Dakota State University

The Madison Cyber Labs — The MadLabs

The MadLabs will drive economic development OUT from DSU and South Dakota and draw INTO DSU and South Dakota cybersecurity expertise, partners and other resources.

I. What is the Madison Cyber Labs – MadLabs - Project?

The Madison Cyber Labs (MadLabs) now under development will build on DSU’s expanding capabilities and strengths to establish a hub of cybersecurity and cyber operations expertise, research, economic development, and application in South Dakota. This R&D hub will act with centrifugal-like force to drive economic development out from DSU — locally, state-wide and regionally. The MadLabs will include Sensitive Compartmented Information Facilities (SCIFs) so students and researchers can pursue work critical to the growth of the cyber universe. Multiple interdisciplinary research and development clusters will act with centripetal-like force to draw into DSU and South Dakota cybersecurity students and professionals, in partnerships with other Regental schools, government, business and industry, non-profits and international higher education.

Components of the MadLabs include:

**Resources:** SCIFs, labs, networking, hardware, software, applications, etc.

**Partners:** government (e.g., NSA, DHS, NSF, etc.); business and industry; nonprofits; international higher ed, etc.

**People:** students (undergraduate, graduate, professional); faculty; researchers; interns; collaborators; etc.

**Programs:** cyber degrees from certificate and associates through masters, doctoral and professional development

**Research clusters:** various interdisciplinary and multidisciplinary research groups and projects

**DSU IT:** Infrastructure protection and security R&D relating to the DSU campus IT environment
II. What will be the costs/necessary budget associated with launching the MadLabs?

We are seeking one-time funding of $18 million for the building to house the MadLabs. The four University Presidents who have proposed research-based economic development projects have jointly approached a major donor for matching funds to enable all of their institutions’ projects to be accomplished.

Local economic development organizations and a private donor have come forward to support DSU in the development of the MadLabs project, including the creation of materials to explain the project to potential funding sources.

DSU is also seeking funding for matching capital fund requests and for related programmatic endeavors. This includes a Board of Regents Innovation Grant just awarded along with institutional matching funds. In addition, DSU is in active conversations about the MadLabs with numerous potential partners. These include the National Security Agency (NSA), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), Samsung, Booze Allen Hamilton, IBM, Fujitsu, F5 Networks, Facebook, Amazon Web Services, University College London and the e-commerce component of the European Union Washington Delegation, among others.

The project includes the following:

1. **Facility** - The plan is to build a new 40,000 square foot facility on DSU’s Madison campus.

2. **Sensitive Compartmented Information Facilities (SCIFs)** - The MadLabs will include SCIFs providing secured access to the leading-edge technologies required to do high-level government and industry classified and/or highly sensitive confidential or proprietary cyber work.

3. **People** - Present forecasts are for a layout that will accommodate over 200 students, faculty, full-time researchers and staff, mostly in newly created jobs.

4. **Research clusters** - Initial research clusters will include the **Cyclops Lab** (Cyber Classified Operations); the **PATRIOT Lab** (Protection and Threat Research for the Internet of Things); the **DigForCE Lab** (Digital Forensics for Cyber Enforcement); the **BaSe Lab** (Banking Security); the interdisciplinary **CLASSICS Institute** (Collaborations for Liberty And Security Strategies for Integrity in a Cyber-enabled Society), the **CybHER Security Institute** (Women in Cybersecurity) and the **Campus IT Living Lab** (DSU’s IT infrastructure protection and related research and development). Other clusters are under consideration and development, including Education and Big Data.

*DSU is pursuing multiple funding sources for the MadLabs building and for programmatic endeavors (jobs, equipment, etc.).*
III. What impact will the MadLabs have on South Dakota?

A. LEADERSHIP: Preserve and Expand South Dakota’s Cybersecurity Higher Ed Leadership

1. DSU and South Dakota presently hold a top leadership role in cybersecurity higher education.

a. DSU has three National Security Agency (NSA) and Department of Homeland Security (DHS) Academic Center of Excellence designations: Information Assurance Education, Information Assurance Research, and Cyber Operations (the most exclusive and technical of the designations).

b. NSA chose DSU as its partner for its National Cryptologic School (NCS) degree completion program at the bachelor’s and master’s levels.

c. The National Science Foundation (NSF) chose DSU’s cybersecurity programs for NSF’s competitive CyberCorps®: Scholarship for Service grants. DSU has the largest cohort of recipients in the nation.

d. DSU cybersecurity students earn top honors in national competitions, e.g. the National Cyber Defense Competition of the National Cyber League. Out of 85 teams and over 1,400 competitors the DSU team has been Regional Champions and in the Top Ten in the Nation in 2013, 2014, and 2016.

e. NSA engaged DSU faculty to assist in developing the criteria for the Centers of Excellence awards, as well as mentor other universities in the development of their cybersecurity academic programs.

