Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development

Lance J. Hoffman
The George Washington University

Report GW-CSPRI-2010-3

December 15, 2010

Work supported by National Science Foundation award 0621334

Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development

EXECUTIVE SUMMARY

Recognizing the imminent potential for substantial growth in cyber security education, a group of stakeholders gathered October 13–15, 2010, to reflect on lessons learned from government programs supporting cyber security education and workforce development (CSEWD). Participants focused on improving CSEWD programs to develop the government information technology workforce and produce more college graduates with cyber security skills.

Workshop participants recognized several cross-cutting principles for improving CSEWD, including the need for international and multi-disciplinary approaches, larger programs that reach many more people, and long-term planning and coordination.
They also identified a number of barriers that inhibit CSEWD, such as the traditional organization and reward system of most universities, difficulties securing hands-on educational opportunities, concerns about the relevance of the Center of Academic Excellence "brand," and disagreement about the role of standardization in cyber security education and training.

Through open discussion and brainstorming, participants generated numerous observations about the National Science Foundation's (NSF's) Scholarship for Service program (SFS) in particular, as well as potential approaches to address them, that encompass the following:

- Increasing cooperation, collaboration, and interaction among and within SFS grantee institutions
- Increasing the size of SFS
- Offering strategic planning grants to SFS institutions
- Convening a wide range of stakeholders to address the shortage of cyber security graduates
- Increasing collaboration with related programs within and outside of NSF

For CSEWD in general, the participants offered a wide range of far-reaching suggestions, as well as potential mechanisms for consideration:

- Expand training opportunities and advanced educational opportunities for the workforce.
- Codify the body of cyber security knowledge and identify the desired educational outcomes.
- Create more opportunities for real-world and hands-on learning.
- Consider additional mechanisms to provide experiential learning and frequent education about new cyber security threats.
- Build a coalition of stakeholders to expand support for cyber security education.

Participants agreed that a wide range of stakeholders, including current SFS institutions, should take the next steps to improve CSEWD. In particular, it is important to ensure that universities continue to have incentives to participate in the SFS program.

Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development

TABLE OF CONTENTS

Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development

BACKGROUND

"Cyber security risks pose some of the most serious economic and national security challenges of the 21st century," states the *Cyberspace Policy Review*[1] presented to the White House in 2009. The report is just one of many sources that underscore the need for far more college graduates in information technology (IT) and specifically in cyber security to fill both public- and private-sector needs.

Federal efforts to address those needs include the establishment in 2000 by the National Science Foundation (NSF) of the Scholarship for Service program (SFS) to fund undergraduate and post-graduate education in exchange for entering the federal government's IT workforce after graduation. At approximately the same time, the Department of Defense started a similar effort, the Information Assurance Scholarship Program (IASP). Both programs also provide capacity-building grants to academic institutions to bolster cyber security education and workforce development (CSEWD).

In response to increased public attention to cyber security, a number of proposals currently in Congress (as of late 2010) would increase funding for cyber security education and training. Recognizing the potential for growth of educational opportunities in cyber security as well as the demand for cyber security skills in the workplace, a group of educators, IT professionals, program managers from government agencies, and other stakeholders and experts gathered October 13–15, 2010, at the Airlie Center in Warrenton, VA, to reflect on the successes, lessons learned, and future challenges since the first formal government programs supporting CSEWD were launched.

WORKSHOP GOALS, APPROACH, AND FINDINGS IN BRIEF

The objective of the workshop was to use the lessons of the past to guide consideration of how CSEWD programs can meet the challenges of tomorrow's world—especially developing the government workforce—and to indicate how CSEWD programs can continue to produce post-secondary school graduates who bring up-to-date, applicable cyber security skills to their jobs. (The workshop agenda appears in Appendix 1; a list of participants appears in Appendix 2.) The goals in particular were as follows:

- Share, summarize, and document lessons learned from SFS cyber security workforce development activities.
- Identify continuing challenges to producing a skilled cyber security workforce for the federal government, as well as state, local, and tribal governments; educational institutions; and private industry.
- Make suggestions for improving the quality and quantity of cyber security workforce development.

Workshop participants broke out into workgroups to consider the following questions:

- Is the existing structure of CSEWD programs—targeting, for example, scholarships and capacity-building—adequately meeting the needs of and engaging all of the institutions that can make a significant impact on the field? Are there opportunities for additional areas of emphasis?
- How can CSEWD programs incentivize more interdisciplinary work?
- Are current eligibility criteria, such as Center of Academic Excellence in Information Assurance Education (CAE/IAE) designations, effective and sufficient for determining eligibility for CSEWD programs? Should other factors, such as interface with other national service initiatives, be considered?
- How can CSEWD programs better encourage development and dissemination of better teaching tools, methods, and content?
- What role should an internationally developed education framework have moving forward in CSEWD?
- What licensing/accreditation/professional standards should the field move toward—if any? Who should "own" that process?

