Whither SFS?:
Cybersecurity SFS Workforce Development
Workshop Report

Lance J. Hoffman
Costis Toregas

July 22, 2014
Report GW-CSPRI-2014-04

Support for this work was provided by the National Science Foundation's CyberCorps®: Scholarship for Service (SFS) program under Award No. 1027425. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.
Whither SFS?:
Cybersecurity SFS Workforce Development Workshop
Summary Report

Lance J. Hoffman
Costis Toregas

Abstract

This report describes a workshop that was centered on the Scholarship for Service (SFS) program and its various components and included an in-depth discussion about how to improve the program and maximize its efficiency in generating a quality cybersecurity workforce. The purpose of the workshop was to bring together program experts and/or professionals who have extensive experience with the SFS program and workforce issues. Multiple topics were discussed, including recruiting, course content, transitioning SFS students into the federal workforce, and enhancing understanding and participation in the program within 4-year institutions and community colleges.

Participants examined a variety of current and foreseeable program issues and discussed program changes on which there appeared to be some level of agreement, including technical competency assessment, better coordination and resource sharing, feedback from employer agencies, non-federal government placements, community college articulation, flexibility in duration of scholarship, early clearance processing, expanded eligibility criteria, and use of a common application.
**Whither SFS?:**

Cybersecurity SFS Workforce Development Workshop Summary Report

Table of Contents

1 Introduction ........................................................................................................................................ 1
2 Workshop Process ............................................................................................................................ 1
3 Repeated Themes ............................................................................................................................ 3
4 Possible Actions in Order of Priority ................................................................................................. 4
   4.1 Technical competency assessment .......................................................................................... 5
   4.2 Coordination and resource sharing ......................................................................................... 5
   4.3 Agency employer feedback ..................................................................................................... 6
   4.4 Non-federal government placements ....................................................................................... 6
   4.5 Community College Articulation (first year at a Community College) ............................... 7
   4.6 More flexibility in duration ...................................................................................................... 7
   4.7 Early clearance processing ....................................................................................................... 8
   4.8 Expanded eligibility criteria ...................................................................................................... 8
   4.9 Common Application ................................................................................................................ 8
   4.10 Final thoughts on possible actions .......................................................................................... 9

5 Other Broad Issues .......................................................................................................................... 9
   5.1 Pay scale .................................................................................................................................. 9
   5.2 Institutional impact of SFS ........................................................................................................ 9
   5.3 Scope of workforce .................................................................................................................... 9
   5.4 CAE designation ....................................................................................................................... 10

6 References ....................................................................................................................................... 12

7 Acknowledgements ........................................................................................................................ 13

8 Appendices ..................................................................................................................................... 14
   8.1 Additional Issues ...................................................................................................................... 14
   8.2 Participant Biographical Sketches ........................................................................................... 17
   8.3 Working Group Composition ................................................................................................... 24
   8.4 Agenda ...................................................................................................................................... 25
   8.5 Presentation of Valerie Barr, NSF ............................................................................................ 26
1 Introduction
This report is a discussion of a workshop that explored mechanisms for recruiting the best candidates for Scholarship for Service (SFS) programs, enhancing the SFS potential for articulation and content across all participating educational institutions (K-12 as well as community colleges and 4-year institutions), and linking SFS graduates and the marketplace. In short, the workshop addressed current and potential issues related to the Pipeline, the System, and Placement. This report assumes that the reader is familiar with the CyberCorps Scholarship for Service (SFS) program (NSF 2014).

2 Workshop Process
The workshop took place February 5-7, 2014 in Orlando, Florida. Participants were chosen to represent a wide cross-section of informed individuals from institutions who represented various intersects on that framework template. Invited participants provided insights from two-year community colleges, four-year universities (both SFS and non-SFS), NSF program directors, the U. S. Office of Personnel Management (OPM), accreditations/certification institutions, and the private sector.

Links to read-ahead material were sent to participants about three weeks before the workshop so that everyone had common knowledge as a starting point. Workshop attendees were asked to think about their strongly felt beliefs, and place them as four bullet points at appropriate intersects in a framework (Figure 1) of institutions and mechanisms.
The workshop started with plenary discussions that addressed current issues in the SFS program, drawing on existing literature and participant experience. Then the participants were broken up into three groups to focus on each of the three topics above (Pipeline, System, and Placement). After reports of initial findings and interactions and further discussions by phone with invitees who could not attend because of a major winter storm in the Eastern United States that made travel difficult during the workshop, the subgroups reconvened. They finalized their initial conclusions and developed a short list of actions, strategies and projects for the National Science Foundation to consider for immediate as well as longer term actions.

On the first evening of the workshop, the principal investigators shared with the participants the preliminary results from the bullet points and other observations that were sent in prior to the workshop.

---

**Figure 1. Organizational Template Sent to Participants**

<table>
<thead>
<tr>
<th>FRAMEWORK FOR SFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PJ pipeline into SFS - how do we get the best and brightest candidates?</td>
</tr>
<tr>
<td>SFS operations - how do we leverage the collective wisdom?</td>
</tr>
<tr>
<td>Placement - how can we make placement of graduates of various institutions fit the cybersecurity jobs available and what can we do to facilitate this process?</td>
</tr>
<tr>
<td>2-year community colleges</td>
</tr>
<tr>
<td>4-year traditional undergraduate institutions</td>
</tr>
<tr>
<td>Master’s degree granting programs</td>
</tr>
<tr>
<td>Doctoral degree granting programs</td>
</tr>
<tr>
<td>Certificate programs from traditional universities</td>
</tr>
<tr>
<td>Certificate and other programs from entities not traditionally considered to be in the “education” business</td>
</tr>
</tbody>
</table>

Whither SFS?: Cybersecurity SFS Workforce Development Workshop Report
The next day, Dr. Valerie Barr of the National Science Foundation (NSF), the sponsor of the workshop, gave introductory remarks (see Section 8.5 for a copy of her presentation) and each participant had the opportunity to comment on specific points they thought were important for the group to address. After a synthesis of the previously sent-in bullet points was presented, the participants split into three groups – on pipeline, system, and placement – and moved to separate rooms to develop more nuanced observations about each of these respectively.

Later in the day, these working groups (see Section 8.3) presented preliminary reports and listened to feedback from the entire group of participants, and then went back to incorporate this feedback into their observations before adjourning for the day.

