosys Foundation USA will be a founding member of this public-private collaboration with a $1 million philanthropic donation, and, as an initial participant, Tata Consultancy Services is providing additional support in the form of grants to

[10] https://advancesinap.collegeboard.org/stem/computer-science-principles
[11] https://www.whitehouse.gov/blog/2016/01/30/computer-science-all

teachers in 27 U.S cities. This collaboration will ultimately provide opportunities for as many as 2,000 middle and high school teachers to deepen their understanding of CS.

NSF invests heavily in the preparation of the STEM workforce for tomorrow. Since its founding, NSF has invested in advancing science and the people who would both conduct that science, and be part of the society that will use and appreciate science. Today we have a range of programs that are directly focused on the preparation of the broader STEM workforce, from the Graduate Research Fellowship Program (43 Nobel Laureates were recipients of this fellowship), to the Noyce Teacher Scholarship program, to the EHR Core Research strand on the STEM professional workforce.

Federal Agency Coordination for Cybersecurity Education and STEM Workforce Preparation

NSF continues to work closely with the National Initiative for Cybersecurity Education (NICE) [12] to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. The National Institute of Standards and Technology (NIST) is leading the overall NICE initiative in collaboration with other federal departments and agencies, including NSF, as well as state government, academia, and private industry to build on successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. One of the primary ways in which NSF is actively engaged with this initiative is through the NICE Interagency Coordinating Council (ICC). The NICE ICC convenes NICE federal government partners for consultation, communication, and coordination of policy initiatives and strategic directions for cybersecurity education. NSF further participates in NICE Education Groups which particularly focus on strategies and recommendations for filling the cybersecurity pipeline through primary, secondary, and post-secondary education.

NSF Director Dr. France Córdova co-chairs the National Science and Technology Council's (NSTC) Committee on STEM Education (CoSTEM), with Dr. Jo Handelsman of the Office of Science and Technology Policy (OSTP). The Federal Coordination in STEM Education Task Force (FC-STEM), which I co-chair with Donald James from NASA, is a subgroup of CoSTEM focused on implementation of CoSTEM's *STEM Education 5-Year Strategic Plan*[13]. Recently, an interagency working group was established on Computer Science for All under the purview of FC-STEM and in connection with the 5-Year Strategic Plan, to develop a strategic framework for government investment in computer science education. NSF co-leads that working group, in partnership with the U.S. Department of Education and OSTP.

Conclusions

Continued investment in fundamental research and development is necessary to improve the preparation of a diverse STEM workforce, ready for innovation and leadership in tomorrow's science and engineering. A critical component of that investment is in the area of preparation of cybersecurity professionals, in order to ensure that our Nation's cyber systems are secure and trustworthy, and that the next-generation science and engineering workforce is increasingly cyber-aware, prepared with the knowledge to keep our systems secure. And, the more general education of tomorrow's scientists and engineers, as well as the preparation of all to be STEM-literate, can include attention to fundamental topics in computer science to help raise general levels of awareness and practice for cyber-awareness. With ongoing support and leadership for cybersecurity research, research and new models in cybersecurity education, and development of the STEM workforce, in both the Executive and Legislative

[12] http://csrc.nist.gov/nice/index.htm

[13] https://www.whitehouse.gov/sites/default/files/microsites/ostp/stem_stratplan_2013.pdf

Branches, NSF and its partners contribute 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.

_____

For additional information please see the program solicitations of the CyberCorps®: Scholarship for Service program as well as the Advanced Technological Education program. Portions of this testimony were drawn from the written testimony of Jeremy Epstein, former lead program director for NSF's Secure and Trustworthy Cyberspace (SaTC) program, before the Senate Committee on Commerce, Science, and Transportation on September 3, 2015.