National Science Foundation Programs
Supporting Cybersecurity Education and
Workforce Development

Corby Hovis
Victor Piotrowski

Directorate for Education and Human Resources
National Science Foundation
Arlington, VA
Warning!

- All information provided here represents the opinions of individual Program Officers.

- The only **official** source for NSF policy is published materials.
Not Sufficient Funds
What we hope you take away:

- Understanding of NSF funding opportunities for cybersecurity education
- Can locate additional information about NSF programs and funded projects
- Practical advice on proposal preparation
- We will be available for individual conversations after this talk
NSF Structure

NSF Director

NSF Deputy Director

Biological Sciences

Social, Behavioral and Economic Sciences

Computer & Information Science & Engineering (CISE)

Education and Human Resources (EHR)

Mathematical and Physical Sciences (MPS)

Engineering

Geo Sciences
NSF Impact

With an annual budget of over $7.0 billion, NSF is the funding source for about 20 percent of all federally supported basic research and over 80 percent of CS research conducted by America's colleges and universities.
How We Work

- Program announcements (RFPs) outline programmatic goals in research/education
- Research/education community responds with proposals
- Experts from research/education community decide on the best ideas among the proposals (peer review)
- NSF program officers weigh expert reviewers’ views and agree (often) or disagree (sometimes)
- NSF makes grants
- Grantees do the work
- NSF monitors progress
Programs that *emphasize* workforce development

Programs that *contribute to* workforce development
Federal Cyber Service: Scholarship For Service (SFS, Cyber Corps®)
NSF Investments in Cybersecurity

In FY 2011:

- **Trustworthy Computing (TC)** program was funded at a level of $55 million and supports more than 500 active projects.
- **Scholarship for Service (SFS)** was funded at $15 million and supports 37 campuses offering scholarships. SFS also issues capacity building grants.

In FY2012, NSF created a cross-agency program, **Secure and Trustworthy Cyberspace (SaTC)**

- FY12 at $111M; FY13 request $112M
- SFS in FY12 request $25M; appropriation $45M
- SFS in FY13 request $25M, appropriation ???
SFS History

Page 308
SFS History

**Authority:** The SFS program was established initially as a result of Presidential Decision Directive 63 (May 22, 1998) which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems:

“...This program will fund up to 300 students per year in their pursuit of undergraduate or graduate degrees in the information security field. In return, the students will serve in the Federal IT workforce for a fixed period following graduation. The program will also have a meaningful summer work and internship element. An important part of the SFS program is the need to identify universities for participation in the program and assist in the development of information security faculty and laboratories at these universities...”
SFS History

Defending America’s Cyberspace

National Plan for Information Systems Protection
Version 1.0

An Invitation to a Dialogue

The White House
2000
SFS Mission and Structure

The Federal Cyber Service: Scholarship for Service (SFS) program seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society.

The SFS program is composed of two tracks:

- **The Scholarship Track** provides funding to colleges and universities to award scholarships to students.
- **The Capacity Building Track** providing funds to support curriculum, outreach, faculty, institutional, and/or partnership development.
SFS Program Management

- NSF operates grants program, selects and funds grantees, sets policy.
- DHS National Cyber Security Division partners with NSF to provide strategic support, co-fund activities, and facilitate Federal agencies’ involvement.
- OPM monitors student participants and manages placement process.
- Interagency Coordinating Committee (reps. from NSF, CIA, DoD, DHS, NSA, OPM) is the program's strategic advisory board.
SFS Scholarships

- **Scholarship Component:**
  - Funding: tuition, fees, and stipends ($20K/$25K/$30K per year)
  - Length: 2-3 year scholarship for final years of undergraduate or graduate (master’s or doctoral) education
  - Obligation: Summer internship, post-graduation service requirement (work in Federal agency equal to scholarship length)

- **Student Eligibility:**
  - U.S. Citizen
  - Enrolled in IA program, within 2-3 years of graduation
  - Eligible for Federal employment (must be able to acquire security clearance)
  - Awardee institutions set additional selection criteria