During the evening, comments were elicited from participants who were participating remotely due to a snowstorm that prevented safe travel to the event for some invitees. Via conference call, these comments were gathered and then presented to the entire group the morning of the next (and final) day. Then, the working groups had the opportunity to incorporate those new comments and any additional insights they had since their meeting the previous day into a set of actions for NSF to consider for the SFS program. The working group leaders presented their initial observations. After these presentations, reactions from the whole group of participants triggered discussion of some issues that transcended the boundaries of the working groups. These bigger issues were noted and discussed, and different small groups were sent off to tackle them in the afternoon. These groups came back with initial observations that were then written up. A vote of the entire group was taken to prioritize these observations.

All of this material was captured in a draft report that was circulated to the participants on May 5, 2014. Comments from participants were elicited and requested by May 18, 2014. The received comments were then considered; final action on them ranged from “No action” to a change in the description of aspects of the topic covered. After these actions were taken, a final draft was circulated and an opportunity was provided for any participant who wished to write a brief additional statement for inclusion in the report. None chose to do so. The authors have endeavored to report accurately about this event and the final responsibility for this report remains with them.

The working groups came up with a number of observations. After further discussion by the entire group, some were discarded but many were kept and are reported here as either “Repeated Themes” that can be acted on now or “Other Broad Issues” that should be examined further. As described above, workshop participants then voted to rank order the importance of many observations and these observations are then presented in that order in Section 4.

3 Repeated Themes

After these initial ideas from the various working groups were examined and compared with each other, a few common themes emerged:
1. Recruiting of students is the responsibility of the institutional awardees and several have had difficulty attracting an appropriate number of qualified students for the program. Additional help using outside expertise would be appropriate here.

2. Marketing the program to agencies, making them aware of what its graduates have to offer, needs significant additional work. Timely placement upon graduation is also made more difficult by the uncertainty by many agencies about when they will have positions available. OPM has not allocated the resources to adequately do this and additional resources beyond those made available through OPM should be considered.

3. Sharing resources among SFS institutions when appropriate and on an opt-in basis would make the program more effective and efficient. [This echoes some of the recommendations in (NSF 2014a).]

4. Institution outputs should be matched to employer needs. Institutions are different and have different strengths. Community colleges, four year colleges, master’s degree-granting institutions, doctorate-granting institutions, all offer terminal degrees. In addition, they, along with commercial or nonprofit organizations that are not traditionally thought of as academic institutions, offer certificate programs in cybersecurity. All have a place in fulfilling government workforce needs in cybersecurity.

5. Potential employers of SFS graduates are also diverse with different needs. Consider, for example, all these illustrative organizations that are eligible to hire SFS graduates: Department of Homeland Security, Executive Office of the President, Iowa State University, Montgomery County (Maryland), State of California Franchise Tax Board, MITRE Corporation. They all could use SFS graduates in very different capacities. Other potential employers that contribute to the critical infrastructure but are not eligible (e.g., Raytheon, etc.) also have needs, some of which are similar and some different from the list of employers above.

4 Possible Actions in Order of Priority

Table 1 summarizes the observations and actions that in the opinion of the workshop attendees were the most worthy of further discussion and action, in order of most popular to having some support. Those identified but garnering little or no support for further discussion are noted in an appendix in Section 8, Additional Issues.

<table>
<thead>
<tr>
<th>Place</th>
<th>Topic</th>
<th>Number of votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Technical competency assessment</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>Coordination and resource sharing</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Agency employer feedback</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Non-federal government placements</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Community college articulation</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>More flexibility in duration</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Early clearance processing</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Expanded eligibility criteria</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Common application</td>
<td>2</td>
</tr>
</tbody>
</table>
4.1 Technical competency assessment

Many 4-year institutions leave the technical competencies for junior year, or teach them on a limited basis. The 2-year institutions vary in their coverage of these competencies. Assessment of these competencies in technical areas such as forensics, penetration testing, network defense, etc., would result in the standardization that some felt would greatly improve both the 2-year and the 4-year programs. Others did not see enough benefits coming from standardization at this time. In any case, the entity to be in charge would need to be resolved before this could happen, if it happens.

NSF could consider a pilot program for competency measurement with several CAE2Y institutions geographically positioned to fully develop this program. For example, during the first two years, students (at community colleges) might be expected to prove their competencies in three technical areas (out of a possible seven or eight) such as computer forensics, system and network defense, penetration testing, etc.

4.2 Coordination and resource sharing

In 2001, the Scholarship for Service program made a total of 16 awards to 12 universities, 7 of which were scholarship awards with the remaining 9 awards being capacity building. Since 2001, close to 250 capacity building grant awards and approximately 100 scholarship awards have been issued, and a cursory count shows these 350 awards have gone to about 270 universities, colleges, and institutes.

The community has clearly grown in size. It has also grown in diversity, expertise, and experience. The participating institutions have developed practices, projects, materials, and artifacts that are not being fully leveraged. The assets at these various institutions are different and include, for example: 1) effective recruiting practices and outreach programs, 2) innovative educational approaches, 3) valid and reliable methods for assessing student learning and competencies, and 4) efficacious placement practices. Currently, exchange of best practices is ad hoc and fairly inefficient. For example, if a PI or prospective PI at an institution wants to find out about effective methods for assessing student learning outcomes from Capture the Flag competitions in the SFS community, she/he will have a difficult time conducting an efficient and effective search. Brute force searches on the NSF grant web site are neither efficient nor effective.

While the SFS community has examples of excellence at the various participating institutions and in recent years has instituted institution development events (“boot camps”) for new PIs and others from institutions receiving SFS scholarship grants for the first time, it still lacks ongoing mechanisms to advance, distribute, and leverage this excellence so that the information is available in real time to a PI that is currently faced with a challenge that others may have addressed already. Several ad-hoc alliances have been encouraged by NSF informally, but the
individual universities/colleges are not individually incentivized to organize this type of boundary spanning resource sharing.

At this juncture in the growth of the SFS community, examples of the evolving needs of community and its constituent institutions could include: repositories for sharing of resources, improved competency assessment, and/or information about workforce demands (job roles and their projected growth). Another potentially useful item might be a mapping of the outcomes of the various SFS programs to the NICE framework (NICE 2014) and then an assessment of how the SFS program as a whole is doing to satisfy the projected needs described in NICE.

A potential action/solution would be for NSF to fund an organization that would be tasked to be responsible for coordination and leveraging of existing assets, as well as carrying out some of the projects that are needed, but not currently incentivized. The structure and governance of such an organization was not further examined, but a general consensus was that creating such an organization, at least as a pilot program, was worthwhile. The organization could carry out some actions on behalf of a grantee institution, and that the use of this organization could be voluntary and left up to a decision by the institution’s PI. Sections 4.3, 4.4, and 4.9 below describe activities that could be facilitated by such a group.

