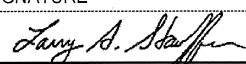
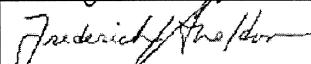
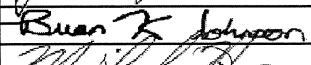

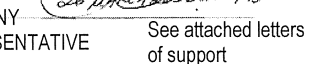
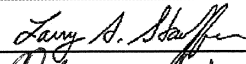
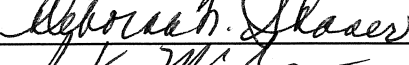
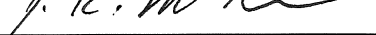



# Security Management of Cyber Physical Control Systems

COVER SHEET FOR GRANT PROPOSALS			
State Board of Education			
SBOE PROPOSAL NUMBER: (to be assigned by SBOE)		AMOUNT REQUESTED: \$2,099,016	
TITLE OF PROPOSED PROJECT: <b>Security Management of Cyber Physical Control Systems</b>			
<p>SPECIFIC PROJECT FOCUS: Cyber-attacks and intrusions are nearly impossible to reliably prevent given the openness of today's networks and the growing sophistication of advanced threats. Knowing the vulnerabilities is not adequate, as the evolving threat is advancing faster than traditional cyber solutions can counteract. Accordingly, the practice of cyber security should focus on ensuring that intrusion and compromise do not result in business damage or loss through more resilient solutions. We will create a platform to facilitate and build complementary and multidisciplinary R&amp;D capabilities to address these pressing problems. Our platform will incubate innovative products and services for safeguarding cyber physical control systems (CPCSs) that are ubiquitous and underpin key sectors of our economy. Early participation of industry will aid in vetting promising technologies. Better methods for assessment combined with more resilient systems design will safeguard against potentially immense economic impact currently being faced by Idahoan stakeholders. Our objective outcomes include: (1) <u>Strengthen our capacity</u> by adding key faculty and enhancing laboratories to increase our ability to deliver improved education and R&amp;D products in CPCS to students and technical professionals in industries within the State that will accelerate economic development, (2) <u>Strengthen collaboration</u> with Idaho industry and other Idaho universities to synergize cybersecurity education, research, and deployment activities, (3) <u>Foster technology transfer</u> and commercialization through technology incubation, and (4) <u>Strengthen and expand the workforce</u> by deploying cybersecurity expertise to Idaho industry and improving the talent pipeline with computer science and engineering graduates. We will empower three important state-based initiatives:</p> <ol style="list-style-type: none"> <li>1. Control Systems Cyber Innovation Center (INL),</li> <li>2. New Security Assessment, Intelligence and Operations Center (Statewide),</li> <li>3. New Resilience Research and Technology Incubation Center (R2TI-Ctr) in Moscow combined with the UI CTOC (Cybersecurity Training and Operations Ctr) in Coeur d'Alene.</li> </ol>			
PROJECT START DATE: <b>7/1/2016</b>		PROJECT END DATE: <b>6/30/2019</b>	
NAME OF INSTITUTION: <b>University of Idaho, Office of Sponsored Programs</b>		DEPARTMENT: <b>Department of Computer Science and the Department of Electrical and Computer Engineering</b>	
ADDRESS: <b>875 Perimeter Drive, MS 3020, Moscow, ID 83844-3020</b>			
E-MAIL ADDRESS: <b>osp@uidaho.edu</b>		PHONE NUMBER: <b>208-885-6651</b>	
PROJECT ORG RELATION	NAME:	TITLE:	SIGNATURE
PROJECT DIRECTOR / PRINCIPAL INVESTIGATOR	Larry Stauffer	COE Dean	
CO-PRINCIPAL INVESTIGATOR	Frederick T. Sheldon	Professor and Chair, CS Department	
CO-PRINCIPAL INVESTIGATOR	Brian K. Johnson	Professor, ECE Dept	
CO-PRINCIPAL INVESTIGATOR	Michael A. Haney	Asst Professor, CS Dept	
CO-PRINCIPAL INVESTIGATOR	Daniel Conte de Leon	Asst Professor, CS Dept	
NAME OF PARTNERING COMPANY(S):	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 33%;">1. INL</div> <div style="width: 33%;">5. Idaho Forest Group</div> <div style="width: 33%;">9. Kootenai Health</div> <div style="width: 33%;">2. BSU</div> <div style="width: 33%;">6. Idaho Falls Power</div> <div style="width: 33%;">10. Avista</div> <div style="width: 33%;">3. Micron</div> <div style="width: 33%;">7. Power Engineers</div> <div style="width: 33%;">11. Hewlett Packard</div> <div style="width: 33%;">4. SEL</div> <div style="width: 33%;">8. Community Security Coalition</div> <div style="width: 33%;">12. Idaho Power</div> </div>		COMPANY REPRESENTATIVE NAME: _____ See attached letters of support
ORG RELATION	NAME and TITLE:	SIGNATURE	
Authorized Organizational Representative	Larry Stauffer, Dean of COE		
	Debra Shaver, Director OSP		
	Jack McIver, VP of ORED		

FY17 IGEM Proposal: Security Management of Cyber Physical Control Systems

SUMMARY PROPOSAL BUDGET				Three-Year Summary		
Name of Institution: University of Idaho						
Name of Project Director: Larry Stauffer						
A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)						
Name/ Title		Salary/Rate of Pay	Fringe	Dollar Amount Requested		
Larry Stauffer, Lead PI and Project Director 5% FY	Base Salary: \$208,060	\$ 32,155	31.1%	\$ 42,155		
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$ 14,626	31.1%	\$ 19,275		
TT, Associate Prof, Security, CS AY	Base Salary: \$115,000	\$290,950	31.1%	\$ 381,435		
TT, Assistant Prof, Power Security, EE AY	Base Salary: \$ 95,000	\$240,350	31.1%	\$ 315,099		
TT, Assistant Prof, Physical Security, CS Idaho Falls AY	Base Salary: \$ 95,000	\$192,850	31.1%	\$ 252,826		
TT, Assistantt Prof, SCADA, Power Systems, Idaho Falls AY	Base Salary: \$ 95,000	\$192,8502	31.1%	\$ 252,826		
Graduate Student RAs		\$ 150,000	2.0%	\$ 153,000		
<b>% OF TOTAL BUDGET:</b>		67.485%	<b>SUBTOTAL:</b>		\$ 1,416,516	
B. EQUIPMENT: (List each item with a cost in excess of \$1000.00.)						
Item/Description				Dollar Amount Requested		
VT Equipment (improved VT facilities, Moscow, Boise, and Idaho Falls) in Year One				\$ 117,000		
Enhance Power Lab (computing and test equipment, software) in Year One				\$ 180,000		
<b>SUBTOTAL:</b>				\$ 297,000		
C. TRAVEL:						
Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging	Per Diem	Dollar Amount Requested
Attend Conferences						\$ 18,500
Visit Agencies						\$ 10,000
Visit Industry						\$ 10,000
<b>SUBTOTAL:</b>						\$ 38,500
D. Participant Support Costs:						
1. Stipends						
2. Other						
<b>SUBTOTAL:</b>						

