ORGANIZATIONAL UNIT PROPOSAL FORM

DIRECTIONS: *Use this form when proposing a new organizational unit, center, institute, department, school, or college.*

DATE OF REQUEST: Oct. 20, 2013

INSTITUTION: University of Nevada, Reno

NAME OF PROPOSED UNIT: Cyber Security Center

DATE OF IMPLEMENTATION: Jan. 1, 2014

Date of AAC Approval:
October 29, 2013

Date of Board Approval:

PART 1

A. Action requested
We seek to formally establish the Cyber Security Center (CSC) at the University of Nevada, Reno.

B. Brief description and purpose of proposed unit
At the 2012 Aspen Security Forum, General Keith Alexander, the head of the U.S. Cyber Command, stated that on a 1-10 scale he rated American cyber security a "3." He went on to say that an "unparalleled theft" of intellectual property was under way, imperiling our economic recovery. When one adds to General Alexander's comments statistics that indicate a rapid rise in cyber crime, along with acts of cyberwar, the picture grows even darker. Cyberspace is a dangerous place, and none of the regulatory or market-driven attempts to improve security over the past twenty years have made matters better. Thus cyber security remains a "grand challenge," one that calls not just for technical solutions, but requires the skillful blending of business, engineering, scientific, sociopolitical, and strategic expertise.

Cyber security has enormous implications for economic development in Nevada, including industries such as banking, healthcare, data centers, and online gaming, all of which are increasingly important components of Nevada's economy. Cyber security also has important implications for our power grid as well as for the large and growing military presence in Nevada.

As noted above, cyber security is not only a technical challenge. In response to this complex problem, the Cyber Security Center (CSC) will bring together expertise from a range of disciplines including political science, information studies, journalism, criminal justice, mathematics, philosophy, psychology, military science, and computer science and engineering. This melding of disciplines is what makes UNR's approach to cyber security truly unique.

Preparing the next generation of cyber-security experts requires education and career development experiences in highly multidisciplinary research settings that are integrated with a curriculum that transcends the structures of the standard academic curriculum. The Center will not only provide

cutting-edge applied research on cyber security, but will also provide educational resources for the state. As an immediate goal, the center will develop an undergraduate minor and a cross-disciplinary graduate certificate in cyber security. The students from these programs will contribute substantially to our workforce, and their availability will make Nevada a much more attractive destination for a broad range of industries.

C. Outline plans for the success of the proposed unit

Over the course of the past several months, UNR faculty and administrators have actively engaged in a series of meetings to discuss how expertise in various disciplines that span the university can and must come together to address applied and basic issues that relate to cyber security. Initial leadership for the CSC has been identified and will include faculty co-chairs, one from social sciences and one with technical expertise. UNR is pursuing hiring initiatives in cyber security and "big data in social sciences and humanities" and is in the process of filling 6 faculty positions that will build additional capacity in these areas. This infusion of faculty, in combination with our considerable existing faculty talent, provides a solid foundation of expertise for the CSC. The CSC, has been endorsed by local and statewide economic-development groups, law enforcement, and private industry (see attached letters). The undergraduate minor and graduate certificate proposed below will largely consist of existing courses, though we anticipate that additional specialized courses will be developed that cross disciplinary boundaries. We plan to pursue large-scale funding opportunities from federal sources such as NSA, DOD, DHS, NIJ, and NSF and also anticipate substantial opportunities with private companies.