Following reports from the workgroups and discussion, the participants identified gaps, barriers, and challenges to implementing and improving CSEWD in general. They composed a list of observations specific to SFS and potential approaches to address them that could also be used by IASP and other institutions to begin meeting the challenges. They also developed a number of suggestions to address CSEWD more broadly.

This document first describes a set of cross-cutting principles that participants felt should inform efforts to address CSEWD needs. Next, it provides a summary of the pervasive barriers to improving CSEWD identified by the workshop participants. Finally, it lists some of the participants' observations and suggestions for SFS in particular and CSEWD in general, as well as potential approaches for addressing those observations and suggestions. (The SFS-specific and general observations and suggestions are summarized briefly in Exhibits 1 and 2.)

Exhibit 1: Observations About SFS

SFS has been very effective at producing qualified graduates for federal cyber security needs. However, the number of trained workers is still insufficient to meet the federal demand, and there are similar needs within state, local, and tribal governments; educational institutions; and private industry. The workshop participants made the following observations aimed at increasing the number of future workers trained through SFS:

- SFS would benefit from facilitating more cooperation, collaboration, and interaction among and within programs.
- To increase the number of students educated, SFS would have to increase the number of funded institutions, increase the number of students funded at each institution, or explore alternative modes of preparing qualified employees (in parallel with the existing SFS model).
- In addition to scholarships and capacity-building grants, institutions would also benefit from strategic planning grants.
- By casting a wider net to involve more stakeholders, SFS could better identify what roles these stakeholders should play and assess what stakeholders are willing to do to address the shortage of cyber security graduates.
- SFS could identify opportunities for collaboration by evaluating its relationship with other federal programs.

Exhibit 2: Suggestions for Improving CSEWD

Current CSEWD programs have not produced the number of trained people necessary to meet the overall demand. Therefore, the workshop offered the following suggestions to increase the impact of CSEWD programs in general:

- Expand training opportunities and advanced educational opportunities for the workforce.
- Codify the body of cyber security knowledge and identify the desired educational outcomes.
- Create more opportunities for real-world and hands-on learning.
- Because cyber security is a rapidly changing field that requires experiential learning and frequent education about new threats, consider alternatives to the traditional university model for providing relevant education.
- Build a coalition of stakeholders to expand support for cyber security education.

It is important to recognize that participants approached the workshop as an opportunity to brainstorm; the ideas that resulted do not represent formal recommendations, nor do they necessarily reflect consensus among all who took part. Rather, they represent the opinions of leading stakeholders in the field, to be used as a starting point in addressing CSEWD challenges.

A note about terminology: This document uses the term "cyber security" as a catch-all phrase that encompasses both information assurance ("measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities"[2]) and information security ("protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction"[3]).

WORKSHOP FINDINGS

CROSS-CUTTING PRINCIPLES FOR ADDRESSING CYBER SECURITY EDUCATION AND TRAINING

Workshop participants identified a number of cross-cutting principles—concepts that should be applied to any efforts to improve CSEWD:

- Cyber security is an **international issue**. Strategic planning should go beyond the federal level, taking into account needs, concerns, and opportunities at the national and international levels. As one of the dominant countries in both development and use of IT, the United States has an opportunity and, some might say, an obligation to nurture this planning.

- Cyber security requires a **multi-disciplinary approach**. Efforts should be made to educate and partner with disciplines not always thought of as related to cyber security (e.g., decision sciences, forensic sciences, public policy, law). A holistic approach will foster more collaboration across disciplines, increase interest in cyber security as a necessary component of nearly all types of work, and increase resources and support for cyber security.

- **Curative—not palliative**—approaches are needed to address causes rather than symptoms of the continuing security breaches in computer systems.

- The field of cyber security education requires the **development of metrics and processes for evaluation** to identify successes and areas for improvement. Tools to measure, monitor, and track programs should be developed, tested, and validated, then made available to educational institutions and programs to implement as appropriate.

- **Recruiting and retaining minorities and women** into cyber security education and the cyber security workforce is vital to meet the workforce demand. Women and minorities make up an increasingly large proportion of the workforce. "Unless the science, engineering, and technology labor market becomes more representative of the general U.S. workforce, the nation may likely face severe shortages in science, engineering, and technology workers,"[4] noted the Congressional Commission on the Advancement of Women and Minorities in

Science, Engineering and Technology Development.

- **Long-term sustainability and integration** of CSEWD efforts must be considered, given the scope of the need and the rapid pace of developing technology. Better strategies are needed to connect the currently unconnected segments of cyber security education and awareness from kindergarten through graduate school and beyond. A **lifelong learning continuum**, or "K-through-gray" approach, should be developed.