FY17 IGEM Proposal: **Security Management of Cyber Physical Control Systems**

E. Other Direct Costs:		Dollar Amount Requested
1. Materials and Supplies (includes research supplies and software)		\$ 34,200
2. Publication Costs/Page Charges		\$
3. Consultant Services (Include Travel Expenses)		\$
4. Computer Services		\$
5. Subcontracts		\$
6. Other (specify nature & breakdown if over \$1000)		
Start-up/search funds—specified by hire to initiate research	\$205,600	
Moving expenses in year one (maximum 10% of bases salary)	\$ 21,000	\$ 312,800
Moving expenses in year two (maximum 10% of bases salary)	\$ 19,000	
Grad student tuition/fees	\$ 67,200	
SUBTOTAL:		\$ 347,000
J. Total Costs: (Add subtotals, sections A through I)		\$ 2,099,016
K. Amount Requested:		\$ 2,099,016
Project Director's Signature: 		Date: 04/01/2016

<b>INSTITUTIONAL AND OTHER SECTOR SUPPORT</b> (add additional pages as necessary)	
A. INSTITUTIONAL / OTHER SECTOR DOLLARS	
Source / Description	Amount
Internship opportunities to COE students from industry partners.	TBD
Industry partners will provide time and talent for assessments pertaining to CPCS Security Management.	TBD
Faculty start-up offers are negotiated to be \$100,000 to \$300,000 in computer science to attract quality assistant or associate professor candidates. The UI will likely be providing \$200,000 to \$400,000 of additional funds over three-years for the new faculty start-up packages. Faculty start-up Includes funds for student support, summer salary, individual travel, supplies, software, etc.	\$200,000 to \$400,000
B. FACULTY / STAFF POSITIONS	
Description	
The Co-PIs in this project will provide support in managing and executing the project plan including limited assistance from outside faculty including the CSDS. The COE including the CS and ECE Departments will offer both Administrative and Sys-admin (IT) support.	
C. CAPITAL EQUIPMENT	
Description	
There exists VTC facilities/equipment and technical personnel that support the UI and COE that will be utilized on an as needed basis. The equipment described in Section 4 and Appendix A (e.g., PAL, RADICL and ICCL) will also be provided as needed and/or upgraded to ensure the successful implementation of this project including existing computers, printers and other general purpose office equipment.	
D. FACILITIES & INSTRUMENTATION (Description)	
Please see relevant comments above in "C. CAPITAL EQUIPMENT"	

# Security Management of Cyber Physical Control Systems

*FY17: State Board of Education, Higher Education Research Council  
Idaho Global Entrepreneurial Mission (IGEM) Initiative Grants*

1. **Name of Idaho public institution:** University of Idaho
2. **Name of principal investigator:** Larry Stauffer, Dean, College of Engineering (COE) and *Co-PIs:* Fredrick Sheldon, Chair, CS (COE, Moscow); Brian Johnson, ECE (COE, Moscow); Michael Haney, CS (COE, Idaho Falls); Daniel Conte de Leon, CS (COE, Moscow).
3. **Project objective and amount requested:** Protecting the Idaho economy from damages caused by cyber espionage and extortion, security breaches, or other targeted cyber-attacks is a top priority. From manufacturing<sup>1</sup> to medical, Idaho industries rely heavily on *control systems* in their facilities and in their equipment and are vulnerable to cyber security risks. Furthermore, utilities that supply electric power to all segments of our economy are vulnerable to cyber security risks because of their control systems. Notwithstanding, control systems have importance to most all sectors of today's economy and all are at risk.

*Secure-by-design* means that the systems have been designed from the ground up to be trustworthy. Major security vulnerabilities exist today from the lack of security-by-design in industrial control systems. For example, the computer worm known as *Stuxnet* reportedly ruined almost one fifth of Iran's nuclear centrifuges by disrupting industrial programmable logic controllers in a targeted attack. Recently, the Obama administration warned the nation's power companies, water suppliers, and transportation networks that sophisticated cyber-attack techniques used to bring down parts of Ukraine's power grid two months ago (January 2016) could easily be turned on them<sup>2</sup>. It is not just these major situations. Hospitals have experienced cyber extortion for payment as hackers infiltrate cancer radiation treatment facilities through equipment control systems. Countless breaches/break-ins have amounted to billions in lost

---

<sup>1</sup><https://idaholabor.wordpress.com/2015/05/27/idaho-exports-expanding/> Idaho manufacturers account for 12.25% of total output \$7.62B, employing 9.12% of the workforce (59,100 manufacturing jobs produced \$61,515/year on average in 2013 wages). <https://research.stlouisfed.org/fred2/series/IDNGSP> and <http://goo.gl/5epFLA>.

<sup>2</sup><https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01> NY Times articles: <http://goo.gl/sKXBxw> and <http://goo.gl/geHxFd>, SANS Rpt: [http://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf) (also see Archer summary: <http://goo.gl/vtZNCf>).

revenue and damages nationally and Idaho is not exempt. Accordingly, this project's purpose is to protect Idaho's economy from damages caused by cyber espionage and extortion, security breaches, or other targeted cyber-attacks and power disruptions.