2. HOWEVER, DSU and South Dakota face growing competition in cybersecurity education:

a. DSU was awarded its first NSA/DHS Center of Academic Excellence (CAE) credential in 2012, as 1 of 74 university programs. As of 2016 there are now 291 university cybersecurity programs with CAE credentials.

b. DSU is one of only a very few institutions with CAE credentials that does NOT have a cybersecurity center or institute with advanced capabilities. DSU’s NSA credentials are up for renewal in 2017.

3. The MadLabs will bring to South Dakota business and industry partnerships to educate and train their cybersecurity workforces.

CloudPassage, recognized as the “Most Innovative Cybersecurity Company” in the 2016 Cybersecurity Excellence Awards, has already been in contact with DSU with a request for the University to develop a Cloud workforce.
professional training program for their potential staff. The MadLabs will make this and other such partnerships possible.

4. The MadLabs will bring to South Dakota international partnerships with other cybersecurity universities and organizations.

a. DSU has partnering conversations already in progress with University College London’s Academic Centre of Excellence for Cybersecurity Research, the UCL Institute of Security and Crime Science, and the UCL Security Science Doctoral Research Training Centre (SECRet).

b. 5 Academic Alliance – The MadLabs will facilitate DSU’s development in South Dakota of an international alliance of cybersecurity higher education institutions endorsed by the Five Eyes, the intelligence alliance of Australia, Canada, New Zealand, the U.K. and the U.S.

5. The MadLabs will attract and keep in South Dakota highly qualified professionals as faculty and researchers who can lead the State in cybersecurity R&D and business development.

DSU and South Dakota face stiff competition for recruiting and retaining cybersecurity faculty and researchers. The MadLabs will be a powerful attractor for faculty, students and researchers who want to have access to leading edge cybersecurity resources and facilities.

B. WORKFORCE DEVELOPMENT – Expand South Dakota’s Cybersecurity Talent Pool

1. Educate South Dakota students for high-demand, high-wage cybersecurity careers.

a. There are presently over 300,000 UNFILLED cybersecurity jobs in the U.S., a 74% increase in the last 5 years.

b. The U.S. Bureau of Labor Statistics reports that in 2015 the median wage for all U.S. cybersecurity jobs was 149% higher than the U.S. median wage.

c. DSU has a strong heritage mission to train K-12 teachers. The MadLabs will enrich the technology environment of DSU, ensuring that DSU teaching graduates can prepare their K-12 students for cybersecurity higher education.
d. Companies are especially looking to **diversify** their cybersecurity staffs to include **more women**.

DSU faculty have had unique success in interesting young women in cybersecurity careers through multiple outreach activities, especially the GenCyber Girls Camp. This camp is for 7th to 9th grade girls and for the 2nd year in a row had more than double the number of applicants for the spaces available. Plans are in process to create a more extensive program to attract and nurture communities of young women interested in cybersecurity careers (the CybHER Security Institute).

**e. The MadLabs will** make it possible for DSU to develop a comprehensive higher education cyber curriculum of degrees for all levels: badges, certificates, associate degrees, baccalaureate degrees, master degrees, doctoral degrees, graduate certificates and post-docs, as well as continuing and executive education.

**2. Keep South Dakota educated cybersecurity professionals IN South Dakota.**

**a. Service Completion/Jobs:** The MadLabs will improve South Dakota’s ability to retain South Dakota-educated professionals in the State’s workforce. The MadLabs will develop more opportunities for CyberCorps®: Scholarship for Service graduates to complete their required service in South Dakota. Most recipients have to **leave South Dakota to fulfill their scholarship obligation.** Once out-of-state, with few cybersecurity jobs in South Dakota and heavy recruitment from other locales, South Dakota loses most of these graduates for the State’s workforce.

b. The MadLabs will give DSU students access to leading edge technology resources IN South Dakota so they will **not need to go out of the State for advanced education.** The access to secure facilities housing SCIFs will also open up possibilities for government agencies and businesses to partner with DSU and its students to do classified and/or highly proprietary cybersecurity work.