4.3 Agency employer feedback

As the SFS program has grown, so has the placement of students into internships and jobs. While NSF review panels assess the performance of grant applicants, they do not usually have the benefit of using any type of standardized protocol or bank of assessment items for SFS schools to gather feedback from internship and hiring supervisors on the effectiveness of their graduates. Using employer data to inform program improvements is a long standing practice in academia. Accrediting bodies customarily require such evaluation. University programs have a long-standing tradition of using industrial advisory boards to offer feedback on the program content, and on the preparedness of graduates. Some fields also utilize a licensure exam to verify the acquisition of a body of knowledge.

The SFS program is reaching a point of maturity that this type of program assessment should be pursued. A potential action/solution would be to establish requirements and mechanisms for getting agency feedback on interns and permanent hires, so that information can better inform program improvement. This could be an activity undertaken by the coordinating body mentioned in Section 4.2.

4.4 Non-federal government placements

Opportunities for students to take internships or jobs in local, state and tribal governments are growing. And while many federal jobs are in the greater Washington DC area, SFS students also have opportunities to work for the federal government at sites across the United States. (For example, students interested in SPAWAR could be placed in San Diego, CA, Charleston, SC, Norfolk, VA, or New Orleans, LA). These locales could be very appealing to a wide variety of SFS students, and especially to students from these regions of the country. Furthermore, hiring managers at these locales should know about the SFS schools in their region.
While the labor market for cybersecurity is national, it is regional as well. Currently the job fair is for federal agencies alone, and does not appear to have an intentional focus on connecting regional supply and demand. A potential solution/action would be to improve mechanisms to place students in local, state and, tribal governments. This could be done by cooperation with associations like the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Counties (NACo), and the National Association of State Chief Information Officers. This could also be an activity undertaken by the coordinating body mentioned in Section 4.2.

4.5 Community College Articulation (first year at a Community College)

A previous report on SFS workforce development (Hoffman 2012) argued for a broader and more holistic approach to cybersecurity education. It stated, “…a well-considered cybersecurity workforce development strategy must be conceptualized holistically.” Inclusion of 2-year institutions into the SFS program is in line with these statements. Clearly, the expansion of the SFS program to include participation starting in the sophomore year would require input from all stakeholders with careful attention to criteria and expected outcomes. It is not expected that every 4-year institution would want to be a part of this program. Nor would all community colleges be eligible for it. The 2-year institutional participation could, for example, be limited to CAE2Y institutions. This would ensure a degree of standardization due to the required mapping to the same KU’s, and criteria that are similar to those for other CAEs.

Community college students typically go directly into the workforce or transfer to a baccalaureate granting institution. Important outcomes of such an expansion could be: more diverse cybersecurity workforce; stronger 2-year degree programs in the participating community colleges, thus leading to a better educated and more qualified workforce (many community college students go directly into the workforce, rather than transfer); stronger faculty developed from the greater interaction of faculty in the two institutions, and better opportunities for professional development) which would positively impact all students; and greater opportunity for external partnerships for both 2-year and 4-year institutions.

A program on a limited basis with 3-4 different community colleges and 4-year SFS institutions could be piloted to provide the basis for the permanent program planning and development.

4.6 More flexibility in duration

Building a greater degree of flexibility into the SFS program might increase the number of scholarship applications each year for all participating schools and strengthen the longevity of the program. Flexibility in duration would allow students to spread the SFS scholarship over more years to enable them to incorporate work outside of the academic institution.

More flexibility in duration would also help promote the visibility of the program. For example, if there were more flexibility in duration, it may be more appealing to the younger students entering the university. If the program changed and could fund three years of study (already possible for students studying at the doctoral level or in five-year BS/MS programs), a university could begin promoting this to individuals of freshman class standing. It could also help general recruitment for the university. Interest level could be higher in the program in a larger part of the student population because more people would be eligible to receive it. Such an approach might
give the program a level of customization that would allow for smoother transitions from undergraduate to graduate study and easier integration with cooperative work-study programs.

4.7 Early clearance processing

The suggestion was made that the clearance process start early at intake (and early intervention be taken if problems arise with an individual’s ability to get a clearance). This would not supplant an agency clearance but rather give a baseline or a picture of suitability for SFS. Currently, no checks are done on applicants submitted by institutions; background investigations do not even begin until the student has received an offer from a hiring agency, typically almost a year after they have been accepted into the SFS program. The program should look into the possibility of doing at least a National Agency Check with Inquiries (Bennett 2013) on students prior to their acceptance into the program.

4.8 Expanded eligibility criteria

Expansion of the eligibility criteria to the SFS program beyond the 3.0 GPA to examine a broader, more inclusive view of the student (include student portfolios, competitions, involvement in independent projects, etc.) was supported by several participants. Such an expansion would act as a supportive mechanism for important activities outside mainstream academic class participation and enrich the candidates with important skills before entering the SFS program.

4.9 Common Application

Getting the word out to talented prospective students about the SFS program is not easy. Typically, SFS program administration sits within various colleges, departments, and programs at participating universities. Individual programs at the respective universities often approach recruiting in a manner that conforms to local recruiting practices that may or may not best feature the SFS program. Many students don’t realize that there are other participating universities who together are the production engine for the CyberCorps. Indeed, several SFS PIs can tell stories about savvy applicants who shopped different SFS institutions and received multiple offers before picking the university that they would attend.

A potential solution/action would be to implement a common application, possibly one where individual SFS participating institutions can choose to use portions of the common application (including required portions with common data elements) and add supplemental information to the application that relates to their local program. Reports from the Common Application, a non-profit membership organization that today provides a common, standardized first-year application at over 500 colleges and universities, indicate that institutions see application increases between 20-25% when they move from an institutional application to the common application. In addition, at least one school that has instituted its version of the all-electronic Common Application from the same vendor (Hobson’s) reports much-improved clarity and much less confusion among staff that previously had to manage the paper applications and supporting documents. (Hoffman 2010). Some workshop attendees felt that the SFS program should develop national recruiting for the program and its constituent schools. They thought that the recruiters should be trained and the faculty (PIs) should also be trained in recruitment and
retention techniques. The coordinating body mentioned in Section 4.2 might provide help to participating SFS schools in standardization of information elicited and to scholarship applicants in awareness of opportunities at various institutions.