Thus, our project will create a program to incubate innovative products and services for safeguarding Cyber Physical Control Systems (CPCSs) that are ubiquitous and underpin key sectors of our economy. Early industry participation will aid in vetting promising technologies. Better assessment methods combined with resilient systems design will safeguard the potentially immense economic impact currently faced by Idaho stakeholders. Our objectives include:

1. [Strengthen our capacity](#) by adding key faculty and enhancing laboratories to increase our ability to deliver improved education and R&D products in CPCS to students and technical professionals in industries within the State, especially those that depend on reliable electrical power, which will accelerate economic development.
2. [Strengthen collaboration](#) with Idaho industry and other Idaho universities to synergize cybersecurity education, research, and deployment activities.
3. [Foster technology transfer](#) and commercialization through technology development and incubation.
4. [Strengthen and expand the workforce](#) by deploying cybersecurity expertise to Idaho industry and improving the talent pipeline with computer science and engineering graduates.

In pursuing these four objectives, we will leverage expertise from the Control Systems Cyber Innovation Center at the Idaho National Laboratory (INL), expand the UI Cybersecurity Training and Operations Center (CTOC) in Coeur d'Alene [[www.uidaho.edu/cda/uirp/ctoc](http://www.uidaho.edu/cda/uirp/ctoc)] to include security assessments and initiate a Resilience Research Incubation Center (RRIC) in Moscow. To provide increased protection of Idaho's economy through security management of CPCSs, we request \$2.1 million (\$700,000/yr.) to support our four objectives.

#### **4. Resource commitment**

This project directly supports the first three goals of the UI's new Strategic Plan: Scholarly and creative work with impact; Outreach that inspires innovation and culture; and Educational

experiences that improve lives. The objectives of this proposal also directly support the mission and all four goals of the 2016-2020 Strategic Research Plan for Higher Education, as well as two of the five areas of focus, namely Energy and Software Engineering. Furthermore, expanding cyber security capability is a top priority of the College of Engineering. The previous UI IGEM grant to hire a multidisciplinary cyber-security faculty cluster completed in 2015 by the Center for Secure and Dependable Systems (CSDS) facilitated the College of Engineering and the department of Social Science to hire five faculty and one post-doc focused on cybersecurity of software and analytics. This team still meets bi-monthly turning ideas into proposals, projects, and publications. Moreover, the team brought over \$3 million in new extramural funding to support research, scholarships, and lab enhancements and has established an Annual Cybersecurity Symposium ([www.cybersecuritysymposium.com](http://www.cybersecuritysymposium.com)). In its 3rd year, this symposium has become internationally recognized for collaboration in transportation, modeling, power, and cybersecurity. A sub-team of these researchers developed new technology (core IP for a Moscow startup) that won 2nd place in the National DARPA Cyber Challenge competition.

Educational outreach has been a colossal success. Since the formation in 2001 of the NSF Scholarship for Service program (aka CyberCorps), UI has educated students who have become leaders in cyber security for government agencies/laboratories and the private sector, playing a vital role in our nation's security. Presently, CSDS maintains over 3000ft<sup>2</sup> of lab space, supports 30+ students and includes 10 COE, 3 Business and 1 Law faculty plus many associate researchers. Consider these CPCS team facilities (also Appx. A): (1) Power Applications Lab (PAL) enables testing and simulation of Power System control technologies and devices and is an excellent resource for hands-on training and (2) RADICL, the Reconfigurable Attack-Defend Instructional Computing Lab enables hands-on training/research in cybersecurity.

The UI is committed to expanding our cybersecurity expertise into the area of cyber physical control systems, especially complementing our nationally recognized expertise in power systems,

and helping to meet the needs of the State for well-trained and experienced cyber security professionals. Other UI laboratory facilities and equipment are exhibited in Appendix A. However, the needs of the State of Idaho for talented and experienced professionals in cybersecurity currently far exceed our collective capacity to produce them. We continue to seek resources to grow our faculty, facilities and our across-the-state presence to deliver timely education and research in this critical area of need.

## **5. Specific project plan**

A holistic research, development, deployment, and demonstration (RDDD) strategy will be formed based upon some recognized principles of resilience toward achieving significant improvements in security management of CPCSs<sup>3</sup> to protect Idaho's industry. Accordingly, to achieve these improvements, we will pursue our four objectives as follows:

### **Objective 1 Strengthen our capacity**

We will strengthen research and educational capacity at the University of Idaho by hiring four new faculty, two in computer science and two in electrical engineering. In year one we will focus on building up our infrastructure to enable better connectivity and collaboration between UI, INL and BSU (e.g., developing some detailed plans/requirements and canonical local/remote activities/experiments, establishing standards of interoperability and scoping out base line equipment and capabilities). About \$478,500 of our first year budget is devoted to start/up and search funds, operating software and supplies, tuition and fees for two graduate students as well as travel. This also includes \$297,000 for improved video/audio equipment and facility improvements to better connect UI faculty and labs at Moscow and Idaho Falls and those at BSU as well as enhancing the Power and RADICL labs on the Moscow campus. Also, we plan to hire the first new faculty in CS and a second in ECE which would account for the remaining

---

<sup>3</sup>Rieger, C.G., "Resilient Control Systems Practical Metrics Basis for Defining Mission Impact," 7<sup>th</sup> *Int'l Symp. on Resilient Ctl. Sys.*, Aug. 2014.

\$221,500 in year one (including two graduate students).

In year two, we will focus on faculty searches for the rest of the planned faculty hires and graduate students (\$589,500 in personnel expenses and \$110,000 otherwise) and consequently enable usage of the enhanced facilities in all three locations (Moscow, Boise and Idaho Falls) and development of proposals/plans for extramural funding.

**Objective 2 Strengthen collaboration**

In achieving greater collaboration, we will have linked ourselves through higher fidelity and ease from investments made for Objective 1 in year one with both INL (via our UI Idaho Falls site) and BSU, leveraging combined resources. Therefore, in year two we will begin to utilize these capabilities to synergize/collaborate in delivering cybersecurity education, research, and deployment activities. Moreover, we plan to seek internships by engaging our industry partners with a goal of 6/year: 3 CS and 3 ECE. (On a separate but potentially related project, Dr. Sheldon is currently working with Ken Edmunds at the State Department of Labor on a CS Co-op pilot program to educate students through industry experience and education. If successfully implemented, students will graduate in five years but with very useful experience across multiple employers.)