PART II

A. Mission statement

The mission of the UNR CSC is to master the challenge of cyber security by bringing together cross-disciplinary teams to work in synchrony, examining each problem through disciplinary "lenses" and seeking solutions that incorporate societal, technical, ethical, political and economic considerations. The CSC will provide educational and research opportunities for both undergraduate and graduate students that will prepare them to pursue careers in cyber security and related fields

B. Goals and objectives

i. Teaching

We anticipate two educational tracks as part of this initiative: (1) An undergraduate-level minor for those who would move straight into a security-operator position in different fields; and (2) A cross-disciplinary graduate-level certificate program that aims at adding significantly to knowledge in this rapidly growing field.

ii. Research

The UNR CSC will bring together cross-disciplinary teams to examine cyber-security problems and seek potential solutions through their various disciplinary "lenses." For example the issue of infrastructure protection would be viewed from several perspectives simultaneously: engineers will think through how to improve the protection of systems built long before the Web and the Net, but which are now connected to them; business expertise will help determine what types of solutions are economically feasible; political scientists will consider the pros and cons of regulation; media-communication scholars will examine the impacts upon communication networks and information flows; and strategists will view the problem from the perspective of national security. As to other areas where cyber security is important – from electronic commerce and banking to online gaming – the same cross-disciplinary approach will be taken.

2

By bringing many points of view to bear, a kind of collective intelligence will be created that takes on this grand challenge in ways that the Academy has not yet tried. Some universities have focused on technical problems, others on policy and related matters. None have built teams that bring all perspectives together. We anticipate that this unique scholarly synergism will make us competitive for a variety of substantial funding opportunities from federal agencies and private foundations.

iii. Service

We will actively seek partnerships with local and statewide law-enforcment and private organizations. The relationship with the Northern Nevada Regional Intelligence Center and VereSoftware (attached letter) is an example of a partnership that is already underway. Because cyber security has implications for virtually every aspect of society, the opportunities for outreach and service are virtually limitless.

C. Major participants or collaborators

i. Internal to campus

UNR faculty from a broad range of disciplines have indicated their enthusiasm for the CSC and plan to be active participants. Participants include faculty from computer science and engineering, journalism, mathematics, philosophy, political science, psychology, military science, and information systems. The Dean of the Graduate School and the Vice President for Research and Innovation have also expressed their strong support of the CSC.

ii. External to campus

Beyond UNR, but in the immediate geographic area, is a robust commercial sector that has developed deep insights into the cyber-security problem set. Also, a significant proportion of the local population is actively involved in and contributes to the larger discourse about cyber security (e.g., the National Security Forum and the Northern Nevada Network). At a state-wide level, Nevada provides an almost laboratory-like setting for examining such matters as infrastructure protection, and as a "small state" will prove attractive for those doing research at the policy, regulatory, even societal levels of analysis. Further, Nevada is home to national leaders in the gaming industry, now taking early steps in the online arena. There is tremendous potential for economic growth here, but great risks if security issues are not properly addressed. Research into online gaming will naturally benefit from close connections with industry leaders in Las Vegas. Large data centers such as Switch also place Nevada at the nexus of cyber-security interests. Addressing these challenges and opportunities will require close collaboration with experts at UNLV and DRI, and we anticipate that the CSC will quickly expand to include our sister institutions.

D. Evidence of contact within and between affected academic units

Beginning in the spring of 2013, a series of formal and informal meetings were conducted on the UNR campus. Initial discussions were among academic deans, the president, the provost, and an internationally recognized cyber-security scholar, Dr. John Arquilla of the Naval Postgraduate School in Monterey, CA. Subsequent meetings included deans and all interested UNR faculty as well as Dr. Arquilla. The UNR Faculty Senate was informed of incipient plans for a CSC and invited to participate in discussions. Deans were invited to comment on a white paper that was prepared for discussion at the Sept. 2013 meeting of the NSHE Academic Affairs Council. Finally, a draft of this proposal was distributed to faculty and administrative stakeholders for comment.

E. Proposed physical location

The CSC will reside on the UNR campus but will not initally require dedicated space. Participating faculty will use their currently assigned office and research space. CSC activities will make use of common-use meeting facilities and classrooms.