4.10 Final thoughts on possible actions

Before making changes, it is important to keep in mind that the scope of the cybersecurity workforce should be addressed fully and holistically through the SFS programs. Change for the sake of change is usually not a good use of resources. However, if there is a perceived shortcoming to the current SFS model, then some of these may be worth considering. If there are established metrics for the SFS program, for example, a target number of students at each matriculation level or further granularity by discipline, ethnicity, gender, that would inform which of the possible actions might be worthwhile.

5 Other Broad Issues

A few other issues surfaced in these initial discussions. These broader issues may go beyond just the SFS program, so they were captured and are presented separately here.

5.1 Pay scale

Certain agencies have been better than others at using the GS scale to attract talent, and salaries are an issue (Lawrence 2014). New agencies at job fairs have a steep learning curve, and as they learn about the SFS program and return for a second and third year, they refine their approaches. Organizing training and information sharing mechanisms for the employers (and not only the educational institutions) is a direction that the SFS program may wish to explore in subsequent years.

5.2 Institutional impact of SFS

While the primary purpose of the SFS program, based on the enabling legislation, is to build a larger and stronger cyber security workforce for the federal government, SFS has had a much broader impact than is formally recognized. Institutions that receive an SFS grant are often changed by receiving the funding, and expand and grow their courses, programs, activities, and presence in cyber security. In turn, these institutions advance their education to a much broader set of students, many of whom go to work for the government, thus, supporting the mission of the SFS program to improve the cybersecurity workforce. These institutional changes have not been adequately chronicled and should be captured in order to document a more complete picture of SFS program impact.

5.3 Scope of workforce

Presently, the number of hired SFS graduates varies across federal agencies. In this context, there are questions including:

- What is the cyber security workforce need of government agencies on the federal, state, local, and tribal level?
- What is the appropriate size of the SFS program to meet this need?
- Should SFS cover the need of all government agencies?
- Do all of these agencies know about the SFS program?
- If not, what can be done to change this? Should graduates of SFS programs be better distributed across all agencies, and if so, how?

5.4 CAE designation

The Centers for Academic Excellence in Information Assurance Education (CAE/IAE) designation is sponsored jointly by the National Security Agency and the Department of Homeland Security. The CAE program has grown from the original seven centers in five states in 1999 to the current total of 181 CAE institutions in 43 states and the District of Columbia. There is one in each state except Maine, Kentucky, Wisconsin, North Dakota, Montana, Wyoming, and Oregon (NSA/DHS 2014). While the CAE program has contributed significantly to the growth of the cybersecurity workforce over the last 14 years, there have also been a number of concerns raised about the program, such as extensive paperwork involved in the CNSS mapping along with the dissatisfaction with the CNSS standards and the lack of funding support for the centers (Bishop 2009). In recent years, much has changed about the program and new types of and requirements for CAEs have been created.

During the workshop, there was a limited conversation on the CAE program in general. However, there are clearly divergent opinions about the value of CAE program and its overlap with the SFS program. 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 may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees.” (OPM, 2014) The SFS program provides funding support and produces significant number of cybersecurity professionals for the federal and state government. The CAE program designates institutions that produce cybersecurity professionals on different levels with degrees ranging from AA to Ph.D., and potentially could address the growing need for cybersecurity faculty. In addition, CAE, and especially CAE-R, institutions are in a position to assist with important research questions.

While some think that the CAE requirements are important in specifying minimum requirements for SFS grants, others feel that these are useful guidelines but not an appropriate requirement. For example, institutions like MIT, Stanford, and UC-Berkeley are all producing quality graduates in cybersecurity while none of them have opted to date to apply for any CAE designation that is awarded by DHS and NSA. Indeed, the actual SFS solicitation requires only that an institution “provide clearly documented evidence of a strong existing academic program in cybersecurity. Such evidence can include Center of Academic Excellence in Information Assurance Education (CAEI/AE, or in Research, CAE-R) designation by the National Security Agency and the Department of Homeland Security; a specialized designation by a nationally recognized organization (for example, in forensics or cyber operations); or equivalent evidence documenting a strong program in cybersecurity.” (NSF 2014)

The CAE program offers many positive aspects, especially the CAE2Y and the CAE-R designations. The CAE2Y designation ensures a high degree of standardization and provides a measure of quality needed for the articulated CAE2Y SFS program to succeed. If SFS is to
focus on only the technical portion of the cybersecurity workforce, then tying SFS and CAE programs together may be justified. If not, then tying the programs together could be detrimental to producing students across the broad spectrum of cybersecurity career fields. It may be appropriate to also approach non-CAE institutions that are already producing quality cybersecurity graduates to examine whether a perceived CAE requirement or something else has deterred them from participating to date in the SFS program and what would motivate them to do so.
6 References

(Bennett 2013) Bennett, J., “What is a National Agency Check with Inquiries?”,


http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.7854&rep=rep1&type=pdf


http://www.nap.edu/catalog.php?record_id=18446{must login as guest for free download}

(NSA/DHS 2013) Information Assurance/Cyber Defense (IA/CD)


7 Acknowledgements

This event could not have taken place without the support of Victor Piotrowski, Valerie Barr, and Paul Tymann, Program Directors at National Science Foundation. We also wish to acknowledge the hard work of Katelyn Anders, Coordinator for the Cyber Security Policy and Research Institute (CSPRI) at the George Washington University.
8 Appendices

8.1 Additional Issues

A. More recruitment at community colleges and competitions

Some attendees felt that further emphasis should be placed on recruiting, in more efforts to include students from community colleges and underrepresented groups, and more strategic leveraging of existing events such as the National Collegiate Cyber Defense Competition (NCCDC 2014) and Cyber Patriot competitions (CyberPatriot 2014) to attract committed students into the program.

Some felt that recruiting is severely hindered without a central application process. It was noted that today, no entity has an incentive to do that. This is discussed in Section 4.9. One relevant question here is: What is the capacity for programs to increase output assuming there is more student interest? For example, if we doubled the amount of scholarship funding available, could we increase the number of graduates significantly, and would they all be placeable and placed into government positions?

B. Middle and high school outreach

Some felt that cybersecurity education should start at the middle school and high school levels to inform students what this profession is and why they should consider pursuing it, and that SFS institutions should have outreach programs to middle and high schools. These could include a variety of approaches – for example, having SFS students coach middle school children and or high school students for competitions, or to bring middle school teachers to summer workshops and institutes at SFS institutions. Others felt that this is not an SFS role, but the role of the National Initiative for Cybersecurity Education (NICE 2014) and others. This reinforces the fact that general awareness has traditionally not been a focus of the SFS program; it currently has neither the mandate nor funding to focus more resources on K-12 education and awareness.