**Objective 3 Foster technology transfer**

In year three, will continue these activities (\$605,600 in personnel expenses and \$94,000 otherwise) including R&D, expansion of the UI Cybersecurity Training and Operations Center in Coeur d'Alene (including security assessments) and activities to initiate a Resilience Research Incubation Center in Moscow. We will conduct assessments with willing industry partners to better understand the threats and potential impacts of compromises associated with CPCSSs.

**Objective 4 Strengthen and expand the workforce**

This objective is a natural outcome from the prior three. By increasing our capacities to deliver education course work (both for credit and non-credit professional development) and research



and leveraging our INL/BSU partnerships, we will achieve this objective. Furthermore, providing internships and relevant targeted curriculum (especially related to cybersecurity), we will deliver more highly qualified graduates with first-rate hands-on education/experience for Idaho industry.

In summary, our overarching theme of security management for CPCSs will provide the basis to engage industry about our RDDD strategy thereby helping to strengthen capacity, collaboration, and technology transfer and workforce expansion. We will grow the research team (expertise), grow extramural funding (capital), develop technology (incubate and validate), and then commercialize solutions that underpin key sectors of the economy informed through intimate public/private partnerships. Letters of commitment and support from our partners are provided in Appendix C which highlight the needs to find robust, efficient, and intelligent ways to create/maintain resilient CPCSs. With the assistance of our partners, we will investigate the primary issues and hard problems underlying outstanding cybersecurity and resilience issues prevalent within Idaho's public-private sectors and devise practical/novel solutions/constructs on which future cybersecurity advances toward developing new products/services. We will effectively support decision makers as they discover how existing data/information can be acquired and fused with the effect of engendering greater understanding of cyber threats. We will develop adaptable intelligent data collection agents toward building greater situation awareness within organizations to enable modeling of complex interactions to enable high fidelity visualization and understanding of cyber weaknesses and potential impacts. We will contribute to the science of CPCSs and systematic cyber engineering as well as assessment and prioritized mitigation of emerging threats and provide continuing education about CPCSs cybersecurity principles to professionals in the field.

## 6. **Potential economic impact**

The architecture of the Nation's digital infrastructure, based largely upon the Internet, is neither

secure nor resilient. Without major advances in the security of these systems (e.g., CPCS) and significant change in how they are constructed and operated, it is doubtful that Idaho industry can protect itself from the growing threat of cybersecurity problems. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive information. Other intrusions threaten to damage portions of our critical infrastructure, especially our electric power infrastructure upon which all industry depends. Idaho industry is just as vulnerable as any place else in the US. Manufacturers among other sectors help to drive Idaho's economy however potential losses from improper security management of CPCSs are immense. As a state, we must address the challenges posed by these threats to strengthen our State's domestic security posture as described here through this IGEM Proposal. Given our capability in power engineering and security, the capability at the INL, and the growing capability at BSU, Idaho has the potential to be a national leader in research, development, deployment, and demonstration for CPCS. Personnel supported through this effort will seek to leverage the IGEM funds to acquire major federal and private research grants to further our four objectives.

In 2013, Idaho (the most recent published data) employed 632,328 workers supporting a gross domestic product of \$61Billion, which is even larger today. The majority of this economy is dependent on reliable infrastructure, especially electric power infrastructure. The U.S. Bureau of Labor Statistics reports that information security specialists can expect to enjoy rapid job growth of at least 18% over the next few years. The field predicts a *shortfall* nationally of up to 1.5 million cybersecurity professionals by 2019 and a disproportional number of these will be in Idaho if we do not grow our own. Information security professionals are some of the most sought-after workers in an already thriving sector, with industry reporting that these professionals can afford to be selective about the employers they agree to work for. Thirty-four percent of employees report that they will only consider working for a leading company, while

forty-four percent say a reputation for integrity is a must in an employer. Read more [here](#) (<http://goo.gl/z579Bs>).

## 7. **Criteria for measuring success**

The Security Management of CPCSS project metrics align with our 4 objectives.

### 1. [Strengthen our capacity:](#)

- 1.1. Hire four faculty: conduct searches (Yr 1); faculty start (Yr 1, 2)
- 1.2. Enhance and operationalize the current engineering laboratories: equipment purchases completed (Yr 1, 2); enhancements completed (Yr 2); connectivity between UI Moscow, UI Idaho Falls (IFs), and BSU completed (Yr 2).

### 2. [Strengthen collaboration:](#)

- 2.1. Number of significant collaborations with industry in Idaho (yearly)
- 2.2. IRON and video connectivity between UI Moscow, UI IFs, INL, and BSU demonstrated and used (Yr 2)
- 2.3. Number and success of collaborative research and educational projects started (yearly)

### 3. [Foster technology transfer:](#)

- 3.1. Number of research projects initiated and completed; dollar value of research awards and expenditures (yearly)
- 3.2. Number and dollar value of license agreements made (yearly)
- 3.3. Number of papers/reports submitted and published (yearly)
- 3.4. Number of startup ventures (yearly).

### 4. [Strengthen and expand the workforce:](#)

- 4.1. Number of persons completing credit and non-credit instruction (yearly)
- 4.2. Number of persons awarded degrees, certificates, and other post-secondary credentials (yearly)
- 4.3. Number of persons engaged in K-12 events/activities to support the talent pipeline (yearly)

We will manage items 1.1, 1.2, and 2.2 as milestones with respect to the bi-annual reporting to HERC. The other items (2.1, 2.3, 3.1-4, 4.1-3) will be reported as measures of success against project objectives stating increases over the course of the grant on a yearly (or bi-annual) basis.

## 8. **Budget**

Funds are requested to support new faculty hires and startup costs. There is also a modest

request for project management support from the PI and one Co-PI. Graduate students will be used to support the faculty in meeting the project objectives. The actual cost for graduate students will be higher but we will augment the IGEM funds with college and grant support. Total salary request is \$1,416,516. Other direct costs are for video/audio equipment (\$140,000), laboratory modernization (\$180,000) to enable collaboration as mentioned (Sections 3-5 and 7-8), travel (\$38,500), supplies (\$34,200), start-up funds (\$182,600), moving expenses (\$40,000), and graduate student tuition and fees (\$67,200) for a total request of \$2,099,016.

