Dakota State University
College of Computing
820 N Washington Ave
East Hall 104A
Madison, SD 57042

Written Testimony from:
Joshua J. Pauli, Ph.D.
Professor of Cyber Security
Dakota State University
Josh.Pauli@dsu.edu
605-256-5181

Senate Commerce Committee: Confronting the Challenge of Cybersecurity (9/3/2015)

Recent DSU Successes

There is much to celebrate at Dakota State University in Madison, SD as our cyber security programs are experiencing explosive growth in both the quantity and quality of student enrollments. Since 2012, our three undergraduate degrees most closely aligned with cyber security, those being Cyber Operations, Network Security, and Computer Science, have seen an 83% increase in students from 382 in the fall of 2012 to 698 in the fall of 2015 as introduced in the table below.

	2012 Fall	**2013 Fall**	**2014 Fall**	**2015 Fall**
Cyber Operations, Network Security, & Computer Science BS Degrees at DSU	382	470	569	698

Approximately 400 of these students are on-campus and account for an estimated 1/3 of the entire on-campus student population of DSU, while the remaining 300 are online students from around the country. Our graduate programs, which include a Masters in Applied Computer Science, a Masters in Information Assurance, and a Doctorate in Cyber Security are also growing rapidly as Dakota State University's reputation for high-quality education in cyber security at a reasonable price continues to expand across the country.

Much of this student growth at DSU can be traced back to three main milestones. First, DSU was awarded a grant from the National Science Foundation (NSF) in 2011 to join the CyberCorps SFS program to award full ride scholarships and stipends to high-achieving students that are interested in working for the government in a cyber security position after graduation. 44 DSU students have been awarded this scholarship and we've placed 100% of our interns and graduates in government positions around the country.

Second, DSU's Cyber Operations undergraduate degree program was designated as a Center of Academic Excellence in Cyber Operations (CAE-CO) by the National Security Agency (NSA) as one of the first four such Centers in 2012. This is a very exclusive honor for DSU as there are currently only 14 designated programs in the nation. Less than 25% of university applying to the CAE-CO program meet the stringent requirements for this designation and DSU is widely viewed as one of top Cyber Operations programs in the nation by the government and academic communities alike for our deeply technical focus and hands-on approach.

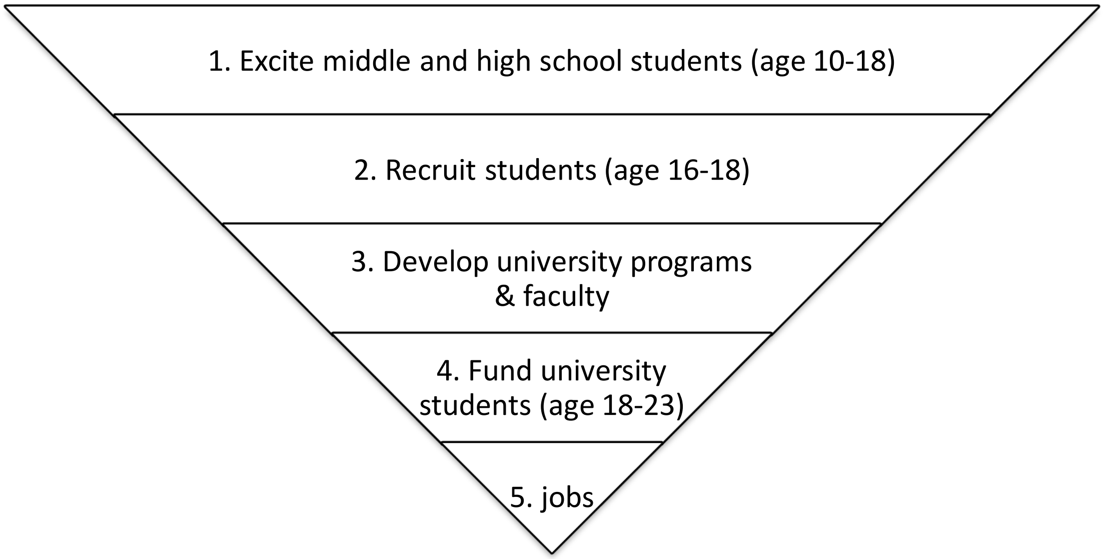
Third, DSU entered an academic articulation agreement with the NSA in 2015 to award DSU academic credit towards our Cyber Operations undergraduate program for education and training that NSA employees, primarily military personnel, complete as part of their work at the Agency. This articulation agreement is the first such agreement in the history of the NSA and will enable these employees to be retained by the NSA or Department of Defense (DoD) after graduating from DSU. This is also likely the first such agreement by any Federal Government agency dedicated to cyber security education, which has huge potential for all agencies to help attract and retain top cyber security graduates.