C. “Try before you buy” for students

Some felt that the SFS program should develop ways for students to have introductory experiences in cyber security and government service (“try before you buy”) before being asked to commit to accepting the scholarship, and the subsequent service, in a manner similar to that used by the Reserve Officers Training Corps (ROTC) model. They thought that additional administrative costs should be allowed for schools that experimented with providing this introduction. Another idea, sharing material across universities to provide an introductory experience, was articulated but not presented separately.

D. Facilitate PI-Agency contacts

Some felt that OPM or some other entity could facilitate contacts between PIs and federal,
state, local, and tribal hiring governmental bodies. A regional job fair was one mechanism suggested, and here the coordinating body of Section 4.2 was viewed as a more effective mechanism than the Office of Personnel Management (OPM), and one that could work more closely with specific agencies such as DHS that have elements in a number of communities around the nation.

E. Develop metrics for the program

The overall program needs metrics and a mechanism for collecting a variety of data, such as applications to SFS, acceptance rates of SFS, completion rates of SFS program of study, number of job offers, number of internships and full-time jobs, performance on the internship/job, etc., that could be used by various stakeholders.

Metrics are also very important in making decisions about direction. We first need to understand what the intended outcomes are and then build the metric and measurement protocols to determine where the program is meeting the objectives and where it is falling short. These metrics might also measure, to some extent, the impacts on participating institutions of the SFS program.

F. Have OPM augment placement and other student-oriented activities

A number of suggestions were discussed in the context of OPM’s past, current, or future performance as a partner with NSF. They were treated separately. While in some cases there seemed to be agreement that the suggestions were desirable, there was almost no support for OPM expanding its role, as shown by the lack of votes for these when participants were polled.

Training of students on how to search for jobs is currently handled locally within SFS grantee institutions, although OPM does provide some training during an online student orientation session about writing resumes and searching for jobs within the federal government. The idea of OPM providing additional training on job searching to students received no support. One person favored having OPM develop a skills-based resume format that could be used by all SFS institutions, and such a format has been used successfully by at least one existing SFS institution (University of Tulsa). Another person suggested that OPM should provide more awareness about the existence of SFS students, their availability and skill sets, to a broad range of federal agencies. These ideas also did not garner enough broad support to warrant further discussion.

A number of placement issues were discussed that demonstrated the view that OPM could provide more help. Some frustrations were expressed in that it apparently takes 120 days to hire an IT staffer in agencies, and often this requires direct hire authority; also, sometimes, preference given to those already in government impedes the acquisition of new hires. Some suggested that SFS students should be able to be hired into any government IT position since so few of the job descriptions explicitly mention cybersecurity, as many persons in these positions actually do cybersecurity (often with little education or training in it). In contrast, NICE has seven categories of jobs, and an individual is deemed an Infosec professional if 25% of their job touches security.
It was pointed out that on a day of the workshop, 16 of the 79 cybersecurity positions on USAJOBS were at the GS-3 to GS-9 levels, and the rest were above GS-11, and several suggestions were made (for OPM) to make more jobs available to graduating SFS students:

1. The SFS program should consider opening jobs to critical infrastructure employers who are not government entities. (A justification given was Presidential Decision Directive 63 for CI protection.)

2. The government could institute a requirement for each hiring agency to fill a certain percentage of IT positions annually from SFS students. (OPM could be more forceful in urging agencies to consider SFS students when filling cybersecurity (not “IT”) jobs.)

3. OPM should consider establishing a hiring authority specifically for SFS students, making it easier for agencies to reach students that have an obligation to work for the government.

4. OPM could look at the pay scale for IT/IA positions and modify the pay scale for these positions. For example, someone fresh out of an undergrad program comes in at a GS-5 position in some agencies. However, other agencies have alternative, more attractive plans, for hiring SFS graduates. The pay scale differences between government and private alternatives are often dramatic.

5. OPM could add SFS to many job descriptions as a requirement or an advantage for potential employees.

G. Fund unpaid internships.

A suggestion was made that NSF fund (otherwise) unpaid cybersecurity internships at agencies that cannot provide funding for CyberCorps students. (This currently requires approval on an individual student case-by-case basis by the Program Manager if the grant has sufficient funds and the PI wishes to do so).
8.2 Participant Biographical Sketches

Diana Burley

Diana L. Burley is Associate Professor in the Graduate School of Education and Human Development at The George Washington University (GW). Her research and scholarly activities advance understanding of knowledge management initiatives, IT/cybersecurity education and workforce development strategies, and the impact of IT-enabled change on individuals, organizations and society (social informatics). Dr. Burley has served as the inaugural Chair of GW’s Department of Human and Organizational Learning and as Director of the Executive Leadership Doctoral Program.

Additionally, she served as a Program Officer at The National Science Foundation where she managed multi-million dollar grant programs designed to increase the capacity of the U.S. higher education enterprise to produce professionals in scientific (specifically computer science, including cybersecurity) fields. For this work, Dr. Burley was honored by the Federal Chief Information Officers Council and the Colloquium on Information Systems Security Education for outstanding efforts toward the development of the federal cyber security workforce. She has served as Vice Chair of the Association for Computing Machinery Special Interest Group on Computers and Society and as a member of the leadership team for CyberWatch, an NSF-funded cybersecurity center housed at Prince George's Community College in Maryland.

Dr. Burley holds an M.S. in Public Management and Policy, an M.S. in Organization Science, and a Ph.D. in Organization Science and Information Technology from Carnegie Mellon University. At CMU, she studied as a Woodrow Wilson Foundation Fellow in Public Policy.

Tony Coulson

Over the past 12 years, Professor Coulson has made it his mission to demonstrate to the community, state and nation techniques to forward Cybersecurity education. Within his university Tony’s major accomplishment has been his work to have the University recognized as a National Center of Academic Excellence in Information Assurance education. This recognition, given to only 110 universities, opened the door for grants, scholarships, and job opportunities for CSUSB students.