- **Institution Eligibility:**
  - National CAE/IAE designation or equivalent (DC3 Forensics, NSA Cyber Ops or alternative evidence)
  - Offer full-time program of study in IA field(s)
Federal Cyber Service: Scholarship For Service

Scholarship For Service (SFS) is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning. Additionally, participants receive stipends of up to $8,000 for undergraduate and $12,000 for graduate students. The scholarships are funded through grants awarded by the National Science Foundation (NSF).
SFS Participating Institutions

- States with at least one school participating
SFS Scholarships: Participating Colleges/Universities

- Air Force Institute of Technology
- Arizona State University*
- Auburn University
- Cal State Sacramento
- Cal State San Bernardino
- Carnegie Mellon University
- Dakota State University
- Florida State University
- George Washington University
- Georgia Tech
- Idaho State University
- Iowa State University
- James Madison University*
- Johns Hopkins University
- Mississippi State University
- Naval Postgraduate School
- New Mexico Inst. of Mining & Technology
- Norfolk State University*
- North Carolina A&T State University
- Northeastern University
- Pace University
- Penn State*
- Polytechnic University of New York
- Purdue University
- Stevens Institute of Technology
- Syracuse University
- University at Buffalo
- University of California, Irvine
- University of Idaho
- University of Illinois, Urbana Champaign
- University of North Carolina, Charlotte
- University of Nebraska, Omaha
- University of Pittsburgh
- University of Texas, Dallas
- University of Texas, San Antonio
- University of Tulsa
- University of Washington*

* New sites Fall 2011
SFS Statistics

- First graduates entered the Federal IA workforce in 2002
- Scholarship funds are distributed primarily to graduate students, with 77% of SFS students being enrolled in Master's or Ph.D. programs
- 1,547 SFS scholarship recipients, of these 343 in current academic programs and 1,204 have already graduated
- 60% under 25 years old
- Government placement rate >93%
- Capacity building grants to more than 90 institutions
SFS – Scholarship Track

- **FY07-10:** 28 awards totaling $43.7M

<table>
<thead>
<tr>
<th>Calendar Years</th>
<th>SFS Graduates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>9</td>
</tr>
<tr>
<td>2003</td>
<td>75</td>
</tr>
<tr>
<td>2004</td>
<td>152</td>
</tr>
<tr>
<td>2005</td>
<td>179</td>
</tr>
<tr>
<td>2006</td>
<td>172</td>
</tr>
<tr>
<td>2007</td>
<td>157</td>
</tr>
<tr>
<td>2008</td>
<td>121</td>
</tr>
<tr>
<td>2009</td>
<td>86</td>
</tr>
<tr>
<td>2010</td>
<td>116</td>
</tr>
<tr>
<td>Total</td>
<td>1067</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Students enrolled FY2007-10</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Tulsa</td>
<td>107</td>
</tr>
<tr>
<td>Carnegie Mellon University</td>
<td>75</td>
</tr>
<tr>
<td>Mississippi State</td>
<td>48</td>
</tr>
<tr>
<td>University of North Carolina</td>
<td>46</td>
</tr>
<tr>
<td>Naval Postgraduate School</td>
<td>44</td>
</tr>
<tr>
<td>Idaho State University</td>
<td>42</td>
</tr>
<tr>
<td>Syracuse University</td>
<td>35</td>
</tr>
<tr>
<td>New Mexico Tech</td>
<td>31</td>
</tr>
<tr>
<td>Stoney Brook University</td>
<td>31</td>
</tr>
<tr>
<td>Polytechnic University</td>
<td>30</td>
</tr>
<tr>
<td>AFIT</td>
<td>28</td>
</tr>
<tr>
<td>North Carolina A&amp;T</td>
<td>28</td>
</tr>
<tr>
<td>George Washington University</td>
<td>27</td>
</tr>
<tr>
<td>Iowa State University</td>
<td>26</td>
</tr>
<tr>
<td>Georgia Tech</td>
<td>22</td>
</tr>
<tr>
<td>Johns Hopkins University</td>
<td>22</td>
</tr>
</tbody>
</table>
Capacity Building - Faculty Expertise

