Senate Commerce Committee Hearing
Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown
July 11, 2018

Written Testimony of José-Marie Griffiths
President, Dakota State University
Madison, South Dakota

THE PROBLEM

We have grown accustomed to attacks on computer systems that exploit the inevitable flaws resulting from vast conceptual complexity. Our computer systems are the most complex artifacts ever built, and the growth of complexity has far outstripped our ability to manage it. The problem is that we now live, breathe and have our being within a cyber universe driven by a critical and vulnerable multi-dimensional infrastructure. These dimensions include the vast range of products, providers, demands for increased proficiencies, the pervasiveness of cyber, and the enormous number of people now interacting with and dependent on our technology systems.

PRODUCTS

The products of our cyber systems are muti-layered and varied, but generally they fall into one of the three tiers of hardware (the computer), firmware (permanent software programmed into the read-only memory of the computer), and software (applications loaded onto the computer). We have grown used to cyber attacks occurring at the software level.

However, Meltdown and Spectre were unusual in that they exploit flaws in the design of the complex interaction between the three levels of cyber products, and especially processes in the firmware, code that comes embedded in hardware devices. Cyber vulnerabilities in firmware are not only much harder to prevent or detect but also in most cases, unavailable to mitigate or remediate. The shock of the threat from this newly identified class of vulnerabilities comes from the sheer number of devices they impact and how persistent they will be over time.

A specific piece of application software can be removed from a computer and other applications on the machine will continue to work. Some firmware can be replaced but firmware can never be entirely removed; without firmware code the hardware will not function. Changing the firmware of a cyber device may rarely or never be done during its lifetime; some firmware memory devices (especially Internet of Things devices like kitchen applicances or home security systems) are permanently installed and cannot be changed after manufacture. There are millions of diverse devices now in use across the planet with a wide variety of firmware embedded in them. Full protection can only come from replacing vulnerable equipment with new devices that contain fundamentally more secure chips and components. This replacement process will take years and will primarily depend on the devices' eventual retirement or demise. In the meantime, many devices will remain exposed to these niche, but potentially effective, cyber attacks.

PROVIDERS

No matter how you count them, there are many thousands of hardware/firmware providers globally and they compete fiercely. Third-party smaller specialized providers often operate with slim profit margins and are forced to cut corners to lower prices. Most smartphones have components from at least 10 different companies in as many countries. The screen, battery, microphone, camera, etc. – each requires highly specialized design and manufacturing. No one company – or country – can competitively produce more than a few of them. The Heritage Foundation, in their report on cyber supply chain security, noted that "Increased demand has led to acute competition and, consequently, more outsourcing and innovation to

lower costs and remain competitive. This can be seen in the U.S. computer manufacturing sector, which over the past five years has declined at an annual rate of 21.8 percent as computer manufacturing has increasingly moved abroad….the expanding market for computer products, innovative and useful software applications, and faster chip designs means that even these industries are seeing international competition and outsourcing that will likely grow over time."

The vast majority of users have no idea of the component makeup of a technology device, much less who made the piece or where. When users send a text, very few question who made the modem their smartphone is using to send it. However, the design and production of every piece of technology comes with certain goal and value choices. Is the goal of a company – or a country supporting that company - merely to manufacture and deliver a component piece of hardware and be done with it? Or is the goal of the company to embed within that piece of hardware the ability for the company – or country – to surepetiously maintain access to that device, its user and activities, on an ongoing basis, using that information to further its own endeavors? The Internet of Things is exponentially expanding the number of cyber devices we rely on, from crockpots to cars. The computer screen on a fridge – are those in the home assuming that the device is built with a value of privacy for what goes on in someone's kitchen that the manufacturer doesn't share? Very often the users of a cyber device have very little understanding of its full capabilities. Recently a user who had installed an Internet-connected video doorbell in his home was amused by the actions of a delivery man who clearly did not understand the ramifications of the device. The user had a pleasant conversation from work over his smartphone connected to the home doorbell video cam, instructing the delivery man where to leave his packages. The delivery man dutifully did so, and then, apparently unaware that the user could still see him, walked over to the side of the house, dropped his pants, and urinated on a retaining wall. The delivery man's assumption of privacy was not shared by the device's design and functionality.

PROFICIENCIES
We want our technology to be fast and faster, tuned to the vagaries of our personality, workstyle, activities and preferences, and easy to use. The less we have to figure out or do to make it work, the better. But every added cyber proficiency comes with a set of decisions made by someone about access, privacy, control, and more. Autonomy means freedom from the will of another. But every autonomous device is based on a set of assumptions defined and built in by someone. Do we know – or care – who that someone is, and the basis for their choices and assumptions?