#### 9. **Budget justification**

This project will include three significant sectors of support: the UI, INL, and BSU. The UI and COE are fully behind this project (described in Section 4), including space available in the New IRIC (Integrated Research and Innovation Center) building. We also have existing laboratories and equipment located in Moscow and Idaho Falls that will become a part of this project. The UI permanently funded five faculty positions from the last IGEM capacity building project and is committed to permanently funding the four faculty positions at the conclusion of this grant to ensure what is developed will continue.

The management structure is very strong. Dr. Larry Stauffer, COE Dean, will provide overall project management and ensure project success. While not an expert in cybersecurity, in his fourth year as Dean he has demonstrated superior management acumen and can give this project the attention and authority for successful execution. He will facilitate communication and support with (1) upper administration of the university including the President, Provost/EVP and VP of Research, (2) administrators, faculty, and staff executing the project plan, all of whom report to him, and (3) external stakeholders. He will ensure the funds are used wisely and appropriately, objectives are met, responsible parties are held accountable, and grant reporting requirements are done correctly and on time. He has finance and administrative support from his office to assist in these responsibilities.

Frederick (Rick) Sheldon, Chair of the Department of Computer Science, will provide technical management of the project. He will be responsible for hiring the personnel and delegating responsibilities to existing faculty and staff to assure successful execution of the project plan. His expertise in cybersecurity and decade of previous experience at Oak Ridge National Laboratory makes him uniquely qualified to manage all technical project aspects. He has the department's financial and administrative support to ensure the tactical aspects of purchasing, accounting, and facilities/operations are appropriately managed. As Dr. Sheldon reports directly to Dean Stauffer, close coordination and support is ensured.

The Idaho National Laboratory (INL) in Idaho Falls has collaborated with us in the planning of this proposal and will be a significant partner if funded. In fact, Co-PI Michael Haney is on a Joint Appointment with the INL and the result of a joint search from the previous IGEM initiative in cyber security. We have a long history of working together on educational and research initiatives. As outlined in their letter of support we will partner on education, workforce development, and research activities. They will be part of our faculty search committees and where possible, provide additional financial resources to enhance this project.

The College of Engineering at Boise State University will collaborate with us in regard to building a distributed, cyber physical control systems laboratory. They have secured \$1 million from the legislature this year to establish a teaching and research laboratory in support of industrial control system cyber security. If this proposal to IGEM is funded, our two colleges will work together to build a more comprehensive laboratory, connecting both facilities through the IRON network as explained above. Outcomes from this initiative will build upon existing UI capabilities in cyber security and power engineering and enhance collaboration between our two programs. The letter of support from Dean Amy Moll describes their commitment towards this project.

# **Appendix A: Facilities, Equipment, and Other Resources**

## **General Laboratory Facilities**

This effort will be carried out at multiple UI locations and facilities. The Moscow, Idaho main campus and the Idaho Falls Center for Higher Education (IFCHE) and Center for Advanced Energy Studies (CAES) in Idaho Falls, as well as the Northern Idaho College campus in Coeur d'Alene will be the primary locations for this effort. Their facilities and capabilities are described in more detail below.

## **Teaching Capabilities and Resources**

In 2001, the National Science Foundation (NSF) created the Scholarship for Service (CyberCorps®) program and the UI was one of the first five schools in the nation to host a scholarship program specifically for students focusing on Information Assurance and Cybersecurity studies.

### **National Center for Academic Excellence in Information Assurance/Cybersecurity Education:**

The UI has been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a Center of Excellence in Information Assurance/Cybersecurity Education (CAE/IAE), and now in Cyber Defense Education (CAE/CDE). The first designation was in 1999 and later successfully renewed in 2005, 2008, and 2014. The current designation certificate expires in 2021: [https://www.iad.gov/niotp/reports/cae\\_designated\\_institutions.cfm](https://www.iad.gov/niotp/reports/cae_designated_institutions.cfm)

### **RADICL: A Hands-On Educational Computing Laboratory**

The UI's RADICL is the Reconfigurable Attack-Defend Instructional Computing Laboratory. The goal of this special purpose laboratory is to enable hands-on teaching and research in the areas of cybersecurity, cyber-defense, and modern computing platforms and networks. RADICL was originally created and implemented in 2003 by Computer Science and CyberCorps(R) Scholarship for Service students under the initiative and direction of Dr. Paul W. Oman and with

funding provided by NSF Award 0416757.

Since RADICL's inception, its computing and software infrastructure has gone through several improvements. The latest improvements, implemented in 2014, were funded by the State of Idaho under the Idaho Global Entrepreneurial Mission (IGEM). The current configuration of RADICL makes full use of virtualization features built into modern computing environments.

RADICL enables teams of students and researchers to create and deploy multiple independent experiments easily configurable and extensible. Within the context of these isolated experiments, students and researchers are able to design, implement, examine, explore, and develop a detail-oriented hands-on view of modern computing infrastructures, along with their associated applications and protocols, strengths, weaknesses, and vulnerabilities. Additionally, users are able to develop a clear, detail-oriented, hands-on understanding of the approaches, techniques, and tools used to *protect today's computing systems and applications*. RADICL is a dedicated and isolated platform that enables students to prepare and practice for cyber defense competitions, such as the Pacific Rim Collegiate Cyber Defense Competition (PR-CCDC) and the CSAW Capture the Flag Competition. RADICL is a world-class and state-of-the-art computing laboratory that enables hands-on and student-oriented instruction as well as an excellent medium for hands-on graduate and undergraduate research.

### **Research and Development Facilities**

#### **Power Applications Laboratory (PAL)**

The UI's Power Applications Research Group facilities in Moscow include educational and research laboratory facilities and office space for students. The laboratory facilities include an analog model power system that is capable of simulating interaction of control and protection hardware in a network with up to five lines of up to 300 miles length that can be arbitrarily cut and connected together. Our system protection hosts a full complement of Schweitzer

Engineering Laboratories (SEL) protective relays and a fault generator capable of any type of

common fault with any fault impedance and any duration from balance of a 60 Hz cycle to two minutes at a 50usec tolerance on fault initiation. Multiple generation sources can be interfaced with the system including synchronous machines, a doubly fed induction generator and power electronically coupled generation. Our laboratory floor in this lab has 983 square feet of space for experiments. The lab also includes a SCADA test-bed that is set up for Synchrophasor measurement and control studies.