BARRIERS TO ADVANCING CYBER SECURITY EDUCATION, TRAINING, AND WORKFORCE DEVELOPMENT

Despite the pressing need for more workers skilled in cyber security, CSEWD continues to face barriers—notably, a lack of consensus on how to integrate cyber security education into current academic settings. The CSEWD workshop participants identified several "inconvenient truths," or entrenched barriers that inhibit efforts to advance CSEWD:

The university model does not completely satisfy all cyber security education and training needs. Traditional undergraduate and graduate programs tend to take several years to complete and include general courses not related to cyber security (in service of the larger educational mission). Because university programs often do not address the time-specific needs of industry and government, they sometimes face difficulties educating students about a rapidly changing field. They often do not meet the needs of people who cannot take time out of the workforce to pursue a degree. They are generally not intended to provide short, intensive courses that respond to specific and current concerns.

Academic silos prevent collaboration and integration. Cyber security is a relatively new field that does not always integrate neatly with other computing programs. Academic departments are notorious for guarding their resources and are justifiably resistant to giving up faculty spots, laboratory space, or funding opportunities. Most academic programs have tended to build their own tools rather than exchange resources with others, and they tend to hold firm ownership over whatever they create. Alternative approaches to education, such as online learning and co-op education, sometimes are seen as a threat or as too difficult to incorporate while maintaining a core mission of the university (education, as opposed to training). Often, universities lack incentives to try new approaches; that is, the current system of rewards is insufficient.

Experiential education is not popular with employers. Employers want cyber security graduates with real-world experience but are reluctant to provide that experience through internships or part-time work because 1) the return on investment is uncertain, 2) screening and training interns for meaningful work is expensive and time-consuming, and 3) organizations cannot afford to make their systems vulnerable to possible threats. Some organizations want students to have

specialized education but don't provide the state-of-the-art tools and related resources (training, maintenance) that correspond with their specific needs.

Upper-level management generally does not buy in to advanced education and training. Few opportunities are available for working people to increase their cyber security knowledge and skills without leaving their jobs permanently. Even fewer opportunities are available to those at the highest levels of an organization—the people with the most influence in their companies.

The CAE/IAE designation lacks solid prestige. Granting CAE status to so many institutions has diluted the cachet of the label, and private-sector employers don't see CAE as a meaningful credential. Some of the country's most prestigious universities that produce technically accomplished graduates with computer security knowledge are not CAEs. Historically, universities have selectively applied for designations such as "CAE" on the basis of their goals and aspirations, internal competencies, target student audiences, and budgets. Because university departments have not traditionally taught courses geared toward standards such as those that CAEs are required to teach, it is not surprising that many fine universities have not applied to become CAEs. Even among CAEs, there is no independent mechanism for validating outcomes or results, so it is not clear to what extent grant-receiving institutions actually teach to the required standards.

There is strong disagreement over whether barriers to cyber security education and training could or should be addressed through standardization. Standardized curricula, program accreditation, and specialty certification have all been recommended as mechanisms to improve CSEWD. But cyber security threats change rapidly, as do technology and platforms, so standards must be updated in a timely manner. If consensus were reached about some minimum guidelines around a set of generally accepted skills, organizations would have to emerge that can be trusted to take responsibility for applying appropriate metrics impartially (to accreditation or certification programs, for example). One recently formed non-profit organization, the Center for Internet Security,[5] may be nimble enough to produce and update standards that adapt to the changing landscape.

National security concerns can hinder international collaboration. The Internet is global, and while cyber security issues are international and multi-national, they are also nation-specific and intertwined with national security, competitiveness, and wide variations in the laws that govern privacy and data protection.

Current efforts to link employers with high-quality students are not positioned to meet large-scale needs. Within SFS, the Office of Personnel Management has established the SFS job fair to bring together a wide range of employers and students. However, to become more effective and efficient, the job fair should draw from more agencies, and SFS should provide more graduating

student job candidates. Both within and outside of SFS, some academics have forged relationships individually with certain employers, on whom they rely to place their graduates in internships and jobs. These informal networks are tight-knit, difficult to penetrate, and do not scale well.

UPDATING SFS TO MEET CAPACITY NEEDS

To address the needs of SFS, participants came up with the following observations, which are also relevant to the IASP. However, many of the concepts are applicable to CSEWD in general. Participants offered a wide array of suggestions on which SFS policymakers, administrators, and stakeholders may further deliberate. Implementing these ideas may require substantial cost or effort (e.g., new Congressional legislation); therefore, the goals and potential benefits should be weighed carefully against the cost and effort required. Participants noted that the cost of inaction now is that it will be more expensive to address systemic problems and the need for individuals trained in cyber security in the future.