PERVASIVENESS
Cyber devices are now embedded in almost every aspect of work and play, and thus we are now facing serious vulnerabilities in our supply chain. Rapid technological advancement and the constant rush to market with added functionalities has resulted in complex and sophisticated integrated circuits now virtually ubiquitous in every device, in every country. They are relied on to control critical infrastructure subsystems such as power, finance, communications, transportation, healthcare and agriculture.

In the past, attackers worked to exploit security gaps that might exist in corporate of national defense IT systems, today the gaps they are exploiting are in the integrity of the supply chain. As the threat landscape evolves, it is essential for an effective supply chain security strategy to proactively minimize exposures throughout the lifecycle from cradle (secure integrated circuits (IC) design, fabrication and manufacturing) to grave (ethical e-waste disposal) and everything in between. Modern IC computer chips are enormously complicated. For example, an average desktop computer chip has over 1 billion transistors. In addition, the manufacturing process is not entirely predictable and there can be significant variances in the chips produced. The complexity of both design and production create multiple opportunities for practically undetectable cyber infections at the very beginning of the supply chain.

Cyber systems are increasingly complex and the dependency on third party libraries of software code in the supply chain seems to be growing. For example, most of today's integrated circuits use at least some common off-the-shelf components (COTS), mostly in the form of third-party intellectual property. This should be considered a top security issue because much of it is integrated into the chip as trusted code, regardless of whether it actually is. As the Internet of Things/Everything, Cloud of Everything (IoT/E, CoT) evolves rapidly to be autonomous and inexpensive, the use of COTS will expand even more dramatically and the need to encapsulate this potential security risk will be even more pressing. Security issues with COTS include undocumented or unverified code and sloppy programming that opens devices to intrusion. This makes it very difficult, if not impossible, for an organization to test all of the software code they actually use and potentially ship to a client. There have been several notable supply chain incidents of companies unknowingly distributing malware with dire impacts. However, it is not at all clear where the responsibility for ensuring safe software code lies. Is it the obligation of the third party company or the company or organization that used and distributed dangerous code? And who decides? We do not yet have best practice guidelines for these types of issues, but they are far overdue.

The risk of dangerous firmware can be the most difficult to defend against. Firmware is embedded in hardware and can be put there either at the point of creation or at some other stage as it moves through the supply chain. This malevolent code can be extraordinarily difficult to detect. Some contain logic bombs that are set to go off at a designated time in the future, or only when a certain event occurs to trigger them. There is great potential for this malicious code to be used to damage or destroy key components of critical infrastructure, which could result in high economic costs or even political turmoil.

The only way to ensure absolute cyber safety would be able to ensure that the entire supply chain of relevant electronic components occurs in the United States and is performed by carefully screened and vetted, trustworthy employees. The system would need to include all stages of the supply chain from design, creation, fabrication, assembly, to distribution. Strict surveillance of the manufacture of such electronics would need to occur, and protocols would need to then be in place to ensure that no modifications have been made and that the electronics are created exactly to specifications. Unfortunately, this is simply not pragmatic as the costs of having to do all of this, including manufacture, would be astronomical and unsustainable without years of public investment. Presently most cyber device manufacturing occurs in Asia at very inexpensive rates. U.S. tech firms would never be able to compete in a world market. Furthermore, because most electronics are created, assembled, and distributed outside the this country, U.S. government regulated security processes would be irrelevant for the vast majority of the supply chain.

The statistics of the pervasiveness of cyber today are staggering. There are currently more than 8 billion connected devices globally, according to a new report by IHS Inc. That works out to four devices for every household in the world. As of 2014 there were more cyber devices than people in the world, including a growing number – about 250 million – that only communicate with other machines. And all of these devices are multiplying five times faster than the human population is (a rate of about two people per second, or 1.2 percent annually). Over 3.8 billion people use the internet today, which is 40 perent of the world's population, and we are busy users. OMG, a website design and online marketing company published a set of technology facts and stats that includes: "More than 570 new websites are created every minute; there are over 3.5 billion searches per day on Google; every minute 24 hours of video is uploaded to YouTube; more video content is uploaded to YouTube in a 60-day period than the three major U.S. television networks created in 60 years; 340,000 tweets are sent per minute and 500 million tweets are sent per day; there are more than 300 million photos uploaded to Facebook every day with 800 million likes per day." Not only are cyber systems becoming more complex, that complexity is multiplied millions of times over by the pervasiveness of their presence.