In addition, the laboratory has a real time digital simulator with two racks, providing the ability to model somewhat larger systems with more generators. The real time digital simulator can runs electromagnetic transients simulations and perform data input/output in real time relative to common power systems measurement equipment such as PMUs and relays. The lab facilities have been built up through a working relationship with POWER Engineers, Schweitzer Engineering Laboratories, Idaho Power and Avista in addition to federal research grants.

The lab facilities also include an electric power laboratory with DC power sources rated 125V / 250V DC at 400/200 Amps. Our AC is 120V, 240V three phase at 50kVA each. We have three other individual DC generation sets at 120V, 100A each and two synchronous and three induction machines at 10hp, each with its own dynamometer capability. Our five individual DC electronic power supplies are 120V, 7A. We have a full complement of instruments to support measurements at these levels. Our laboratory floor in this lab has 4681 square feet of available space in a main open bay and three separate secure rooms to set up experiments. Available software tools include the following general-purpose tools: Matlab, Mathcad, and LABView, in addition to power system specific software tools such as Powerworld, DSATools, ATP, and PSCAD/EMTDC.

#### Center for Secure and Dependable Systems (CSDS)

The Idaho State Board of Education established the Center for Secure and Dependable Systems (CSDS) at the UI in response to the overwhelming need for computer-related security education



and research. CSDS comprises faculty in the areas of Computer Science, Business, Electrical and Computer Engineering, Civil Engineering, Mathematics, and Sociology, including associates at Idaho National Laboratory (INL) and Pacific Northwest National Laboratory (PNNL), over 30 students, and 3,000 square feet of laboratory and office space. It is housed in the Janssen Engineering Building, on the Moscow, Idaho campus, faculty offices are not included in the space totals for CSDS.

Completely self-funded, CSDS brings together collaborative research and efforts and serves as an educational focal point for the design, development, analysis, and use of technologies that result in secure and dependable computing systems and networks. CSDS is also a leader in Information Assurance and Cyber Defense education in the Northwest.

#### National Institute for Advanced Transportation Technologies (NIATT)

The University of Idaho's National Institute of Advanced Transportation Technology, is a U.S. Department of Transportation center of excellence. NIATT's mission is to develop engineering solutions, both knowledge and technology, to transportation problems for the state of Idaho, the Pacific Northwest, and the United States, and to prepare our students to be leaders in the design, deployment, and operation of our nation's complex transportation systems. NIATT faculty and researchers engage in research to solve challenging, practical, and relevant transportation problems that have regional and national significance.

#### The Center for Advanced Energy Studies (CAES)

CAES is a research and education consortium between the INL, Boise State University, Idaho State University, University of Idaho, and University of Wyoming. Through its collaborative structure, CAES combines the efforts of these five research institutions to provide timely research support on both technical and policy issues. The 55,000-square-foot CAES building is located on University Boulevard in Idaho Falls, near both Idaho State University's University Place campus and the INL's education and research campus. All five CAES partners have

faculty, staff, and students who collaborate in interdisciplinary approaches to solve today's energy problems. The CAES facility is one of the few LEED-certified buildings in Idaho.

CAES has a host of instruments and various laboratories and computing facilities as part of its public/private collaborative mission. Laboratories include the Advanced Materials Laboratory, Radiochemistry Laboratory, Analytical Chemistry Laboratory, Analytical Instrumentation Laboratory, Geothermal Fluids Laboratory, Microscopy and Characterization Suite (MaCS), Advanced Transportation Laboratory, and the state-of-the-art Computer Assisted Virtual Environment (CAVE) used for advanced data visualization and human-computer interaction research. CAES also has several collaborative centers, which help focus resources in critical energy areas and partner with CAES researchers and staff, such as, the Autonomous Systems Center of Excellence (ASCE), Nuclear Science User Facilities (NSUF), Energy Policy Institute (EPI), CAES Energy Efficiency Research Institute (CEERI), and the Center for Space Nuclear Research (CSNR).

### **General University of Idaho and College of Engineering Resources**

#### **The University of Idaho**

The UI is the leading research university in the State of Idaho and a land grant university established in 1889. The student enrollment is about 11,500 and the annual research expenditures are about \$100 million. The university offers 130 bachelor, 88 master, and 32 doctoral majors. The main campus is located in Moscow, Idaho and it spans 1,585 acres; these include 80 acres of arboreta and 860 acres of farms. The university offers students a friendly academic environment with access to all necessary resources for student success. In addition to the centers and computing facilities dedicated to computing and cybersecurity related education and research, which are described below, the university's Information Technology Services maintains 22 computer laboratories dedicated to academic use.

#### **The College of Engineering**

The UI's College of Engineering is composed of 6 academic departments and 5 research and development centers. The college has about 200 faculty and staff that supports a student body of 1500 undergraduate students and 350 graduate students. The College of Engineering has several full-time dedicated Information Technology (IT) personnel and two full-time IT system administrator dedicated exclusively to manage research infrastructure. Our research infrastructure includes many fully virtualized modern servers and supporting network infrastructure, among other specialized computing equipment. In addition, the Computer Science department has a full-time dedicated systems administrator working to ensure the availability of teaching computing infrastructure and systems.

#### The University of Idaho Library

The UI library houses over a million books and almost ten thousand periodical subscriptions, in print and online. It has served for over a century as an official regional depository of U.S. federal government publications, making almost two million government documents available to the public. The library's Special Collections are an invaluable resource for researchers, providing access to historical photographs, state documents, university historical materials, rare books, digital collections, and the International Jazz Collections, the premiere jazz archives of the Pacific Northwest.