The observations were not prioritized. However, to get a sense of priorities related to SFS, at the end of the workshop, participants were asked to make suggestions for two potential scenarios. In the first scenario, , the SFS budget would be increased threefold, immediately, and remain at that level for the foreseeable future. In the second, the SFS annual budget would be cut drastically, immediately, and for the foreseeable future

The "increased budget" scenario was conceived in response to the increasing legislative attention received by SFS in the past year. One proposal under consideration by Congress would provide a dramatic increase in funding for the program over the next 5 years. Currently, SFS is funded at approximately $15 million per year, which is spread out over 30 universities and provides education funding for about 250 students—125 of which graduate and enter the federal workforce each year. The proposed Cybersecurity Act of 2010 would increase the funding to $50 million or even $70 million per year over the next 5 years. This increase would provide enough scholarship funding to support 1,000 SFS students per year. To meet that need, it is likely that more schools would participate in the program (doing so under the assumption that the funding would be stable and predictable). Many of the approaches the participants suggested below could be implemented with a modest increase in funding. However, to produce the number of educated professionals desired, more substantial increases in funding are necessary.

Through the "decreased budget" exercise, it became clear that participants feel the overall structure and approach of SFS is sound. Some suggested focusing on mechanisms for better leveraging existing resources and encouraging universities and federal agencies to invest more of their own resources. However, participants emphasized that any significant cut to the program would severely undermine the goal of contributing skilled workers to the federal IT workforce. The SFS program was found to be a strong and important response to the challenge, and participants clearly want to see the program not only continued but expanded.

Observations and Potential Approaches for SFS

SFS Observation 1: **SFS would benefit from facilitating more cooperation, collaboration, and interaction among and within programs**.

Potential Approaches

Create a position/office that coordinates networking and interaction among grantee programs.

Create a one-stop portal for vetted resources from grantee programs that are publicly available, searchable, and up to date. Such resources could include course syllabi, faculty development materials, and tools that can be adapted by other grantee programs (e.g., streamlined forms or applications that reduce paperwork).

Create more mechanisms for sharing resources and knowledge, similar to the existing SFS job fair, virtual laboratories (e.g., the Advanced System Security Education, Research and Training Center at the University of Alaska, Fairbanks, and the Center for Systems Security and Information Assurance at Moraine Valley Community College), and "boot camps" (or program orientation) for faculty and administrators with new SFS programs.

Encourage interdisciplinary networking and interaction internally within grantee programs (e.g., George Washington University's Cyber Security Policy and Research Institute, New York University's Center for Interdisciplinary Studies in Security and Privacy, and Purdue's Center for Education and Research in Information Assurance and Security).

Develop additional specific mechanisms that facilitate collaboration, such as the Office of Personnel Management's annual SFS job fair or a web site for sharing resources, results, and opportunities in a clear and user-friendly manner. An example (from the National Institutes of Health's Clinical and Translational Science Awards program, where stakeholders from government, academia, and industry are collaborating in unprecedented ways to speed the translation of science from the bench to the bedside) is shown in Exhibit 3.

Exhibit 3: Example of a User-Friendly Web Site for Sharing Professional Resources

Consider streamlining paperwork with a universal SFS application and online application and tracking system (that takes into account federal education privacy regulations).

Evaluate the IASP "football draft" model (in which agencies gather together to select scholarship recipients/future employees from a pool of applicants) to determine whether some limited use of this approach would have a positive or negative effect on cooperation among SFS faculty and programs and on the overall quality of students recruited.

SFS Observation 2: **To increase the number of students educated, SFS would have to increase the number of funded institutions, increase the number of students funded at each institution, or explore alternative modes of preparing qualified employees (in parallel with the existing SFS model).**

Potential Approaches

Create separate funding programs or other mechanisms to support both basic (e.g., startup or "suborbital") educational programs and advanced (e.g., established or "orbital") efforts in established programs (similar to the way the U.S. Department of Health and Human Services supports basic research on medical countermeasures through the National Institutes of Health and advanced research through the Biomedical Advanced Research and Development Authority).

Establish a hierarchy of qualifying institutions, such as CAE/IAE levels one through five. The new category for 2-year institutions (CAE-2Y) should provide a surer way for students to articulate from 2-year to 4-year institution programs. Provide scholarships and capacity-building grants to encourage bridge or feeder programs that help students transition to the next level of education or employment.

Expand participation through outreach and creative approaches to engage other schools and students, such as the following:

- Use of satellite campuses
- Creative, engaging programs (e.g., the Cell Phone Forensic Laboratory at the University of Tulsa)
- Use of subcontracts between CAEs and non-CAEs to encourage participation by qualified non-CAE schools (an approach that has been used, for example, by The George Washington University and neighboring Marymount University)
- Use of social networking sites to increase communication among students and faculty and spread the word about SFS

Explore alternative service models:

- Emphasize the ability of the service agencies to include state, local, and tribal government agencies, an expansion already permitted in the program but not well appreciated or utilized. (This approach would be appealing to students who would prefer to stay in their home region; it also enhances the local workforce.)
- Allow teaching to qualify as the service in appropriate, qualified government-funded and private institutions.
- Consider more flexible payback terms, such as a third year of service (in exchange for a third year of scholarship funding) to be completed later in the grantee's career or shorter/longer service terms depending on the type of service selected.
- Consider a cyber security "reserve corps" of grantees willing to return to service on short notice or after retirement (see, e.g., the SCORE program for business counseling by retired executives).
- Establish a cooperative extension program for computer security. Teach or coach students to provide services (e.g., disinfecting computers) or training to local businesses or individuals for modest fees and, perhaps, course credit.