PEOPLE

The human element of the problem is perhaps even a greater challenge than the number of devices involved. Getting users to click on automatic software updates has only ever been marginally successful, even when enormous efforts are made to reach those users and explain the importance of the update in protecting their machine and data. The human element in the mix can extend the lifecycle of exploited vulnerabilities, not only through noncompliance but also value tradeoffs. For example, users sometimes decide not to install patches and updates if a side effect of the protection is a hefty performance degradation. Some of the initial firmware code distributed to address the Spectre/Meltdown vulnerabilities resulted in machines refusing to boot up and others slowing down by as much as 30 percent. These problems were quickly resolved, but they demonstrate the risks and challenges of fixing complex system problems. To explore potential impacts of running non-remediated software, researchers recently set up a set of computers, each running a different operating system software, many no longer the current version. They then connected the machines to the Internet and monitored how long it took before the machine experienced a successful cyber attack. One machine running (outdated) OS software still in use in over 80 percent of large corporations lasted only 13 seconds before experienced a cyber attack and was compromised. Writing replacement non-vulnerable firmware code and getting it installed in every existing device that needs it around the world is even more challenging. Meltdown and Spectre exposed hardware/firmware design assumptions that were reasonable when they were created. However, technological sophistication and knowledge has now developed to the point that the basic firmware approach and architecture can now be exploited to trick the computer into revealing sensitive data, like user names and passwords.

After the Spectre and Meltdown vulnerabilities were discovered, researchers anticipated that similar flaws would eventually be revealed as well, and that has happened recently. New categories of security exploits often follow a predictable lifecycle, which can include new derivatives of the original exploit. Sometimes the fix for these derivatives benefits from the fixes created for the original exploit. However, it also complicates and extends mitigation and remediation. IT professionals have often likened this to the "whack the mole" game: no sooner is one security breach beaten down but a new one erupts through a different hole.

POTENTIALS

Within this grim problem context, what are the potentials for fixing the problem? I believe that in the U.S. we have the people and organizations who can design and implement protective strategies and tactics to keep us safe. But we need both carrots and sticks.

We need articulated standards, guidelines and best practices. These are the floor not the ceiling, but it's a good start. The collaboratively-developed and public NIST guidelines are far more effective than what we saw when Spectre/Meltdown was discovered: corporations circling the wagons, hiding what was going on and trying to fix it by themselves. That was not totally a self-serving move – you don't want adversaries to know your flaws before your fix – but it also showed that we need best practice established standards, participants, and processes for responsible coordinated disclosure. An increasing number of organizations are developing and adopting formal or informal vulnerability disclosure programs. Formalized programs include published policies describing how information about security vulnerabilities will be received and addressed, and how vulnerabilities may be disclosed to affected parties and/or the public. These policies may also describe authorized methods for discovering vulnerabilities in the organizations systems, services and products and how – and how quickly – a component vendor must respond. For example, Google's Project Zero gives vendors 90 days to respond and implement a fix before Google goes public with a vulnerability that they discovered. This puts the pressure on the vendor to respond, and in a timely manner. The Cybersecurity Unit of the Computer Crime and Intellectual Property Section, Criminal Division of the U.S. Department of Justice has recently published *A Framework for a Vulnerability Disclosure Program for Online Systems* which provides an excellent starting point for organizations to develop their own programs. Coordinated vulnerability disclosure is most likely to minimize risk to technology users.

Vulnerabilities privately disclosed and fixed through coordinated disclosure practices by all software vendors appear to work best. They do not create panic by early disclosure without solutions and do not alert criminal elements of current vulnerabilities. The balance between early public disclosure and tested solutions is tenuous at best. However, coupled with a clear and consistent messaging, the potential damage can be minimized.

Who to do this? The country needs to identify a strong leader to take control of planning and response; coordinate with others and avoid the almost universal aversion to admitting weakness. Clarity and consistency in messaging are important but must be tailored to different audiences.We need to pull together and structure government, corporate, and academic/research oversight and engagement in cyber security. And from those collaborations we need a system of rewards for good cyber citizens and punishment for rogues.

We need best practices for building secure products. Given the conceptual complexity of today's computer systems, perhaps the ultimate solution would be the automated evaluation of designs with the aim of mathematically proving that under all circumstances a design will behave in a way that is considered secure – in particular by not leaking secret data. This is a long range project but significant improvements could be achieved through partial results in the form of weaker properties and by establishing desired properties in a less rigorous fashion. A necessary and long-overdue first step is a new and improved hardware-software contract. Both sides need to work to an interface – the instruction set architecture which presents the contract between hardware and software functionality, and it must be adequately specified for ensuring security.

We need a far more comprehensive and robust cyber education system in this country, both to develop professionals and increase the cyber knowledge of the general population. And that educational program must include consideration cyber ethics and commitment to individual and corporate responsibility and societal cyber participation. Traditional university computer science programs tend to not delve too deeply into software development, let alone secure software development. While the trend seems to be changing, this has created a significant security skills gap in the current cyber workforce. Organizations are struggling as to how to address this with their current workforce. It is often difficult for a company to readily identify the skills of their employees to address gaps in organizational cyber security skill and systems.

We also need much better publicly required and shared cyber knowledge. The FDA requires that food manufacturers list a product's ingredients and its country of origin. Reading labels I can make an informed decision - is the less expensive brand worth it if it is full of chemicals and preservatives, or comes from a country whose values the buyer opposes? We have no such listing requirements for the technologies we buy. Why not?