In 2008, Tony was awarded the Innovative Excellence Award in Teaching, Learning and Technology at the International Conference of Teaching and Learning. As the Director of the Cal State San Bernardino Cyber Security Center, Tony has worked with industry and government to map out opportunities for students and Cybersecurity strategies for the nation. Tony runs multiple programs that provide specialized skills to the Federal government as well as the DoD. Tony is also one of the founders of Cyberwatch West, a national Advanced Technology Education Center focusing on Cybersecurity in the western United States.
Melissa Dark

Melissa Dark is currently the W.C. Furnas Professor of Technology in Computer and Information Technology and the Assistant Director of Educational Programs at CERIAS (the Center for Education and Research in Information Assurance and Security). From 2003-2011 she served as the Assistant and then Associate Dean for Research and Strategic Planning in the College of Technology. She was the first research dean in the history of the College and successfully led the College in increasing it sponsored research funding from $300,000.00 to over $11,000,000.00.

Melissa provided key leadership in launching and managing our strategic plan, especially as it related to faculty recruitment in key academic signature areas and accountability through measurable metrics to our goals. Melissa has led national projects in educational transformation, focused on cybersecurity over the last 13 years. Her areas of expertise are in educational research, instructional development, and assessment. For example, she is currently leading the following projects in information security education: a fellowship grant; a grant that supports research experiences for undergraduate students; a project to develop a research/education network with other Centers of Academic Excellence in Information Assurance Research and Education, the National Security Agency, and the Department of Homeland Security; an assessment project in cyber operations education; and a project to look at representational fluency in fundamental areas of cybersecurity.

Nicole Dean

Nicole Dean is Director for Cyber Programs, Raytheon Company. Raytheon, with 2012 sales of $24 billion and 68,000 employees worldwide, is a technology and innovation leader specializing in defense, homeland security and other government markets throughout the world. She is responsible for developing customer-focused strategies and partnering with customers and industry teammates to shape markets and create business opportunities with a focus on cyber programs.

Prior to joining Raytheon, Ms. Dean was the Director of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS), as well as the National Cybersecurity Protection System Program Manager. She provided executive leadership in coordinating a national defense against Internet-based attacks; maintaining an effective national cyberspace response system; and implementing a cyber-risk management program for the protection of critical infrastructure. She worked collaboratively with public, private and international entities to secure the nation’s critical cyber infrastructure.

As the Director of the DISA Information Systems Center, Ms. Dean oversaw the design, development, and deployment of tools and technologies to enhance and secure the agency’s world-wide classified and unclassified networks and information systems, which span 38 locations and support over 8500 users. Ms. Dean was also the Joint Worldwide Intelligence
Communications System (JWICS) Program Manager and NASA National Security Systems Program Manager where she was responsible for the cybersecurity and management of these systems. Ms. Dean holds a Bachelor of Science Degree in both Liberal Arts and Information Technology. She holds a Masters degree in Information Systems Security from Colorado Technical University.

**Ron Dodge**

Ron Dodge is an Associate Professor permanently stationed at the United States Military Academy where he serves as the West Point Chief Information Officer and the Associate Dean for Information and Education Technology. Previously he was a senior research scientist and Director of the West Point Information Technology and Operations Center, where he led research into emerging technologies and grew cybersecurity awareness programs around the United States through innovative and pioneering use of virtualization for cybersecurity research, education, training, and operations and through cybersecurity exercises. These efforts developed curricula and cyber exercises built on a virtualized environment.

Ron has served in leadership positions in many international consortiums including the Institute for Infrastructure Protection (I3P), the Colloquium for Information Systems Security Education (CISSE), and the Honeynet Project. Currently Ron is the chair of the International Federation for Information Processing (IFIP) Working Group for Information Assurance Education. He also chaired the Information Assurance and Security knowledge area working group for the IEEE/ACM 2013 Computing Curriculum and is an active duty Colonel in the United States Army. His over 25 years of military assignments ranged from combat duties in an attack helicopter squadron to faculty at the United States Military Academy.

Ron received his Ph.D. from George Mason University in Computer Science. His current research areas are information warfare, network deception, security protocols, internet technologies, and performance planning, and capacity management. He is a frequent speaker at national and international security events and has published many papers on the topic.

**Lance Hoffman**

Lance J. Hoffman is Distinguished Research Professor of Computer Science and the Director of the Cyber Security Policy and Research Institute at The George Washington University (GW) in Washington, D. C., and the author or editor of numerous articles and five books on computer security and privacy. He directs the Department of Homeland Security and National Science Foundation computer security “Cyber Corps” scholarship programs at GW; these programs have produced over seventy federal government experts in computer security, all of whom have a working knowledge of privacy as well. He continues to lead efforts on cybersecurity workforce development and on integration of technological, policy, and social science perspectives on cybersecurity.
Professor Hoffman developed the first regularly offered course on computer security at the University of California, Berkeley in 1970 after serving on the Advisory Committee to the California Assembly Committee on Statewide Information Policy. A Fellow of the Association for Computing Machinery, Dr. Hoffman institutionalized the ACM Conference on Computers, Freedom, and Privacy in 1992, and has served on a number of Advisory Committees including those of Federal Trade Commission, the Department of Homeland Security, the Center for Democracy and Technology, and IBM. Dr. Hoffman received his B. S. in mathematics from Carnegie Mellon University and his M. S. and Ph. D. from Stanford University in computer science.

Alan Greenberg

Mr. Greenberg is the Senior Director for IT Security and Risk Compliance at PPL Corporation. PPL is an Energy company headquartered in Allentown Pennsylvania and has subsidiaries in Kentucky, Montana and the United Kingdom. Mr. Greenberg is responsible for cybersecurity, security regulatory compliance and supports security design, implementation, testing across all of the company’s business areas. This includes IT Operations; Network and Cloud Systems; Data Centers; Mobile Device Security; policies, technologies, cybersecurity personnel, and protecting the energy generation operations systems. Mr. Greenberg has previously served as Technical Director for Boeing’s Cyber Security Business Unit; supporting activities in the federal sector, energy, aviation, automotive and satellite industries and Department of Defense programs; Additionally, Mr. Greenberg has also been with Raytheon’s Communication Network Group Division as the Information Assurance Group Program Manager. Alan is retired from the U.S. Army as a Signal Corps Officer serving in a variety of assignments including Battalion, Brigade and Division G6 assignments, Signal Battalion Operations Officer; serving on multiple communication systems fielding teams; Communications Officer at the VII Corps TAC during Desert Storm, and as a Program Manager at NSA’s Information Assurance Division. Mr. Greenberg has a MSA from Central Michigan University and a B.S. from Western Illinois University.