- Professional development of faculty expertise
- In information assurance, cybersecurity or digital forensics
- Broad impact required
Capacity Building - Curriculum Guidelines

- Development, deployment, and evaluation of curriculum models
  - Information assurance
  - Cybersecurity
  - Digital forensics
- Leading to wide adoption nationally
Capacity Building - Pathways

- Development of pathways between two-year and four-year programs
- Development of pathways between four-year and graduate programs
- With extensive adoption
Capacity Building - Accelerated Programs

• Development of fast track bachelor's + master's degrees
• Development of accelerated degree or certificate programs for veterans, career changers, and non-traditional students
Capacity Building - Curriculum Integration

- Integration of security topics into computer science, IT, engineering or other programs
- Pervasive adoption
Outreach

- Promote interest at K-12 level
- Evaluation of the effectiveness of competitions, games, and other outreach and retention activities
Capacity Building - Increase Diversity

• Increase the diversity of the cybersecurity workforce.

• A focus on recruiting and retaining underrepresented minorities, women and/or veterans is strongly encouraged.
SFS in the News

• H.R.2096 - Cybersecurity Enhancement Act of 2011
• S. 773 Cybersecurity Act of 2010
• H.R.4061 - Cybersecurity Enhancement Act of 2010
• DEPARTMENTS OF COMMERCE AND JUSTICE, AND SCIENCE, AND RELATED AGENCIES APPROPRIATIONS BILL, FY 2012 and FY 2013
• Both Lieberman and McCain Senate Bills (2012)
• Federal CIO Councils IT Workforce Committee Initiative
• 2010 State of Cybersecurity from the Federal CISO’s Perspective – An (ISC)² Report
In your staffing plans, what percentage of your hires will come from:

- Scholarship for Services Program - 20.1%
- Internal - 29.8%
- Other agencies - 21.3%
- Contractor conversions - 30.2%
- Private Sector - 28.9%
SFS – Next Due Date

- Expected September/October 2012
Advanced Technological Education (ATE)

- Education (degree programs, not “training”) of technicians in high-tech fields (IT/cybersecurity, biotech, chemical tech, engineering tech, manufacturing, etc.)
- Goal: High-quality technician workforce
- Community colleges have leadership role
- Partnerships involving CCs, secondary schools, 4-year colleges and universities, business/industry, and government
ATE Grants for Cybersecurity Education

- 4 ATE Centers (~$750k – $1M per year)
- ~12 active projects (~$150k – $400k per year)

Activities:
- Development of materials, labs, courses, curricula, programs (degrees and certificates)
- Professional development for faculty
- Transfer agreements with 4-year colleges/universities
- Internships for students
- Mentoring of other CCs to develop new programs
- K-12 curricula and outreach (students, teachers, counselors, parents)
- Student competitions (Cyber Defense, Digital Forensics Challenge)
- Cybersecurity awareness in communities
ATE Centers for Cybersecurity Education

- **Ctr. for Systems Security & Info. Assurance (CSSIA)**
  - Moraine Valley CC (IL) and partners
  - [www.cssia.org](http://www.cssia.org)

- **Cyber Security Education Consortium (CSEC)**
  - University of Tulsa, Oklahoma CareerTech, and partners
  - [www.cseconline.org](http://www.cseconline.org)

- **CyberWatch**
  - Prince George’s CC (MD) and partners
  - [www.cyberwatchcenter.org](http://www.cyberwatchcenter.org)

- **CyberWatch West**
  - Mt. San Antonio College (CA) and partners
  - [cyberwatchwest.org](http://cyberwatchwest.org)
One Outcome…

CAE2Y

Center of Academic Excellence – 2 Year
Some Programs That *Contribute* to Cybersecurity Workforce Development
Transforming Undergraduate Education in Science, Technology, Engineering, and Mathematics (TUES)
TUES (formerly CCLI) Program