## **Appendix B Biographical Sketches**

Larry Stauffer, Dean, College of Engineering

Fredrick Sheldon, Chair, Computer Science (CoE, Moscow)

Daniel Conte de Leon, Computer Science (CoE, Moscow)

Michael Haney, Computer Science (CoE, Idaho Falls)

Brian Johnson, Electrical and Computer Engineering (CoE, Moscow)

Larry Stauffer, Ph.D., P.E.

### **Professional Preparation**

Ph.D., Mechanical Engineering, 1987, Oregon State University

M.S., Agricultural Engineering, 1979, Virginia Polytechnic Institute and State University

B.S., Mechanical Engineering, 1978, Virginia Polytechnic Institute and State University

### **Appointments**

2011-present: Dean, College of Engineering, *University of Idaho*

1995-present: Professor of Mechanical Engineering, *University of Idaho*

2009-2011: Senior Associate Dean, College of Engineering, *University of Idaho*

1995-2009: Director, College of Engineering Boise, *University of Idaho*

1987-1995: Associate Professor of Mechanical, *University of Idaho*

1992, 94-95: Shared Faculty, *Hewlett-Packard Company*, Boise, Idaho

1979-1983: Design Engineer, *Westinghouse Electric Corp.*, Idaho Falls, Idaho

### **Selected Publications**

Domain 8 Management of Technology, Research, and Development, *A Guide to the Engineering Management Body of Knowledge*, 3<sup>rd</sup> Edition, 2012, ISBN 978-0-9831005-3-9; revised 2015. Book Chapter.

Pawar, T., L. Stauffer, T. Ives, and D. Abramsohn. "Analysis of the Toner Charging Process in a Single Component Non-magnetic Development System", *Journal of Imaging Science and Technology*, 58(3), 2014

Ruyf, C. and L.A. Stauffer. "The Perception of Women Engineers by Men and Women Co-workers", *Proceedings of the 32<sup>st</sup> ASEM National Conference*, October, 2011

Matson, E.L. and L.A. Stauffer. "Developing an Assessment Tool for Two Organizations Using Six Sigma Principles", *Engineering Management Journal*, 21(4), 2009

Perry, K. and L.A. Stauffer. "Multiple Views of Motivational Factors in a Federal Research Laboratory", *Proceedings of the 30<sup>th</sup> ASEM National Conference*, October, 2009

Helgeson, S. and L.A. Stauffer. "Indian Health Service Strategic Planning Using Design for Six Sigma", *Proceedings of the 28<sup>th</sup> ASEM National Conference*, November, 2007

Phillips, B. and L.A. Stauffer. "Managing Product Development Projects When Manufacturing Is Overseas", *Engineering Management Journal*, 18(4), pp. 23-27, 2006

Kirby, A.D. and L.A. Stauffer. Analysis of Pin Characteristics for a Variable Geometry Mold" *Journal of Manufacturing Systems*; fall 2006

Stauffer, L.A., Rule, R., and H. Ren. "A Template for Design for Manufacturing Guidelines," *2003 ASME Design Technical Conferences, Chicago, Ill., September 9-12, 2003*

Maupin, A.J., and L.A. Stauffer. "A Design Tool to help Small Manufacturers Reengineer a Product Family," *Proceedings of the 2000 ASME Design Technical Conferences, Baltimore, Maryland, September 10-13, 2000*

Gershenson, J.A., and L.A. Stauffer. "A Taxonomy for Design Requirements from Corporate Customers," *Research in Engineering Design*, Springer-Verlag. 11(2), pp. 103-115, 1999

Morris, L.J., L.A. Stauffer, and D.V. Khadilkar. "Eliciting and Managing Information for Product Definition," *International Journal of Computers and Industrial Engineering*, Elsevier Science Ltd., 31(3), pp. 665-668, 1996

### **Selected Professional Activities**

Member, American Society of Mechanical Engineers (ASME), 1986-present  
Session Chair, ASME-Design Theory & Methodology Conference, 1990, 92, 02, 05  
Program Chair, ASME-Design Theory & Methodology Conference, 1991  
Conference Chair, ASME-Design Theory & Methodology Conference, 1992, 93, 95  
Reviewer, ASME-Design Theory and Methodology Conference, 1989, 90, 92-2007  
Member, American Society of Engineering Management (ASEM), 2006-present  
Board of Directors and Communications Committee Chair, 2009-2011  
Session Chair, ASEM Annual Conference, 2007, 2008, 2010, 2011  
Reviewer, ASEM Annual Conference, 2005-present  
Member, American Society of Engineering Education (ASEE), 1987-present  
Engineering Deans Council, 2011-present  
Associate Editor, *Engineering Management Journal*, 2009- present  
Scientific Advisory Board, Bi-Annual DESIGN Conference, 2005-present  
Executive Team and Review Board, Idaho Quality Award, 1999 - 2003

### **Selected Collaborations**

Dr. Stauffer was on the core team that established Idaho TechHelp in 1996 and served as the University Director for 15 years. TechHelp is Idaho's manufacturing extension organization and a partnership between BUS, ISU, UI, and NIST. He also developed curricula for teaching lean principles for workforce training.

Dr. Stauffer was a collaborator on a UI project sponsored by the Micron Foundation to better understand the factors that influence students' motivation for entering STEM fields. The UI is in the final year of this project and presently summarizing project results.

**Frederick T. Sheldon, Ph.D.**  
**Professor and Chair of Computer Science**  
**University of Idaho, JEB 237, Moscow, Idaho 83844-1010**  
**(208) 885-6501 | sheldon@uidaho.edu**

**Professional Preparation**

**University of Texas at Arlington, College of Engineering**

Ph.D. in Computer Science May 1996, and MS in Computer Science August 1988

**University of Minnesota, Institute of Technology and College Biological Science**

BS in Computer Science December 1983, and BS Microbiology December 1977

**Appointments**

Academic experience

**University of Idaho, Department of Computer Science From: 7/15 – Present**

*Professor and Chair*

**Wuhan University, Int'l School of Software Engineering From: 5/15 – Present**

*Visiting Professor China's High-end Foreign Expert Program*

**University of Memphis, Department of Computer Science From: 8/14 – 9/15**

*Visiting Associate Professor*

**Washington State University, School of EECS Period: 06/99 – 09/02**

*Assistant Professor*

**University of Colorado Colorado Springs, College of EAS Period: 08/96 – 06/99**

*Assistant Professor, Computer Science Department*

**University of Texas at Arlington, College of Engineering Period: 01/93 - 05/96**

*Assistant Instructor, Computer Science and Engineering Department*

Non-academic full time experience

**Acadia Cyber Solutions LLC Period: 9/13 – Present**

Principal Consulting Engineer leading partnerships and proposal development

**Siemens, Industry US Period: 12/13 – 04/14**

Cyber Security Services Architect for industrial control systems security risk assessments, mitigations and security operations center for NIST SP 800-82.