PROPERTIES

Problems and potentials lead to where the rubber meets the road – the needed properties and resources to move forward. We must leverage this country's intellectual assets, especially the human capital in U.S. universities.

Dakota State University (DSU) in Madison, South Dakota, was founded in 1881 and is a public university in the state South Dakota university system. In 1984, a remarkably prescient South Dakota state legislature decided that South Dakota needed to dive in to the technology revolution, and DSU was the educational institution to lead the way. DSU has developed into a powerhouse school of technology-intensive and technology-infused undergraduate through graduate degree programs. DSU's Beacom College of Cyber and Computer Sciences, one of its 4 colleges, has over a thousand students studying cyber defense; secure software development and engineering; computer science principles and best practices; and the

ethical and social issues of technology use. DSU has multiple Academic Center of Excellence designations in education, research, and regional resource development from the U.S. National Security Agency and Department of Homeland Security. The university's cybersecurity students have competed and won notable national titles against universities ten times DSU's size. The university continues to graduate an impressive stream of much-in-demand tech savvy professionals, who have landed jobs in top government, education, and business and industry organizations, nationally, and internationally. Small in size, DSU has become a big player in cyber workforce development and research and development.

DSU has developed the Madison Cyber Labs — MadLabs — a cyber research hub of research clusters that leverages the "mad skills" of our faculty, staff and students in collaborations with government and corporate partners, from local and area partners all the way through federal agencies. The MadLabs is a reproducible model of using the intellectual resources of a university to engage in product and penetration testing; vulnerability assessments; and detection, remediation, and mitigation tool development. Ten clusters across multiple disciplines – and more planned - combine disciplinary and cyber experts for targeted innovation. Present MadLabs labs and institutes include:

- **Cyclops Lab** (Cyber Classified Operations) The Cyclops lab is a secure facility for the conduct of classified, sensitive and confidential research and development. Cyclops is working federal agencies and private corporations on multiple cyber security projects.
- **PATRIOT Lab (Protection and Threat Research for the Internet of Things)** The PATRIOT Lab is focused on the security of the devices and related cloud services that comprise the Internet of Things (IoT). The structure and nature of IoT devices may make them an important vector for malicious attacks and the Patriot Lab researches and develops solutions for these vulnerabilities.
- **FinTECH Lab (Financial Technology**) The mission of the FinTech MadLab is to develop software and processes that support the security and reliability of the financial services industry. Initially, this will include addressing Automated Clearinghouse (ACH) fraud and wire fraud but will expand to many financial transactions. The FinTECH MadLab will support the traditional financial platforms and emerging technologies such as Block chain, digital currency and online platforms. An industry advisory board will guide the development of this MadLab.
- **DigForCE Lab (Digital Forensics for Cyber Enforcement)** The digital forensics MadLab is a resource for government agencies, businesses and attorneys that have a need for the extraction, preservation and analysis of data from digital devices. This includes data from traditional devices like computers and phones and non-traditional devices such as gaming consoles. The digital forensics MadLab will also provide staff training for various organizations

and a state-wide call center for businesses and individuals to use for cybersecurity questions and analysis including a safe way of forwarding suspect email, files and documents.

- **Campus IT Living Lab (DSU's IT infrastructure protection and related research)** The Campus IT Living Lab performs testing on technology hardware and software solutions to determine if the solution can be implemented in a campus environment. Some of these areas include IT infrastructure, classroom multimedia, and facilities. Utilizing the Campus Living IT Lab, Information Technology Services (ITS) will collaborate with DSU faculty and students on projects to determine the viability of different technologies in a campus environment.
- **CAHIT (Center for the Advancement of Health Information Technology)** The mission of CAHIT is twofold: First CAHIT intends to research the interplay of "aging in place" and the Internet of Things (IoT). Secondly, CAHIT will address the unique security concerns of connected medical devices, both in the home and in medical institutions. CAHIT will utilize their existing industry partnerships and their strength in information security and information analysis in developing their research proposals.
- **AdaptT Lab (Research in Adaptive Technologies)** Working collaboratively in teams the AdapT Lab researchers work to creatively explore, develop, test and modify real-world assistive technologies that can be used to break through barriers, digital or physical. We are also committed to educate others to become knowledgeable and skilled in using and developing assistive technologies in their fields, to increase employment and life participation for those experiencing disabilities or constraints.
- **C-BAR Lab (Center for Business Analytics Research)** The C-BAR MadLab is a research and analysis platform for the College of Business and Information Systems (BIS). The goal is to make the expertise of BIS faculty available to businesses organizations, education entities, and government agencies to assist with their projects and apply analytics to assist in solving problems.
- **Cyber Education and Teaching Technologies Lab** The mission of the Education MadLab is to expand Cyber Education to K-12 teachers and students across the state of South Dakota. The lab will utilize DSU faculty to provide this education within the K-12 districts and on the campus of DSU. The Education MadLab is partially funded by an NSA grant supporting DSU as a Regional Resource Center.
- **CybHER Security Institute (Women in Cyber Security)** CybHER's mission is to empower, motivate, educate, and change the perception of girls and women in cybersecurity. By providing resources for girls from middle school through collegiate programs and into professional careers, CybHER will allow women to foster positive and encouraging relationships within this industry through original and curated content that educates and motivates women. Ultimately, our goal is to increase diversity by introducing more girls to cybersecurity, who will then transition to women in collegiate programs, and highly trained professionals.
- **CLASSICS Institute (Collaborations for Liberty And Security Strategies for Integrity in a Cyber-enabled Society)** The Mission of the CLASSICS Institute is to raise the deep questions about the cyber revolution including those related to: Artificial Intelligence (AI); Security; Privacy; Integrity; and Ethics. The institute will consider these issues in the context of how they relate to public policy.