Dan Manson

Dr. Dan Manson, CISSP, is a Professor at California State Polytechnic University, Pomona (Cal Poly Pomona). Dr. Manson teaches Information Systems Auditing, Internet Security and Computer Forensics in the College of Business Administration Computer Information Systems undergraduate and Master of Science in Information Systems Auditing programs. From September 2003 to March 2004 and January to December 2006, Dr. Manson served as the campus Information Security Officer for Cal Poly Pomona. Dr. Manson led the effort for Cal Poly Pomona to be designated a National Center of Academic Excellence in Information Assurance Education in 2005 and again in 2008. Dr. Manson is in charge of the Western Regional Collegiate Cyber Defense Competition and California Cyber Challenge as part of the United States Cyber Challenge.
Dan has been co-Principal Investigator on three National Science Foundation grants to support workforce, curriculum and professional development in cybersecurity, including the current CyberWatch West NSF ATE Regional Center grant. Dan serves on the Academic Relations Committee for the Los Angeles Chapter of the Information Systems Audit and Control Association and as President of the Southern California High Technology Crime Investigation Association.

**Alan Paller**

Alan Paller founded SANS, a college and professional cybersecurity training school that has trained more than 145,000 cybersecurity technologists in 72 countries. He oversees the Internet Storm Center, the annual identification of the "Seven Most Dangerous New Attack Vectors" and a global program that identifies and celebrates people responsible for remarkable improvement in cyber risk reduction. He has testified before the US Senate and House and was an initial member of the President's National Infrastructure Assurance Council. He was chosen by OMB and the Federal CIO Council as the 2005 Azimuth Award winner, a lifetime achievement award recognizing outstanding service of a non-government person to improving federal information technology.

In 2010, the Washington Post named him one of seven people "worth knowing, or knowing about" in cybersecurity. He co-chairs the Secretary of Homeland Security's Task Force on CyberSkills, and serves on the FCC Communications Security, Reliability and Interoperability Council and on the NASA Advisory Council. Earlier in his career Alan helped build one of the first major software companies, took it public, and merged it into a larger company listed on the New York Stock Exchange. His degrees are from Cornell University and the Massachusetts Institute of Technology.

**Costis Toregas**

Dr. Toregas is the Associate Director of the GW Cyber Security Policy and Research Institute. He is Lead Research Scientist in the GW Department of Computer Science, an adjunct faculty member in the Trachtenberg School of Public Policy and Public Administration at George Washington University (GW), and the Director of Operations and Industry Liaison for the National CyberWatch Center (NCC), an NSF funded ATE Center focused on workforce development in Cybersecurity through networking more than 100 community colleges and universities. He teaches courses in Public Private Partnerships and IT as Empowerment for Public Administrators. His research interests include Computer Security and Information Assurance, the use of games and competitions as learning strategies, the intersect of policy and technology in the public sector, and aspects of Social Equity in public administration.

Professor Toregas led the non-profit Public Technology Inc. organization for more than 35 years, advocating the creation and deployment of new innovative technologies for local governments in
partnership with the private sector, and lectures extensively in 6 continents about the impact of the digital age on government. He serves as the IT Adviser to the County Council of Montgomery County, MD, overseeing the investment of $200m annually in Information Technology goods and services. He is a fellow of the National Academy of Public Administration, and the immediate past chair of its standing panel on Social Equity in Governance. Dr. Toregas holds Ph.D. and M.S. degrees in Environmental Systems Engineering and a B.S. in Electrical Engineering from Cornell University.

**Joseph Tront**

Joe Tront is a Professor of Electrical and Computer Engineering in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He is also the Director of Education for the VT Hume Center for National Security and Technology where he guides several programs on cybersecurity education and intelligence community training. His research work involves the development of various mechanisms for moving target defenses, intrusion detection, sensor security, and home network protection. He has developed a cross-discipline cybersecurity minor at VT as well as a graduate certificate in cybersecurity. He has supported other faculty members in developing a rich offering of courses in cybersecurity. He is an ABET program evaluator. His research and curricular development work is sponsored by the NSF, various agencies in the DoD and government, and a number of private industries.

**Susanne Wetzel**

Dr. Wetzel is an Associate Professor at the Computer Science Department of the Stevens Institute of Technology. She first joined the faculty at Stevens as Assistant Professor in 2002. She received her Diploma in Computer Science from the University in Karlsruhe (Germany) and her Ph.D. degree in Computer Science from Saarland University (Germany) in 1998. Subsequently, she worked at DaimlerChrysler Research (Stuttgart, Germany), Lucent Technologies Bell Laboratories (Murray Hill, USA) and RSA Laboratories (Stockholm, Sweden). Her research interests are in cryptography and algorithmic number theory.

Her recent publications include works on privacy-preserving reconciliation of ordered sets and its applications; identifying transitive information leakages and analyzing their economic implications in complex networks; and parallelizing lattice basis reduction algorithms. Dr. Wetzel is the co-designer and program director of the B.S. in Cybersecurity degree program at Stevens Institute of Technology. She also heads the Stevens SFS Scholarship program. Dr. Wetzel currently serves on the Board of CISSE and the Executive Board of DIMACS.

**Vera Zdravkovich**

Dr. Vera Zdravkovich is the Senior Advisor and past Director and PI of CyberWatch, an Advances Technological Education (ATE) Center. In her leadership role at CyberWatch, Dr. Zdravkovich worked with DHS, NSA, and NSF to establish the Center of Academic Excellence Two Year Cybersecurity SFS Workforce Development Workshop Report
(CAE2Y) designation that became a reality in 2010. She leads this national project and works with community colleges nationally to support them in building their cybersecurity programs. She served as a mentor to several ATE centers, and provided advice and consults to consortia in Louisiana, California, and New York and has served on numerous state and national committees on science and technology education.