F. Proposed organizational structure (include organizational structure within the campus)
The CSC will be led by co-directors, one from a techcnical discipline (e.g., science or engineering) and one from a non-technical area (e.g., humanities, social science, journalism, or business). A political scientist and computer scientist have volunteered to serve as the initial co-directors. The CSC will report to the Vice President for Research and Innovation (VPRI). The VPRI, in turn, reports directly to the Executive Vice President and Provost.

G. Activities to be sponsored (e.g. courses, seminars, research, and outreach) – indicate if courses or seminars will be offered through the proposed unit. Please specify if they will be offered for academic credit and applicable to a degree program. Give estimated enrollment.
There are a number of for-credit UNR courses "on the books" that bear directly on cyber security and can be offered through their home departments. These include technical courses in Engineering as well as courses related to policy and strategy in the Colleges of Liberal Arts, Journalism, and Business. We expect that the Department of Military Science will also provide an introductory course in cyber security and cyberwarfare. We expect to develop capstone courses collaboratively through the CSC (e.g., a survey course on "Society and Security in the Information Age"). In addition to courses and seminars, the CSC will strive to bring together cross-disciplinary research teams, from around and beyond UNR, to advance knowledge and share best practices in the cyber-security field. Public outreach will also form a cornerstone of the CSC, including the creation of key linkages with industry, law enforcement, government, other leading universities, and the general public.

H. Resource Analysis – source of funds necessary for the proposed change (enrollment-generated state funds, reallocation of existing funds, grants, other state funds)
UNR will provide enrollment-generated funds to hire an adjunct faculty member who will participate in leading the CSC and teach courses in cybersecurity. Within three years we anticipate that the CSC will be entirely self supported through external contracts and grants.

I. Projected Budget – identify portions of costs which will require state resources, grants, gifts and/or contracts
We project an initial annual budget of $200,000, which will support the salary and fringe benefits of an adjunct faculty member who will participate.

Please attach any supporting documentation (i.e. support letters from community, industry).

16 October, 2013

Marc Johnson, President
University of Nevada, Reno
Clark Administration, #200
1664 N. Virginia Street
Reno, Nevada 89557

RE: Cyber Security Center Support

Dear President Johnson,

I am pleased to offer this letter in support of your proposal to establish a Cyber Security Center at UNR. Cyber security is an immediate challenge to national security and has enormous implications for economic development in Nevada. It has implications for industries such as banking, healthcare, and online gaming, all which are increasingly important components of Nevada's economy. Cyber security also has important implications for our power grid as well as the large and growing presence of military operations in Nevada.

Cyber security is not only a technical challenge. It includes components that have political, ethical, philosophical, societal, and business implications. In response to this complex problem, the Cyber Security Center will bring together expertise from a range of disciplines including political science, information studies, journalism, mathematics, philosophy, psychology, and computer science. This melding of disciplines is what makes UNR's approach to cyber security truly unique.

I am particularly impressed that you have engaged the guidance and participation of internationally recognized cyber-security expert Dr. John Arquilla, who is currently on the faculty at the Naval Postgraduate School in Monterey, CA. Dr. Arquilla brings instant credibility to the Center. I am also pleased that the Center will reach out to include the substantial faculty expertise at UNLV and DRI.

The Center will not only provide cutting-edge applied research on cyber security, but will also develop an undergraduate major and a graduate certificate in cyber security. These students will contribute substantially to our workforce, and their availability will make Nevada a much more attractive destination for a broad range of industries.

I look forward to seeing the Cyber Security Center blossom and mature and I am confident that it will contribute tangibly to the economic development of Nevada.

Sincerely,

Karsten Heise
Director | Technology Commercialization

October 17, 2013

President Marc Johnson

The University of Nevada, Reno

Dear President Johnson:

National security experts have identified Cyber Intrusion as one of the major threats facing the United States. This capability is a growing concern for our military forces deployed for potential conflicts, but it is also now one of the most serious threats facing our civilian infrastructure. President Obama recently signed a secret directive that enables the military to more aggressively thwart cyber attacks, and—along with other departments— conduct offensive cyber operations. The directive intends to ensure the U.S. has the ability to counter an attack that could occur in milliseconds by unknown assailants utilizing a circuitous route (not necessarily nation-states, but also terrorist groups or even disgruntled hacker organizations).