Across U.S. universities we have the potential to develop a nationwide distributed force that could be mobilized to address initial vulnerabilities and test solutions through multiple disciplines.

We must increase cultivation of a cyber workforce. The shortage of skilled cyber professionals is seriously impacting the ability of organizations – and federal and state government – to protect our cyber resources. As of next year, 2019, it is expected that there will be more than 2 million unfilled cybersecurity

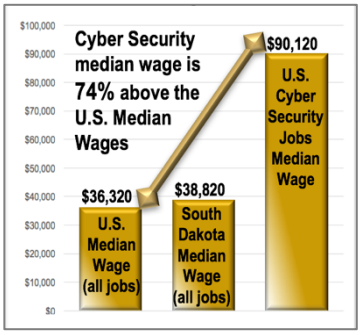
jobs in the world. Eighty-four percent of U.S. companies reported that half or fewer of applicants for their cyber security jobs were qualified. The talent pool of cyber warriors is not keeping up with the growing pace and severity of cyber warfare.

Across the country and the world, increased education is associated with both higher wages and lower unemployment. The greatest barrier to U.S. economic success and growth in the 21st century will be a workforce dominated by those without post-high-school education. Research shows that technology-centric professionals and endeavors — Dakota State's mission focus – have an outsized impact on economic growth, because they provide better-paying, longer-lasting jobs than other start-ups, and they contribute more to innovation, productivity, and competitiveness. There are significant differences between tech-based start-up companies and the typical start-up companies:

Firm Characteristics	Tech-Based Start-Ups	Typical Start-Ups
Examples of Businesses	Biotech, IT products or services	Restaurants, laundromats
Growth Path	Large potential for significant employment and revenue growth	Addition of few jobs in first few years, then bankruptcy
Job Creation	Tend to employ more high- and semi-skilled workers	Tend to employ more semi- and low-skilled workers
Wages	Pays more than twice the national median wage	Pays less than the national median wage
Job Multipliers	Creates up to five indirect jobs in other industries	Creates little to no net new jobs
R&D Investments	Invests heavily in R&D	Little to no R&D investment
Trade	Focused on trade with international markets	Sells predominately in local markets

https://itif.org/publications/2017/11/28/how-technology-based-start-ups-support-us-economic-growth

The Information Technology and Innovation Foundation, ranked as one of the world's leading science and technology think tanks examined the top ten tech-centric manufacturing sectors and services in terms of their contributions to the U.S. economy. They found that across the board tech firms contribute to the economy and economic growth of a region far beyond their comparable size. One tech job generates at least 5 other jobs in the community. For example, while only 3.8 percent of U.S. companies are tech-centric and they account for only 3.6 percent of U.S. jobs, these companies account for 27.2 percent of U.S. exports, critical to business success in the new global economy. The importance of STEM professionals as key to economic success continues to grow. 66 percent of all DSU degree- and certificate-seeking students are in STEM programs. It is interesting to note that according to the U.S. Bureau of Labor Statistics, nationally seven out of the largest ten STEM occupations are technology-centric.