c. **Keep DSU’s Cybersecurity Education Current:** The MadLabs will enable DSU to continually keep academic programs at the forefront of knowledge in cybersecurity. The work of the research and development clusters and the various partnerships will feed back into DSU’s academic programs, ensuring that students will continue to graduate with current knowledge and skills.
C. ECONOMIC DEVELOPMENT – Propel South Dakota into the high-wage, high-growth cybersecurity marketplace

1. Investing in a regional science or engineering capacity, like the MadLabs, has been proven by economists to be the most successful driver of regional economic development

“Public investments in regional science and engineering capacity — as well as in a cluster of complementary human resource and business assets — have emerged as the dominant form of regional economic competition for high-growth, high-wage industries...” - Science Foundation Arizona

a. The worldwide cybersecurity market continues to grow rapidly as defined by market sizing estimates that range from $75 billion in 2015 to $170 billion by 2020.

b. South Dakota has a unique opportunity to develop cybersecurity services for the entire center of the United States, where there are presently almost no cybersecurity companies.

“Businesses on the cutting edge of technology grow through the creation of knowledge, and knowledge is subject to what economists call "spillovers" — meaning that the fruits of research can be shared easily by others. Thus, the market alone does not provide strong enough incentives for entrepreneurs to invest the vast resources required to create the knowledge that is at the core of new high-technology firms. Hence, the role for public support for university-based research.” - Kent Hill, W. P. Carey School of Business, Arizona State University
c. The information technology business sector is, and is expected to remain, one of the largest employers nationally. According to the World Economic Forum, for every ONE IT job that is created, FIVE new jobs are created in the community.

d. Unlike other businesses, expanding South Dakota cybersecurity industry requires almost no State infrastructure upgrades or expense.

e. New industries, like cybersecurity, require physical proximity to leading edge resources and expertise. The MadLabs will provide this for South Dakota.

2. Position South Dakota to obtain regional, national, and international government and business and industry cybersecurity grants, and partnerships as well as draw new cyber-concerned business to the State.

a. Cybersecurity attacks and breaches are only increasing, for government and business and industry, increasing spending in this area.

“Cybercrime costs were widely reported in 2015 as costing businesses globally between $400 and $500 billion annually. In 2016 the newer estimates have moved the needle on cybercrime costs to $2-$3 trillion. Clearly that is going to trigger more cybersecurity spending. As cybercrime rises, so does cyber defense spending — it’s the nature of the beast.” – Steve Morgan, Founder, CyberVentures

According to the publication Business Insider:

b. The MadLabs will build on South Dakota’s/DSU’s cybersecurity credentials and relationships with multiple government security agencies and departments to bring new grants and contracts into the State.

c. The MadLabs will increase South Dakota’s attractiveness for all types of companies to locate or relocate in South Dakota. Corporations are evaluating cybersecurity resources as a key issue when considering possible locations.

D. NATIONAL DEFENSE – Renew South Dakota’s Leadership Role

1. The MadLabs, by growing South Dakota’s cybersecurity resources and expertise, will provide South Dakota with an opportunity to renew its historical role as a key player in U.S. national defense.

a. Cybersecurity is one of the key issues in U.S. national defense today. U.S. governments, federal and state, and all aspects of corporate activity, experience constant and growing attacks. The U.S. Director of National Intelligence James R. Clapper ranks cybersecurity as the No. 1 national security threat, ahead of terrorism, espionage and weapons of mass destruction. Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact.
According to the cybersecurity firm Mandiant, since as early as 2006, China’s People’s Liberation Army (PLA) has been using an elite cyberwarfare unit based in Shanghai to launch hundreds of cyberattacks targeting American interests. Unit 61398 has a staff of “hundred if not thousands” of highly trained cyberattack professionals.

For example, for about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that hijacked U.S. and other foreign Internet traffic so that it traveled through Chinese servers where the Chinese could view and capture emails, file transfers, etc. This incident affected traffic to and from the U.S. government, including Internet traffic for the Senate, the Army, the Navy, the Marine Corps, the Air Force, the office of the Secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

Cyber Command Chief Admiral Mike Rogers said that unlike other areas of military competition, Russia is equal to the United States in terms its cyberwarfare capabilities, with China a close second. Rogers has warned the U.S. Congress that Russia and China now can launch crippling cyberattacks on the U.S. electrical grid and other critical infrastructures.

b. South Dakota is not presently considered to be one of the U.S. states leading the “cyber pack.” However, none of the states included in that characterization are in the middle of the country. **South Dakota has an opportunity to be the national leader for cybersecurity initiatives and activities for not only the Plains Region, but for much of the West as well.** South Dakota is in an excellent position geographically to play this role, given its proximity to important U.S. natural resources as well as key components of national infrastructure.