PROJECT SUPPORT PERSONNEL

Katelyn Anders

Katelyn Anders is the Coordinator for the Cyber Security Policy and Research Institute (CSPRI) at the George Washington University. She holds a BA in Sociology from Christopher Newport University and an MPA from American University. She is interested in the intersection between the social sciences and cybersecurity, focusing on how the cultural values of social media affect views on privacy and security.
8.3 Working Group Composition

GROUP 1
Vera Zdravkovich*, Prince Georges Community College
Alan Paller, SANS
Nicole Dean, Raytheon
Dan Manson, California State University at Pomona

GROUP 2
Melissa Dark*, Purdue University
Joe Tront, Virginia Tech
Lance Hoffman, George Washington University

GROUP 3
Tony Coulson*, California State University-San Bernardino
Suzanne Wetzel, Stevens Institute of Technology
Alan Greenbeerg, PPL
Costis Toregas, George Washington University

GROUP 4 (snowbound, connected via phone in evening)
Diana Burley, George Washington University
Ron Dodge, United States Military Academy
Patrick Kelly, SFS alumnus from George Washington University

OBSERVERS
Paul Tymann, National Science Foundation
Valerie Barr**, National Science Foundation
Kathy Roberson, OPM

*Group leader    ** Day 1 only
8.4 Agenda

Thursday, February 8, 2014

8:45-10:15  Valerie Barr, NSF.  Opening remarks
            Short talks by each participant
            Lance Hoffman, GW, Synthesis of bullet points sent in by participants prior to
            meeting
            Costis Toregas, GW, Working group guidelines

10:15-10:30  Break

10:30-12:00  Working Group Meetings

12:00-12:45  Lunch

12:45-2:00  Working Group Meetings

2:00-2:15  Break

2:15-2:45  Reports from Working Groups

2:45-3:30  Discussion

3:30-3:45  Break

3:45-4:30  Working Groups Revise Their Products

4:30-5:00  Reports from Working Groups

Friday, February 9, 2014

8:45-9:00  Inputs from Snowbound Participants

9:00-10:15  Discussion and Reactions. Put Some Items in “Parking Lot”

10:15-10:30  Break

10:30-11:15  Working Groups Meet to Put Items into Vote-able Statements =
            Action Items for NSF to Consider (and to add or delete other items)

11:15-12:00  Reports from Working Groups

12:00-12:45  Lunch

12:45-2:00  Voting and Announcement of Results; Discussion of Short Term, Long Term, and
            Funding Issues

2:00-2:15  Break

2:15-3:15  For Top Action Items, Vote on Short Term vs. Long Term

3:15-4:00  Discussion

4:00-4:15  Wrap-up
8.5 Presentation of Valerie Barr, NSF

**NSF Investment in Cybersecurity Education and Workforce Development**

Dr. Valerie Barr  
SFS co-Lead Program Director  
National Science Foundation

**Estimate of the number of information security professionals (Frost & Sullivan)**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>2,305,664</td>
<td>2,851,737</td>
<td>2,923,369</td>
<td>3,329,183</td>
<td>3,752,605</td>
<td>4,244,120</td>
<td>4,374,024</td>
</tr>
<tr>
<td><strong>Estimate</strong></td>
<td>2010-2015</td>
<td>30.4%</td>
<td>13.2%</td>
<td>13.2%</td>
<td>13.2%</td>
<td>13.2%</td>
<td>13.2%</td>
</tr>
<tr>
<td><strong>Worldwide</strong></td>
<td>700,845</td>
<td>1,058,772</td>
<td>1,214,341</td>
<td>1,275,195</td>
<td>1,370,320</td>
<td>1,392,236</td>
<td>1,421,941</td>
</tr>
<tr>
<td><strong>U.S.</strong></td>
<td>477,231</td>
<td>750,489</td>
<td>921,376</td>
<td>981,701</td>
<td>1,044,490</td>
<td>1,148,305</td>
<td>1,148,305</td>
</tr>
<tr>
<td><strong>North America</strong></td>
<td>742,418</td>
<td>850,666</td>
<td>754,321</td>
<td>1,020,248</td>
<td>1,008,020</td>
<td>1,205,029</td>
<td>1,138,376</td>
</tr>
</tbody>
</table>

---

**Cybersecurity Education - Funding Opportunities at NSF**

- CyberCorps®: Scholarship for Service (SFS) – $300-900K/Capacity; $1-5M/Grant
- Secure and Trustworthy Cyberspace Education Perspective (SaTC-EDU) – up to $300K/project
- Advanced Technological Education (ATE) – up to $800K/project or $3-5M/center

---

**SFS Mission and Structure**

The CyberCorps(R): 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 development, outreach, faculty, institutional, and/or partnership development.

---

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

---

**CyberCorps®: Scholarship For Service (SFS) History**

- First cohort of 9 students entered the Federal IA workforce in 2002. In 2013, there were 188 graduates.
- To date, 2071 SFS scholarship recipients, of these 463 in current academic programs and 1554 have already graduated.
- SFS graduates served in more than 140 federal departments, agencies, and branches as well as in state, local, and tribal governments.
### Advanced Technical Education (ATE) Centers for Cybersecurity Education

- **Ctr. for Systems Security & Info. Assurance (CSSIA)**
  - Moraine Valley CC (II) 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**
  - Whatcom CC (WA) and partners (moved from Mt. San Antonio College)
    - [cyberwatchwest.org](http://cyberwatchwest.org)

### Clearance Problem

#### Table 9. Master’s Degrees Awarded by Ethnicity

<table>
<thead>
<tr>
<th>Ethnicity</th>
<th>CS</th>
<th>CE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonresident Alien</td>
<td>3322</td>
<td>56.7%</td>
</tr>
<tr>
<td></td>
<td>774</td>
<td>72.6%</td>
</tr>
</tbody>
</table>

### Ecosystem Problem

#### Table 13. Ph.Ds Awarded by Ethnicity

<table>
<thead>
<tr>
<th>Ethnicity</th>
<th>CS</th>
<th>CE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonresident Alien</td>
<td>634</td>
<td>48.1%</td>
</tr>
<tr>
<td></td>
<td>130</td>
<td>67.4%</td>
</tr>
</tbody>
</table>
Teaching hospitals for law school graduates

Learning in Informal Settings

Cybersecurity Athletes

- It takes approximately 10,000 hours of deliberate practice to master a skill; i.e. 20 hours a week for 10 years.
- The average world-class athlete trains 23 hours a week.
- The average athlete in America trains 12 hours a week.
- Equals 10,000 hours.
- In 2012, 3.2 million girls and 4.4 million boys played organized sports in high school.

National Cybersecurity Sports Federation (NSF #1343536; Cal Poly Pomona; PI: Dan Manson)

"...This project develops NCSF, an organization and infrastructure, to support current and future cyber competitions, to help create rules of the game, determine learning objectives, eligibility, metrics, and a code of ethics. A network of stakeholders is organized in a manner that does not threaten individual competitions but provides value to the collective endeavor. The project provides a shared pathway vision for students to learn cyber competitions the way athletes learn a sport. It negotiates an agreement on common goals, learning objectives, performance measurements, and desired outcomes..."