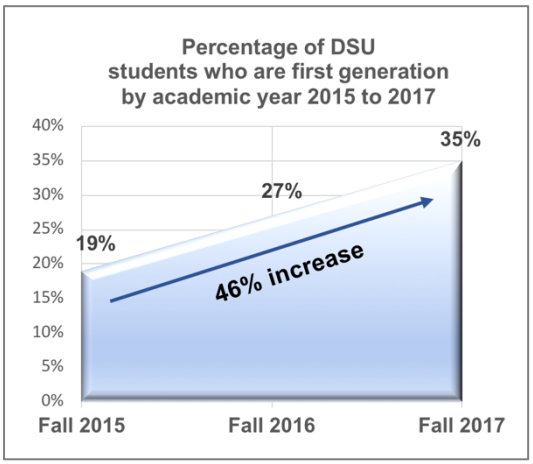
DSU's surging enrollment reflects an understanding that tech professionals are in demand and the jobs are good – good working conditions, high salaries, and stable employment. However, unless grant and scholarship funding is increased – significantly – for all of the country's high school graduates, this trend will not be sustained. Three factors are especially indicative at DSU of the increasing need for additional funding for students to complete a college degree: dropping Pell grant recipient numbers; the number of students qualifying for subsidized loans compared to the number receiving South Dakota's state-funded needs-based scholarship; and the increasing number of first-generation students.

The Pell Grant program is an indicator of the number of students from lower income families pursuing a college education. According to the Free Application for Federal Student Aid (FAFSA), most Pell grant money goes to students with a total family income below $20,000. The maximum Pell Grant award in

2016-17 in the U.S. covered just 29 percent of average in-state public university tuition, fees, room, and board. This is in stark contrast to the Pell Grant award in 1997-98, when the award covered 87 percent of average in-state public university tuition, fees, room and board. This means that at a time when young adults more than ever need a college education to access a good job and the U.S. needs a college-educated workforce to stay competitive and sustainable, federal support has gone from covering almost all of the cost of a college education to covering less than a third. These days qualifying for the maximum Pell Grant award doesn't even get a student half way to covering the expense of their degree.

DSU's percentage of Pell grant recipient students (as a percentage of the entire student headcount) has dropped 8 percent in the last two years, and we expect that trend to continue. According to the College Board, in 2016-2017 32 percent of U.S. college undergraduates were receiving Pell grants. The conservative estimate is that 50 percent of high school graduates in 2015-2016 would have qualified for a Pell grant. When even the maximum Pell Grant only gets a student a little more than a third of the way to paying for their schooling, many young adults are discourage from even attempting to finance a college education.

Another indication of the growing financial need of college students is the number who qualify for subsidized loans versus those who receive monies from state-funded support, for example the South Dakota Needs-Based Scholarship Fund. Federal recipient qualifications for subsidized loans are based on the student's available resources, which includes a calculation of their Estimated Family Contribution (EFC). Subsidized loan qualification thus does identify those students who most likely come from lower-income homes. Two years ago, 758 DSU students from South Dakota qualified for subsidized federal loans. However, there was only enough money in the South Dakota Needs-Based Scholarship Fund to provide scholarship monies for 21 of those 758 students, or a minute 3 percent of those who likely qualified actually received state-funded support for their education. Many states across the country are in even greater more dire straits trying to provide support for students' higher education, especially following the dramatic cuts in state budgets during the recent recession.

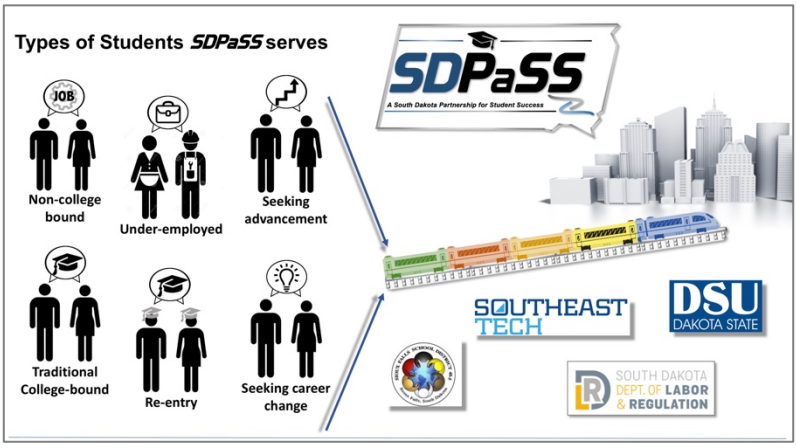


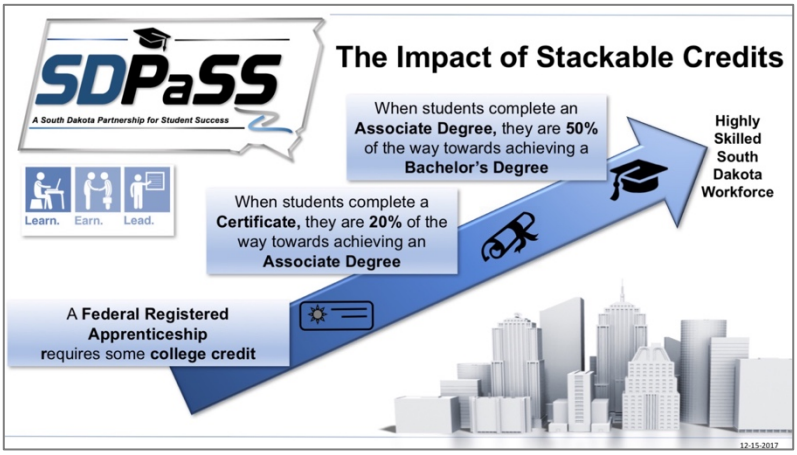
Dakota State is indicative of those universities that are working hard to recruit and retain first-generation students, those who are the first in their families to obtain a college degree. From Fall 2015 to Fall 2017 DSU's population of first-generation students has increased 46 precent.