Current Threat

Despite the good news at DSU and the focus of many academic, government, and professional organizations on cyber security threats today, I believe the United States would lose a cyber conflict between nation states if it took place today. My worries go beyond the data breaches that have dominated the headlines in recent months, but instead extend into the military, intelligence, and business competitiveness arenas of our country. We have an extreme shortage of qualified professionals in the cyber security domain across both public and private sectors. We must greatly expand the quantity and quality of the cyber workforce to ensure the necessary knowledge, skills, and abilities are in place to help protect the nation and conduct cyber operations. We can help solve this capacity problem with existing programs that have already proven to be highly effective and successful as partially discussed in my testimony of S. 1353: Cybersecurity Enhancement Act of 2014.

The Way Ahead

To meet the cyber security personnel needs in public and private sectors, we must increase the numbers in every stage of the process in order to end up with a tangible increase in the number of qualified professional. The funnel introduced below is an accurate representation of the processes that must occur when trying to grow the cyber workforce.


1. Excite middle and high school students (age 10-18)
2. Recruit students (age 16-18)
3. Develop university programs & faculty
4. Fund university students (age 18-23)
5. jobs

1. Excite Middle and High School Students (Age 10-18)

We must increase the funding to the GenCyber Summer Camp program that has been offering cyber security summer camps to middle school students, high school students, and K-12 teachers since 2014 on university campuses around the nation. GenCyber is a joint effort by NSF and NSA that administered 43 camps at 29 universities in 18 different states during the summer of 2015 that supported approximately 1,500 students and 300 teachers. The student population was 50% female, which is a dramatic increase from the 18% of females that enter computer science programs at the university level. GenCyber has been a tremendous success despite never having dedicated funding from the NSA or

NSF in the last two years. It has only been funded by “left over” funding. In order to expand GenCyber, and other similar programs with the goal of increasing student interest at a young age, dedicated funding and programs need to be established. Expansion of this program should also include year-round programming for interested students by the way of after-school programs, college-level courses, and other engagements integrated into the academic year of middle school and high school students. This education of young minds is critical in order to increase the quantity of students that at least consider going into a cyber security field of study at the university level. Programs like GenCyber are the entry point to the funnel, thus it needs to pull from a very wide audience of students and teachers.

2. Recruit Students (Age 16-18)

Direct recruitment of high school students to university programs is not a formal aspect of GenCyber as the camps are 100% about cyber security education and to excite students to pursue cyber security educational and professional pathways. Any recruitment is secondary to the goal of the camps and only happens organically. We need to develop a formal recruitment plan for students that is overt in its mission and can be scaled nationwide. I believe this is an excellent project for NIST’s Security Outreach and Integration (SOI) Group and the National Initiative for Cybersecurity Education (NICE) to work alongside universities and government agencies to develop a “full court press” approach to recruiting students directly into cyber security academic programs and career pathways. With the support of NIST, NSF, GenCyber, and universities around the nation, a recruitment plan to target this population would further widen the audience of upcoming cyber security professionals.