- Bring advances in STEM disciplinary knowledge into curriculum
- Create or adapt learning materials and teaching strategies
- Develop faculty expertise
- Promote widespread implementation of educational innovations
- Prepare *future* K-12 teachers
- Enhance the understanding of how students learn STEM topics (research in undergraduate STEM education)
- Enhance the understanding how faculty adopt instructional approaches
- Build capacity for assessment and evaluation
TUES Project Types

- **Type 1 Projects** *(up to $200K / 2-3 years or up to $250K with 2-year/4-year school collaboration)*
  
  Involve exploratory, initial investigation or adaptation in one of the component areas

- **Type 2 Projects** *(up to $600K / 2-4 years)*
  
  Build on smaller scale but proven innovations, refine and test innovations on diverse users, impact multiple components

- **Type 3 Projects** *(negotiable, up to $5M / 5 years)*
  
  Several diverse institutions, evaluation or assessment activities, combine proven results and mature innovations from several component areas
TUES Projects with a Cybersecurity Focus: Examples

- “SEED: Developing Hands-On Labs for Computer Security Education” (Award No. 0618680)
  Syracuse University
  Kevin Du, PI

- “Building Security In: Injecting Security Throughout the Undergraduate Computing Curriculum” (Award No. 0817267)
  Towson University
  Blair Taylor, PI
TUES – Next Due Dates

- Type 2, 3 – January 14, 2013
- Type 1 – May 2013
Research Experiences for Undergraduates (REU) Sites

- Support ~ 6-12 students per year to engage in thematically related research projects
- Grant $$ are primarily for student support
- Usually run for 8-10 weeks in summer
- Most students must come from outside the host institution
- Strong emphasis on involving students from institutions where research opportunities are limited (including community colleges)
- Encourage recruitment of underrepresented minorities, women, freshman/sophomore-level students

Key foci:
- Leading-edge research
- Student experience: cohort, authentic research, “culture” of discipline
- Good mentoring
- Writing/communication/presentation skills, career pathways, grad school
Purdue University (CERIAS) REU Site: “Multidisciplinary Information Assurance and Security”
NSF Award No. 1062970

PIs: Melissa Dark, Gene Spafford

Areas of student research:
• Assurable software and architectures
• Enclave and network security
• Authentication and privacy
• Risk management
• Policies
• Trusted social and human interactions
University of Connecticut
REU Site: “Trustable Computing Systems Security Research and Education”
NSF Award No. 1062962

PI: John Chandy

Areas of student research:
• Hardware support for computer security
• Hardware Trojan detection
• IC authentication
University of Maryland, College Park
REU Site: “Undergraduates Engaged in Cyber Security Research”
NSF Award No. 1062820

PI: Michel Cukier

Areas of student research:
• Privacy protection for social media
• Privacy and security issues of networked office devices
• Detection of simulated human users with auditory CAPTCHAs
• Security wireless communications in the physical layer
• Software test automation tools for event-driven software
• Security and surveillance using mobile wireless sensor networks
• Security analysis of Ruby-on-Rails Web applications
• Hardware Trojan horse—insertion, protection, prevention
Dakota State University
REU Site: “Information Assurance and Security”
NSF Award No. 1004843

PIs: Dianxiang Xu, Joshua Pauli

Areas of student research:
• Secure design and verification
• Security testing
• Forensics of security incidents
• IAS applied to banking and finance
University of Rhode Island
REU Site: “Digital Forensics Research in Rhode Island”
NSF Award No. 1004409

PI: Victor Fay-Wolfe

Areas of student research:
• Human image detection
• Proactive image searching
• Automatic search string generation for law enforcement
• Systems techniques for network forensics
University of Nebraska at Omaha
REU Site: “Site for Extensive and Collaborative Undergraduate Research Experience (SECURE)”
NSF Award No. 1062995