Consider opening SFS to students who do not attend school full time or who are already in the workforce (perhaps as government workers).

SFS Observation 3: In addition to scholarships and capacity-building grants, institutions would also benefit from strategic planning grants.

Potential Approaches

Encourage strategic planning that leads to self-sustaining programs.

Encourage universities to address issues of long-term sustainability, scaling up, metrics, collaborative programs across grantee organizations, and evaluation.

Fund mechanisms to track SFS grantee performance, job placement, and career trajectories following completion of the SFS service requirement. Emphasize the need for institutions to better plan in advance—before grants are awarded—how they will measure progress. Develop a mechanism within SFS to acquire long-range data on the program.

SFS Observation 4: **By casting a wider net to involve more stakeholders, SFS could better identify what roles these stakeholders should play and assess what stakeholders are willing to do to address the shortage of cyber security graduates.**

Potential Approach

- Convene workshops that include not only educators, IT professionals, and program managers from government agencies that use SFS and IASP, but also, for example:
    - front-line cyber security workers;
    - consumers;
    - high school and community college faculty;
    - high-level federal (i.e., Cabinet departments) policymakers;
    - additional civilian, defense, and intelligence community decision-makers, including managers of other NSF programs;
    - legal experts (to address liability, intellectual property, and other issues); and
    - industry representatives, such as the industrial control systems community (industrial engineers who oversee automated systems that control critical infrastructures).

SFS Observation 5: **SFS could identify opportunities for collaboration by further evaluating its relationship with other federal programs.**

Potential Approaches

- Create opportunities (e.g., through workshops and policy coordination meetings) for staff from various programs to learn from each other, discuss common issues, and coordinate approaches.
- Develop joint program solicitations.
- Continue working jointly with the National Initiative for Cybersecurity Education (NICE), the NSF Computer & Information Science & Engineering (CISE) program, the National Security Agency (NSA), and others.

MEETING CHALLENGES IN CYBER SECURITY EDUCATION

Taking into account the cross-cutting principles and the barriers mentioned, participants proposed a number of suggestions for improving education and better educating and training the workforce. The goal of the workshop was to facilitate a broad examination of the field; as a result, the suggestions are far-reaching and require further consideration by stakeholders. In some cases, suggestions refer to existing, successful programs. In other cases, participants offered novel ideas that would merit much more exploration to

determine their feasibility. As mentioned earlier, the goals and potential benefits should be weighed carefully against the cost and effort required.

Suggestions and Potential Approaches for Improving CSEWD

CSEWD Suggestion 1: **Expand training opportunities and advanced educational opportunities for the workforce.**

Potential Approaches

Target federal workers who want to pursue advanced cyber security education.
Consider public-private partnerships to offer non-traditional training and education opportunities.
Encourage federal agencies to develop their own cyber security scholarship programs. Using the SFS model, agencies could provide scholarships to students (or to existing employees) who better meet their agency-specific cyber security needs, possibly supplementing existing courses with training specific to a given agency. The IASP offers a model for ensuring that the student is hired by the funding agency or division upon graduation.
Evaluate workforce training efforts to ensure that programs are effective and results are useful. Involve industry in ongoing learning initiatives.
Explore models and incentives for virtual cyber security education, such as *a la carte* training options (allowing users to pay only for the courses they want to take) and the Groupon approach (bigger discounts or free courses when users sign up their friends and colleagues).
Explore potential models for flexible learning (see Exhibit 4).

Exhibit 4: Models of Flexible Learning

Weekend master's degree programs that target professionals and focus on real-world management and technical issues
Independent training and certification programs (e.g., SANS, which offers both degree and certification programs)
Modular learning, such as the following:

- Oxford University's master's degree for external students
- England's Open University, which offers professional development courses through a network of regional centers that facilitate networking, coaching, and peer interaction and balance online learning with face-to-face tutoring from program graduates
- Stevens Institute of Technology's systems engineering training, which can be on campus, online, or on-site and offered in semester-long courses or in modules)

Immersion training (e.g., SANS' Security Essentials Bootcamp Style)
Online/distance learning options combined with traditional academic studies (e.g., University of Florida's online education program)

CSEWD Suggestion 2: Codify the body of cyber security knowledge and identify the desired educational outcomes.