3. Develop University Programs and Faculty

Our university programs must continue to grow and evolve in order to keep up with the demands of the professional workplace and the incoming students. While there are capacity building funds attached to various grant programs, the current level of support must be increased to support more academic programs in additional ways. NIST's National Initiative for Cybersecurity Education (NICE) is an ideal mechanism to provide additional resources into the ongoing development of our programs and faculty around the nation. The NICE Workforce Framework is a tremendous effort to identify and classify the necessary knowledge, skills, and abilities (KSAs) that are required in today's cyber security workforce. Now is the time to take this same framework and provide assistance to educational institutions to ensure our programs and faculty are positioned to implement the framework.

An existing mechanism within the Department of Defense (DoD) that needs to be mimicked across the nation is University affiliated Research Centers (UARCs) that enable a closer working relationship among government agencies, university faculty members, and university students. UARCs are very similar to Federally Funded Research and Development Centers (FFRDCs) in that an external entity, such as a university or non-profit corporation, conducts research and development for the US Government. It's now time to have such Centers dedicated to solving the problem of attracting and educating the next generation of cyber security professionals. These Centers would be the hub of activity for government agencies, universities, and high schools across the nation to support the mission of increasing the quantity and quality of cyber security professionals.

Currently the only Department of Commerce FFRDC is the National Cybersecurity Center of Excellence (NCCoE) that is dedicated to cyber security best practices across critical infrastructures, but multiple Departments of the US Government can sponsor an FFRDC, so the Center can conduct research for both Departments. There are many moving parts to such an endeavor, but we must better identify and coordinate our efforts to cyber security recruitment and education and UARCs and FFRDCs are a great approach to this coordination.

4. Fund University Students (Age 18-23)

NSF is the source for 89% of all federal funding to computer science and cyber security at our universities, so we look to the NSF as almost the sole source of federal funding to our programs. The NSF's CyberCorps SFS program is widely viewed by government and academia alike as the most effective way to place top students in cyber security careers within the government. The program has achieved the rare feat of gaining positive endorsements from government agencies, university faculty members, and scholarship students alike. CyberCorps SFS has supported 1,750 students since the programs inception in 2002 and approximately 200 new students per year, which is a drop in the bucket compared to the need we face. The NSF's Graduate Research Fellow (GRF) program, which spans all academic disciplines and is the NSF program CyberCorps is most commonly referenced with, supports 2,000 students per year. The CyberCorps budget for 2015 is $45M, which is 0.62% of the NSF's $7.7B 2015 appropriation and just 13.5% of GRF's 2015 appropriation. An increase to the CyberCorps program is a wise investment for the future of cyber security professionals within government agencies.

5. Place Students in Internships and Graduates in Careers

Any efforts to continue to streamline the hiring process of student into internships and graduates into careers is greatly appreciated by everyone involved. Continued work on raising salaries for the most critical cyber security positions in all government agencies is also a positive step forward and should continue. It's unrealistic to expect government jobs to keep pace with private sector pay, but it must at least be close enough for the student to consider accepting the government position. Often times the application and hiring process is by far the worst experience for students and graduates. These delays also result in government agencies missing out on students and graduates that actually want to work for them, but get hung up during the hiring process. This is a topic that has received discussion for several years between academia and government, but should continue to be researched for a way to make the process better on an on-going basis.

We must also find better ways to get students who are not CyberCorps scholars placed at government agencies. As an example, DSU has 10 new CyberCorps students per year, but realistically has 20-25 students that deserve the scholarship and another 20-25 students per year that would make perfectly capable hires into government cyber security positions. But because the process is so convoluted and slow, these 50 non-CyberCorps students can not get noticed by government agencies and are forced to take jobs, often times lesser jobs, outside of government. There are countless students around the nation who would gladly work for the government, but they are so turned off by the hiring process that they don't even consider public service.

Conclusion

The demand for cyber security professional is only going to increase in both public and private sectors. We need to act now to help fill this demand with the types of graduates that are well prepared for the workplace of the coming years. Although there is much work to be done to generate the quantity and quality of the cyber workforce, there is a proven plan to achieve noticeable progress towards this goal. Now we need to execute this plan.

Respectfully submitted,

Joshua J. Pauli, Ph.D.
Professor of Cyber Security
Dakota State University
Josh.Pauli@dsu.edu
605-256-5181