While certainly not all first-generation students qualify for need-based support, according to the Economic Policy Institute "Americans with no more than a high school diploma have fallen so far behind college graduates in their economic lives that the earnings gap between college grads and everyone else has reached its widest point on record." Those holding only a high school diploma have actually seen their average salary decrease by an average of 3 percent. There are nearly 1.5 million fewer office administrative and clerical jobs now than there were before the recession, according to an analysis by Georgetown's Center on Education and the Workforce. Manufacturing employment is also 1.5 million lower than when the recession began in 2007. The construction industry had offered a lifeline to many high-school educated workers, particularly men, during the housing boom in the 2000s. Yet construction now employs 840,000 fewer people than it did nine years ago. Since the recession, the fastest-growing industry for high school-only grads has been a mostly low-paying sector that includes restaurants, hotels, and amusement parks, according to Georgetown's analysis. Therefore, it is a reasonable conclusion that generally first-generation students will have a significantly lower EFC than non-first-generation students and need more financial support to obtain a college degree.

South Dakota has set the ambitious goal of by 2025 to have 65 percent of the state's under-35 workforce have some post-secondary education. The state has launched *SDPaSS*, the South Dakota Partnership for Student Success, a system of step-wise stackable cyber education programs and credentials that make it easier for high school graduates to continue their education and qualify for higher skill better paying jobs while meeting the needs of companies for cyber professionals. Those already in the workforce can access *SDPaSS* to retool or advance their career. A layered educational program ensures that achievement at one level, e.g., obtaining a professional certificate, is acknowledged and the course work directly flows into the requirements of the next academic level, e.g. an associates degree. The four core partners – Dakota State University, Southeast Tech, the Sioux Falls School District, and the South Dakota Department of Labor and Regulation (DLR) – are collaborating with businesses to design, refine, and implement the program. This collaboration is essential to ensure that the program stays relevant to evolving commercial trends, cyber innovations, and workforce needs. *SDPaSS* components include:

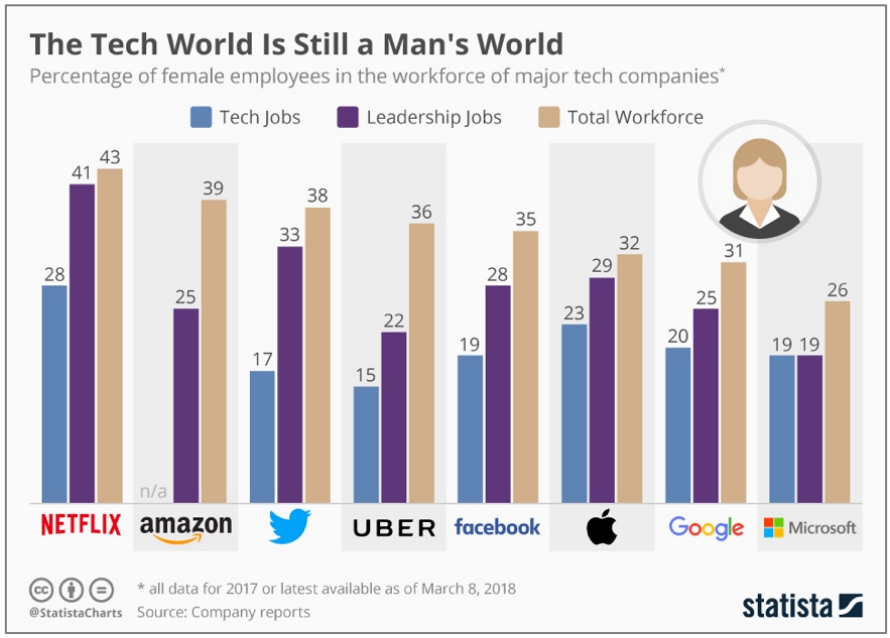
- Internships in business/industry supervised by faculty at Dakota State University, Southeast Tech or the Sioux Falls School District
- Registered apprenticeship connections and guidance through the South Dakota DLR
- Academic certificates in cybersecurity, or network services or software development
- Associate degrees in network and security administration (DSU and Southeast Tech), software development (DSU), and software support (Southeast Tech)
- DSU baccalaureate degrees in network & security administration, cyber operations or cyber defense.