Potential Approaches

Consider developing an international consensus on the key components of cyber security education.[6]

Ensure that educational standards are sufficiently flexible in multiple dimensions. For example, they should include methods for addressing rapidly-changing threats. They should also be responsive to cultural differences between nations and sectors.

Create mechanisms to better integrate current industry needs into curricula.

Consider whether certification or accreditation should play a role in academic cyber security education.

Where a stand-alone cyber security degree is not practical, incorporate cyber security topics into other relevant degree programs. Ensure that graduates of all computer-intensive academic disciplines are "cyber-security literate."

Require NSF grant applicants in relevant fields to include a cyber security/privacy "impact statement" with their federal grant applications that describes how privacy and security issues would be addressed in the intended operational environment (or explain why privacy and security issues are not relevant to the grant request).

CSEWD Suggestion 3: **Create more opportunities for real-world and hands-on learning.**

Potential Approaches

Incorporate coaching into exercises, case studies, and internships.

Facilitate opportunities to work with peers in real-world settings (such as the co-op approach, in which students spend part of their year on coursework and part on an internship) to better understand side effects, unintended consequences, and barriers.

Develop mentoring programs.

Encourage students to take part in (or become familiar with) professional organizations, which provide training opportunities and continuing education.

CSEWD Suggestion 4: **Because cyber security is a rapidly changing field that requires experiential learning and frequent education about new threats, consider alternatives to the traditional university model for providing relevant education.**

Potential Approaches

Explore alternative models of education that require apprentice-style learning (internships, supervised training) and continuing education. (Consider, for example, medical and nursing schools, law schools, apprenticeship training methods, and clerical/rabbinical studies.)

Encourage master's programs to collaborate with 2-year colleges and undergraduate programs to develop preparatory learning tracks, similar to pre-med and 2-year nursing degrees.
Use online education and distance-learning programs to disseminate updates and information about new threats, new techniques, and best practices.

CSEWD Suggestion 5: **Build a coalition of stakeholders to expand support for cyber security education**.

Potential Approaches

Identify cyber security stakeholders and map out their relationships to one another.
Leverage existing technology (e.g., online social networks) to help CSEWD be more nimble in responding to threats and needs.
Create (or improve) mechanisms for industry and universities to work with community colleges and K–12 (e.g., CyberWatch, a consortium of universities and community colleges that share best practices, methodologies, curricula, course modules, and materials and provide faculty training and support; and California's community college transfer and articulation agreement).

ANTICIPATING THE FUTURE OF COMPUTING AND EDUCATION

The "College of 2020"[7] may look very different than traditional universities today. Students may be more ethnically diverse, may have much more flexible schedules, and may use mobile, non-traditional platforms, online learning, and social-network-based approaches to learning. Much coursework in cyber security may be presented digitally. More adjunct professors may be involved in teaching students. Companies such as SANS, Microsoft, and Cisco may provide more training courses, and some universities (e.g., University of Phoenix) may follow their lead.

All education and training approaches should take into account the future of computing, including cloud/distributed computing and sensor-based computing. Efforts should anticipate the need to address big issues, such as large-scale data storage, networking and communication logistics, and privacy. Global perspectives about privacy and security are diverse and changing, and students are already becoming accustomed to being digitally connected all the time. Improving CSEWD (including SFS and IASP) means developing programs with the appropriate foundation and flexibility to anticipate and address the unknowns of the next 10 years.

CONCLUSION

The CSEWD workshop participants developed a number of suggestions for stakeholders to explore as mechanisms to improve CSEWD to meet the pressing need for more skilled workers to address cyber security threats. These suggestions could form the basis for a

larger, more sustained effort to bring together a wide range of stakeholders to determine the next steps.

Workshop participants emphasized that, whatever steps are taken to move forward, stakeholders should document their decision-making so that future generations will understand the rationale for the systems and processes that evolved. Stakeholders, including institutions that currently receive federal grants, should be informed and involved in efforts to improve CSEWD. In particular, it is important to ensure that universities continue to have incentives to participate in SFS.

ACKNOWLEDGMENTS

This workshop would not have taken place without the hard work of several individuals. A steering committee met well in advance of the event and then was involved in a lengthy email exchange to determine and invite the individuals who ultimately attended. That committee was composed of Lance Hoffman, Richard Raines, Eugene Spafford, Susanne Wetzel, Bill Chu, Doug Jacobson, Victor Piotrowski, and Alice Shaffer. Their affiliations are given in the roster of attendees in Appendix 2. Brenda Oldfield of the Department of Homeland Security and Richard Raines contributed as members of this committee but were unable to attend the actual workshop. Gale Quilter Guerrieri ("The Meetings Guru") was in charge of the logistical arrangements. Dana Trevas wrote the first draft of this report. The great majority of the participants responded to that draft with very constructive comments that led ultimately to the final report.