The Obama directive also put a particularly high priority on defending the nation's private-sector computer systems that control critical functions such as electrical grids, the rail and road transportation system, and communications. The National Governors Association, recognizing the threat to domestic critical infrastructure, has established a Cyber-Security element. with a particular focus on the vulnerability of the nation's electrical grid to cyber terrorism.

Dr. John Arquilla has pointed out that there is a reason why cyber security remains so poor: it has not been treated as a "grand challenge." That is, **a problem the solution to which will require bringing together the best minds from many different academic disciplines** – from technical fields to the social sciences – and nurturing a network of thought leaders from government, business, social advocacy, military, and other fields. In short, cyber operations and security need to be seen as posing a challenge as difficult to master as transnational terror or climate change.

What does this mean for academia and NSHE? There is a growing need for cross-disciplinary work on the cyber-security challenges. No single institution has done this (MIT is tech-focused on cyber; Harvard is law-centered; CSIS is trying to integrate technology and policy, but without much success).
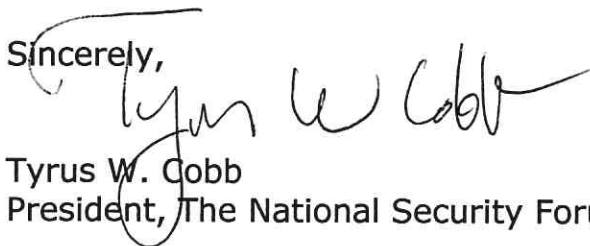
UNR is in a position to become something unique by leading the way forward in designing a coordinated approach to cyber security that will engage engineers, computer scientists, business experts, and political/sociological scientists. It would involve as well the military science department and, importantly, the private sector.

The University of Nevada, Reno, is an institution where an awareness of and sensitivity to the grand challenge of cyber security is well developed. What is needed now is the spark that will ignite a sustained effort by the University and the public and private sector actors already in place in Reno to deal with the grand challenge of cyber security. UNR is the place for this initiative because the network is already forming; all that is needed is a "quickening agent." Significant research and development work has also been accomplished at UNLV and at the Desert Research Institute.

"Mastering the 21st Century Cyber Security Challenges" would first integrate disparate efforts at UNR by coordinating research and policy work being done in different departments and colleges. Further, this initiative would encourage private sector companies—such as NV Energy, Apple, NJVC—to participate in and support this program. **More importantly, Dr. Arquilla believes that UNR could become the hub that brings together a number of other prestigious institutions in this effort—for example, UC Berkeley, Stanford, UCLA, UNLV and the DRI.**

I concur with Dr. Arquilla's recommendation that a Cyber Security Center be established at UNR, which could become the core of a statewide effort incorporating UNLV and DRI, and later, the hub of a consortium of major academic centers on the West Coast. Let's move forward with this promising and exciting proposal quickly.

Sincerely,

Tyrus W. Cobb
President, The National Security Forum

October 16, 2013

President Marc Johnson
University of Nevada, Reno
1664 N. Virginia Street
Reno, NV 89557

Dear President Johnson:

I am writing to express my strong support for the proposed Cyber Security Center at the University of Nevada, Reno (UNR). Cyber security is an ever present issue in all of our daily lives and is critical in the strategic plan to protect the citizens of Washoe County and Nevada.

In recent years, the Washoe County Sheriff's Office has created a Cyber Crimes Unit that deals strictly with computer related security and crimes. This unit was formed to address the ever increasing challenges associated with computer issues, specifically, computer security, computer crimes, computer forensics, internet fraud and internet crimes against children. Additionally, the Northern Nevada Regional Intelligence Center (NNRIC) was created as a regional asset to address all crime problems and trends in addition to terrorism related matters.