PIs: Jong-Hoon Youn, Qiuming Zhu

Areas of student research:
• Wireless communications and sensor networks
• Multimedia data transmission
• Medical informatics (development of HIPAA-compliant database system for real-time patient monitoring)
• Network security (techniques for intrusion detection in wireless networks)
• Antenna array design for wireless sensor networks
Research Experiences for Undergraduates (REU) Sites

- Grants to institutions typically $70k–$120k per year for 3 years
- Proposal deadline in late August or early September annually
Research Centers with Education/REU Components
Team for Research in Ubiquitous Secure Technology (TRUST)

- NSF Science and Technology Center in 8th year of funding; >$28M to date
- Partners: UC Berkeley, Carnegie Mellon, Cornell, San Jose State, Stanford, Vanderbilt, business/industry
- Research and education on cybersecurity issues related to health care, national infrastructure, law, and other areas affecting general public
- TRUST Online Academy: huge array of teaching and learning resources and courseware
- TRUST REU Site: summer research experience for 10-15 undergraduates per year
- TRUST Women’s Institute in Summer Enrichment (WISE): summer residential program for grad students, postdocs, and faculty interested in ubiquitous secure technology
Trustworthy Computing/CyberTrust Program
→ Secure and Trustworthy Cyberspace (SaTC)

- Trustworthy Infrastructure for the Power Grid
  - University of Illinois and partners

- Center for Internet Epidemiology and Defenses
  - UC San Diego, UC Berkeley, and partners

- Situational Awareness for Everyone (SAFE)
  - Carnegie Mellon, UNC Chapel Hill, and partners

- ACCURATE: A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections
  - Johns Hopkins University and partners
Industry/University Cooperative Research Centers (I/UCRC) Program

- Center for Identification Technology Research (CITeR)
  - West Virginia University, University of Arizona, Clarkson University
  - Biometric systems and credibility assessment systems

- Security and Software Engineering Research Center (S^2ERC)
  - Ball State, Iowa State, Virginia Tech, 10 other universities, 23 industry and government partners
  - Research tailored to needs of business/industry, “enabling real-world-companies to meet real-world goals”
Practical Advice
# Top Seven Weaknesses in Proposals

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insufficient detail and unclear plans</td>
</tr>
<tr>
<td>2</td>
<td>Evaluation plan is incomplete</td>
</tr>
<tr>
<td>3</td>
<td>Unrealistic activities &amp; not related to outcomes</td>
</tr>
<tr>
<td>4</td>
<td>Limited dissemination plan</td>
</tr>
<tr>
<td>5</td>
<td>Limited potential for involving underrepresented groups</td>
</tr>
<tr>
<td>6</td>
<td>Does not build on prior work</td>
</tr>
<tr>
<td>7</td>
<td>Not innovative or novel</td>
</tr>
</tbody>
</table>
Some Tips for Planning a Proposal

- Read the solicitation
Some Tips for Planning a Proposal

- Read the solicitation
- Read the solicitation
Some Tips for Planning a Proposal

- Read the solicitation
- Read the solicitation
- Read the solicitation
- Read the solicitation
Some Tips for Planning a Proposal

- Read the solicitation
- Read the solicitation
- Read the solicitation
- Offer to review proposals
- *A Guide for Proposal Writing* (NSF 04-016)
- Discuss your idea with an NSF Program Director
- Get copies of previously funded proposals
  - Directly from the PI
  - From NSF (but takes much longer)
- Search previous NSF awards
Some Tips for Planning a Proposal

- Find a partner, colleague, or collaborator to broaden reach of project
- Get friends to “pre-review” your proposal
- Make sure your evaluation and dissemination plans are strong
MyNSF
(Custom News Service)

http://www.nsf.gov/mynsf/

- Receive notifications about new content posted on the NSF website (program announcements, policy updates, news releases, etc.)

- Notification via email or RSS
More Info…

http://www.nsf.gov

Search NSF awards:
http://www.nsf.gov/awardsearch/