Work on this project was supported in part by National Science Foundation grant 0621334.

APPENDIX 1
Workshop Agenda

WEDNESDAY, October 13, 2010

3:00pm - onward	**ARRIVALS**		
6:00pm – 7:00pm	**DINNER**		
7:00pm - 9:00pm	**PLENARY** PRELIMINARY VISIONS Lance Hoffman, Victor Piotrowski 4 points from each attendee		

THURSDAY, October 14, 2010

7:00am – 8:00am	BREAKFAST		
8:00am – 8:30am	**PLENARY** REACTIONS TO PRELIMNARY VISIONS and SMALL GROUP ASSIGNMENTS		
8:30am - 10:30am	**Working Group 1**	**Working Group 2**	**Working Group 3**
10:30am - 10:45am	**BREAK**		
10:45am - 11:30am	**PLENARY** PRELIMINARY REPORTS BACK by Working Groups *(up to 3 PowerPoint slides)* QUESTIONS AND COMMENTS ON THESE FROM OTHERS		
11:30am - 12:15pm	**Working Group 1 PRODUCE FINAL REPORT**	**Working Group 2 PRODUCE FINAL REPORT**	**Working Group 3 PRODUCE FINAL REPORT**
12:15pm – 1:15pm	**LUNCH**		
1:15pm - 3:15pm	**Working Group 4**	**Working Group 5**	**Working Group 6**
3:15pm - 3:30pm	**BREAK**		
3:30pm – 4:15pm	**PLENARY** PRELIMINARY REPORTS BACK by Working Groups *(up to 3 PowerPoint slides)* QUESTIONS AND COMMENTS ON THESE FROM OTHERS		
4:15pm - 5:00pm	**Working Group 4 PRODUCE FINAL REPORT**	**Working Group 5 PRODUCE FINAL REPORT**	**Working Group 6 PRODUCE FINAL REPORT**
5:00pm – 6:00pm	**BREAK**		
6:00pm - 7:00pm	**DINNER**		
7:00pm - 8:30pm	**PLENARY** EMERGING VISIONS All attendees		

FRIDAY, October 15, 2010

7:00am - 8:00am	BREAKFAST
8:00am – 9:30am	**PLENARY** Reactions to Emerging Visions
9:30am – 10:00am	BREAK
10:00am - 12:00pm	**PLENARY** Identification of Consensus Items; Differing Schools?? Items; and Further Work Items
12:00pm – 1:00pm	LUNCH
1:00pm – 2:30pm	**PLENARY** Development of Roadmap
2:30pm - 3:00pm	BREAK
3:00pm – 4:30pm	**PLENARY** Identification of Next Steps for Stakeholders *(including members of this group)*
4:30pm - 5:00pm	**PLENARY** Closing remarks

APPENDIX 2
Participant List

MEETING COORDINATOR:
Lance Hoffman
Distinguished Research Professor *and* Director
Cyber Security Policy and Research Institute
George Washington University

FOR THE NATIONAL SCIENCE FOUNDATION:
Corby Hovis
Program Director
Directorate for Education and Human Resources, Division of Undergraduate Education

Victor Piotrowski
Lead Program Director
Directorate for Education and Human Resources, Division of Undergraduate Education

PARTICIPANTS:
Bill Chu
Professor and Chairman
Department of Software Information Systems
University of North Carolina, Charlotte

Steve Cooper
Associate Professor
Computer Science Department
Stanford University

Deb Frincke
Chief Scientist, National Security Directorate
Pacific Northwest National Laboratory

Kristen Gates
Executive Director of Education
Team for Research in Ubiquitous Secure Technology

Elizabeth Hawthorne
Chair, Association for Computing Machinery Two-Year College Education Committee
Union County College

Doug Jacobson
Professor
Electrical and Computer Engineering
Iowa State University

Patrick Kelly
Secretary
Cyber Corps Association

David Ladd
Principal Security Program Manager
Microsoft Corporation

Ernest McDuffie
Lead
National Initiative for Cybersecurity Education
U.S. Department of Commerce
National Institutes of Standards and Technology

Gary McGraw
Chief Technology Officer
Cigital, Inc.

Kara Nance
Department Chair
Professor of Computer Science
University of Alaska Fairbanks

Stephen Northcutt
President
SANS Technology Institute

Chuck Pfleeger
Principal
Pfleeger Consulting Group

Angela Sasse
Professor of Human-Centred Technology
Head of Information Security Research
University College London

Alice Shaffer
Recruitment and Grant Coordinator
Information Assurance Scholarship Program Department of Defense/National Security Agency

Gene Spafford
Professor
Executive Director
Center for Education and Research in Information Assurance and Security

Purdue University

Ray Vaughn
Professor
Associate Vice President for Research
Mississippi State University

Susanne Wetzel
Associate Professor
Stevens Institute of Technology

Greg White
Director
Center for Infrastructure Assurance and Security
Associate Professor of Computer Science
The University of Texas at San Antonio

STAFF:
Gale Quilter Guerrieri
The Meetings Guru

Costis Toregas
Assistant Director
Cyber Security Policy and Research Institute
George Washington University

Dana Trevas
Writer, Editor, Rapporteur
Shea & Trevas, Inc.