We must get more women into cyber careers. We will never have enough cyber professionals if the field remains so male dominant. 77 percent of women in the workforce havew reported that no high school teacher or guidance counselor ever mentioned cyber security as a possible career. The MadLabs has the

CybHER Institute, which has reached over 10,000 Kindergarten through 12th grade girls, educating and exciting them about cyber careers for women. CybHER has held over 130 summer camps, events, presentations, and programs in the last four years, and they are constantly expanding their impact.



However, we cannot solve the numbers problem, i.e., not enough cyber professionals, until we are able to recruit and retain more cyber Ph.Ds as faculty to educate the next generation of students. All university cyber programs are facing tremendous threat in their ability to fulfill their purpose because of the increasing challenges of recruiting and retaining tech-skilled faculty. Tech savvy, especially computer and cyber sciences faculty, are few in number and have multiple lucrative job options outside higher education. The publication *Inside Higher Ed* noted recently that it is a supply and demand story on steroids.

On the supply side, U.S. universities are graduating relatively few Ph.D.s in computer and cyber sciences. According to the federal Integrated Postsecondary Education Data System (IPEDS) only 2 percent of all degrees conferred in the cyber sciences are doctorates, compared to 8 percent in the sciences, math, and engineering fields. Only 18 percent of these PhDs are taking teaching positions in higher education; another approximately 10 percent take non-teaching positions at universities, generally in full-time research.

On the demand side, according to many estimates, with a doctoral degree in any of the cyber sciences an individual can on average earn up to five times more in industry than they can as a university professor. Over the course of a career the salary gulf widens. As a result, market competition continues to grow for any cyber sciences professional interested in teaching. A recent report for the National Academies of Sciences, Engineering and Medicine revealed that between 2009 and 2015 there was a 74 percent increase in the number of cyber sciences bachelor's degrees awarded across U.S. colleges and universities. Doctoral-granting institutions as a group reported a 300 percent increase in cyber sciences degrees awarded. Clearly, students are flocking to tech-centric degree programs, just as they are at Dakota State, where the university has seen dramatic increases in enrollment over the last few years. The career opportunities cre-

ated by achieving a degree in a tech field are unquestionable. Bascially 100 percent of DSU's cyber program graduates move immediately into professional-level cyber jobs – well-paying intereting employment in excellent government or corporate organizations. (DSU's cyber graduates are split about 50/50 between government and corporate placements.) Those who don't move into a career placement have either enrolled in advanced degree programs or for some personal reason are not immediately purusing employment.

However, across the U.S. cyber sciences faculty hiring to teach these students is falling farther and farther behind. The Computer Research Association's comprehensive Taulbee Survey reported that 1,780 Ph.D. degrees in cyber sciences were awarded in 2015. Given that only 18 percent of these Ph.D.s took teaching positions in higher education, there were only 320 new Ph.D.s available to fill faculty slots in the 1,577 institutions that offer cyber sciences degrees. The National Academies report extrapolated this out to highlight that those 1,577 institutions can therefore expect to hire 0.2 new Ph.D.s per year, or one Ph.D. every five years. Eighty percent of new Ph.D.s who do move into teaching positions do so at research-intensive institutions. That means that colleges and universities without a robust research environment and community will be doing well to hire one new cyber sciences Ph.D. every 27 years. This is another reason why Dakota State launched the MadLabs. DSU's R&D endeavors are not only critical to productively leveraging DSU's intellectual assets to contribute to South Dakota's economic development but also to strengthen the university's ability to recruit and retain cyber-centric faculty.

A recent study in Computing Research News found that 18 percent of college and university cyber science faculty searches in 2017 failed entirely. Survey respondents at 155 institutions reported looking for 323 tenure-track positions and filling just 241. Even Stanford University, where computer science is the number one major and research opportunities abound, is experiencing the tenure-track faculty shortage. Stanford reports that in the last decade the university has lost twice as many faculty members to other jobs as it has in the previous 40 years.

Finally, we must put into place expected cyber security protections and engagement across every infrastructure sector. Utilities, manufacturing, education, agriculture and food safety – cyber defense and cyber warriors must become as ubiquitous as the technology that requires their aid.

CONCLUSION

There have been prophets in our midst for decades warning of this technological tsunami, and powerful cyber waves are now pounding the shores of almost every human endeavor across our country and around the world. Cyber threats to our nation's critical infrastructure are real and a serious problem. However, the United States also has the potentials and properties to fix it. This country needs leadership to set in motion the strategies and tactics that will protect our enterprises from being engulfed by cyber vulnerabilities. There are individuals and organization across this country, represented in part by those testifying today, who are eager to support and assist congressional efforts to provide that leadership. We are optimistic and encouraged that there are those who are stepping forward to protect the United States from cyber harm such that we can continue to harness cyber power for continued American success, innovation, and world-leading life, liberty, and the pursuit of happiness.