I am aware that a team of faculty members from the Computer Science and Engineering Department at UNR, led by Dr. Bebis, have already had several meetings with members of the Washoe County Sheriff's Office and NNRIC to discuss potential areas of cooperation and collaboration. I have strongly encouraged our staff to continue working with UNR faculty in order to develop a mutually beneficial collaboration. I feel that the proposed Center will present a tremendous opportunity to build significant expertise in cyber security and increase our capacity to further protect our citizens.

Sincerely,

Michael Haley, Sheriff

Marc Johnson, President
University of Nevada, Reno
Clark Administration, #200
1664 N. Virginia Street
Reno, Nevada 89557

RE: Cyber Security Center Support
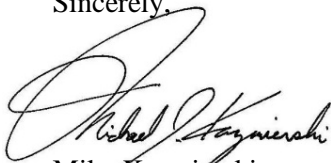
Dear President Johnson:

On behalf of the Board of Trustees of the Economic Development Authority of Western Nevada (EDAWN), I would like to offer my strong support for the establishment of a Cyber Security Center on the University of Nevada, Reno campus. Our daily life, economic vitality, and national security depend on a stable, safe and resilient cyberspace. A center of this caliber in our community will help educate and recruit future generations of cyber security workers.

The Cyber Security Center will be a unique facility as it will engage expertise ranging from political science, information studies, journalism, mathematics, philosophy, psychology and computer science. This new center will have extensive economic implications for the State of Nevada and bring with it important funding opportunities which will in turn create jobs in northern Nevada. At this time it is anticipated that the center will offer an undergraduate minor in cyber security as well as a graduate certificate. These will contribute to large unmet employment demands in the military, as well as the private sector, including Nevada's emerging online gaming industry.

Given the need to continue to diversify the economy of Northern Nevada and our exceptionally high unemployment rate, EDAWN strongly recommends the establishment of a University of Nevada, Reno Cyber Security Center.

If you have any further questions or concerns, I can be contacted at (775) 829-3711.

Sincerely,

Mike Kazmierski
President and CEO

Cc: Kevin Carman

PRESIDENTIAL GOLD INVESTORS

VERE SOFTWARE
— INVESTIGATIVE TOOLS —

October 21, 2013

President Marc Johnson
University of Nevada, Reno
1664 N. Virginia St.
Reno, NV 89557

Dear President Johnson;

I am writing to express my enthusiastic support for the proposed Cyber Security Center at the University of Nevada, Reno (UNR) and to offer our assistance in its development.

Cybersecurity is an area of research and development that requires an effective response. In particular, it requires effective collaborative efforts to accomplish a resolute response. Vere Software and the Computer Science and Engineering (CSE) Department at UNR have successfully collaborated in the past through a research project funded by the National Institute of Justice (NIJ), U.S. Department of Justice (DOJ), on forensic and Investigative tools and technologies for investigating criminal use of Internet anonymizers. This collaboration has led to the development of a one of a kind law enforcement tool that can aid investigators to identify criminal users of anonymizing technologies on the Internet.

The need for research and development in the field of Cybersecurity is critical to government, business and law enforcements ability to respond to emerging threats. The proposed Center will offer significant opportunities for successful public/private collaborations between existing partners. It will also enable Vere Software to use its background and expertise to assist in the research and development of effective responses to the issues surrounding Cybersecurity.

I am closing my letter by re-iterating my strongest possible support for the proposed Cyber Security Center at UNR. Vere Software's expertise in the field of online investigations and its staff's unique understanding of digital evidence collection and forensics will offer UNR a unique partner to jointly address the many challenges of Cyber Security locally, nationally and internationally.

Sincerely,

Todd G. Shipley, CFE, CFCE
President & CEO

4790 Caughlin Parkway, #323, Reno, NV 89519 - 888-432-4445 – www.veresoftware.com