APPENDIX 3:
Web Addresses

Non-profit organization for security:
Center for Internet Security
http://cisecurity.org/en-us/?route=default

Networking and information-sharing among SFS grantee programs:
Advanced System Security Education, Research and Training Center at the University of Alaska, Fairbanks
http://assert.uaf.edu/index.html

Center for Systems Security and Information Assurance at Moraine Valley Community College
http://www.cssia.org/index.cfm

George Washington University's Cyber Security Policy and Research Institute
http://www.cspri.seas.gwu.edu/

New York University's Center for Interdisciplinary Studies in Security and Privacy
http://crissp.poly.edu/

Purdue's Center for Education and Research in Information Assurance and Security
http://www.cerias.purdue.edu/

Models for consortia and cooperation:
National Institutes of Health's Clinical and Translational Science Awards
http://www.ncrr.nih.gov/clinical%5Fresearch%5Fresources/clinical%5Fand%5Ftranslational%5Fscience%5Fawards/

CyberWatch
http://www.cyberwatchcenter.org/

California community college transfer and articulation agreement
http://www.assist.org/web-assist/help/help-igetc.html

Model for supporting advanced research:
Biomedical Advanced Research and Development Authority
https://www.medicalcountermeasures.gov/BARDA/BARDA.aspx

Creative program to engage students in cyber security:
Cell Phone Forensic Laboratory at the University of Tulsa (described in U.S. Secret Service Fiscal Year 2009 Annual Report, p. 40)
http://www.secretservice.gov/FY09_SecretService_Annual%20Report-Web.pdf

Mechanism for drawing on expertise of retired experts:
SCORE
http://www.score.org/index.html

Related federal programs:
National Initiative for Cybersecurity Education
http://csrc.nist.gov/nice/

Computer & Information Science & Engineering (CISE) program of the
http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13451&org=CISE

Models for flexible learning:
SANS training and certification programs
http://www.sans.org/

Oxford University's master's degree for external students
http://www.conted.ox.ac.uk/courses/index.php

England's Open University network of regional centers
http://www3.open.ac.uk/study/postgraduate/computing-and-ict/index.htm

SANS' Security Essentials Bootcamp Style
http://www.sans.org/security-training/security-essentials-bootcamp-style-61-mid

Stevens Institute of Technology systems engineering graduate programs
http://sse.stevens.edu/academics/graduate/overview/

University of Florida's online education option
http://www.nytimes.com/2010/11/05/us/05college.html?scp=1&sq=dorm%20class&st=cse

ENDNOTES

[1] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, a report to the White House by Melissa Hathaway, Cybersecurity Chief at the National Security Council, May 2009, (p. iii). (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

[2] "Information Assurance", DoD Directive 8500.01E, October 24, 2002 (certified current as of April 23, 2007), http://www.niap-ccevs.org/policy/dod/850001p-E.pdf

[3] Definition of "information security" in U. S. Code (http://www.law.cornell.edu/uscode/44/3542.html)

[4] Congressional Commission on the Advancement of Women and Minorities in Science, Engineering and Technology Development: *Land of Plenty: Diversity as America's Competitive Edge in Science, Engineering and Technology*; September 2000 (p. iii). (http://www.nsf.gov/pubs/2000/cawmset0409/cawmset_0409.pdf)

[5] Note that all web site addresses are listed in Appendix 3.

[6] Cooper et al., 2010, in press. *Towards information assurance curricular guidelines*. Appendix 2.

[7] Chronicle of Higher Education. *The College of 2020: Students* (https://www.chronicle-store.com/Store/ProductDetails.aspx?CO=CQ&ID=76319&PK=N2S10XX)

LANCE J. HOFFMAN
Computer Science Department
The George Washington University
Washington, D. C.
lanceh@gwu.edu

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. His teaching innovations include multidisciplinary courses on electronic commerce and network security and the development of a portable educational network for teaching computer security. He also directs the Department of Homeland Security, Defense Department, and National Science Foundation computer security scholarship programs at GW; these programs have produced over four dozen federal government experts in computer security, all of whom have a working knowledge of privacy as well.

Professor Hoffman developed the first course on computer security in a United States University at Berkeley in 1970 after serving on the Advisory Committee to the California Assembly Committee on Statewide Information Policy. Forty years later, he is still advising government agencies, currently serving on the Department of Homeland Security Advisory Committee on Data Privacy and Integrity. 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 the Center for Democracy and Technology, IBM, and the Federal Trade Commission.

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.