**Oak Ridge Nat. Lab., Computational Sci. & Engr Div. Period: 09/02 – 09/13**

Senior Research Scientist (Q-Cleared), Cyberspace Sciences & Info. Intelligence Research Group, Cyberwarfare Research Team: Principle Investigator, Author, and Co-Inventor

**Daimler AG, Mercedes-Benz Research and Development Period: 07/01 – 08/02**

Research Scientist and Software Engineer working in software safety

**ASEE Scholar, Stanford U. & NASA Ames Research Ctr. Period: 6/97–8/98 summers**

**NRC of the Nat. Academies, NASA Langley Research Ctr. Period: 06/96 – 08/96**

Research Associate (postdoc), Flight Electronics Technology Division

**Lockheed Martin Aeronautics Company Period: 10/88 – 1/93**

01/90 - 01/93: Engineering Specialist (promoted 1992), Avionics R&D, Lead GIMADS Task 29: Generic Integrated Maintenance and Diagnostic Systems Formal Methods SW Task; 10/88 - 01/90: Senior Engr, Adv. Avionics Dev., Lead the YF-22 Vehicle Mgmt. Kernel Sys. Dev.

**Raytheon Period: 7/84 -10/88**

9/87 -10/88: Test Engineer, Test Automation Dept., Developed Built-In-Test SW for YF-22 VMS computers (ASIC) boards; 7/84 -09/87: Software Design Engineer, Avionics Systems/Radar Div., Developed test SW and HW diagnostics for turn-key LRUs (Tornado Line Replaceable Units).

**Products (Publications, patents and presentations from past five years)**

- Chen, Q., Abdelwahed, S., Morris, T. and Sheldon, F.T., “Model-based Autonomic Security Mgmt. of Cyber Physical Infrastructures,” Int'l Jr. of Crit. Infrastructure Protection, Elsevier, to appear 2016.
- Chen, Q., Abercrombie, R.K., and Sheldon, F.T., “Risk Assessment for Industrial Control Systems Quantifying Availability Using Mean Failure Cost,” JAISCR, 5:3 (2015): 205-220.
- Aissa, A.B., Abercrombie, R.K., Sheldon, F.T. And Mili, A., “Quantifying Availability Using Mean Failure Cost in Cyber-Physical SCADA Environments,” IEEE SSCI/CIS, Orlando, Dec. 9-12 2014.

- Sheldon, F. T. and J. Todd McDonald, "[Introduction to the Special Issue on Cyber Security and Management](#)," Info Sys E-Bus Manage, Springer (2012) 10:429–431.
- Sheldon, F.T., et. al., Prime Editor of the 2<sup>nd</sup> – 8<sup>th</sup> ACM Proc. Cyber Security and Info. Intelligence Research Wkshp, 8<sup>th</sup> Ann entitled "Federal Cyber Security R&D Program Thrusts," Jan 8-10, '13.
- Sheldon, F.T., Webber, J.M., Yoo, S-M and Pan, W.D., "[Insecurity of Wireless Networks](#)," [IEEE Security and Privacy Magazine](#) SI on Internet Infrastructure Security, 10:4, pp. 54-61, July 2012.
- R. K. Abercrombie, L.M. Hively, S.J. Prowell, B.G. Schlicher and F.T. Sheldon, "[Forewarning of Failure in Complex System](#)," [Journal of Homeland Security](#), 5:1, pp. 1-16, June, 2011
- B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "[Defining and Computing a Value Based Cyber-Security Measure](#)," [Information Systems and E-Business](#), Springer, London: 23 Apr. '11.
- Hively, L.M., Sheldon, F.T. and Squicciarini, A., "[A Vision for Scalable Trustworthy Systems](#)," [IEEE Security and Privacy](#), 9:3 July/Aug 2011.
- Sheldon, F.T., and Vishik, Claire, A., "[Moving Toward Trustworthy Systems: R&D Essentials](#)," [IEEE Computer](#) 43:9, 31-40, September 2010.
- Aissa, A.B., Abercrombie, R. K., Sheldon, F.T., Mili, A., "[Quantifying Security Threats and Their Impact: Theory and Practice](#)," [Innovations in Sys. and SE](#), (Springer) 6:4, 269-281, Mar. 2010.
- Kirkpatrick, M., Bertino, E., and Sheldon, F.T., "Restricted Authentication and Encryption for Cyber-physical Systems (CPS)," Proc. DHS Wkshp Future Directions in CPS Security, Newark, Jul 22-24, '09.
- US Patent 8,762,188 B2 Cyberspace Security System, F.T. Sheldon, E.M. Ferragut and R.K. Abercrombie, June 24, 2014.
- US Patent 20140006332 A1 Scientometric Methods for Identifying Emerging Technologies, F.T. Sheldon, B.G. Schlicher, and R.K. Abercrombie, June 26, 2013.

### **Synergistic Activities**

PI/Co-PI or PM for R&D projects including: (1) SCI-FI: Supply Chain Integration For Integrity, DOE \$750K/\$3M, (2) DDDAS-based Resilient Cyberspace (DRCS) [Dynamic Data Driven Applications Systems], AFOSR \$200K/\$1.2M, (3) Island World: A Small World Simulation Tool in a Virtual Community for Evaluating Environmental Stressors, IC \$240K, (4) Cyber Sciences Laboratory ([CSL](#)) Implementation, NNSA OCIO request for Cyber Security Grassroots Support for 8 DOE Laboratories \$1.3M, (5) Cyber Security and Information Intelligence Workshop (7<sup>th</sup> Annual 2011) DOE \$150K, (6) Application for Centralized Cryptographic Key Management, DOE/CEDS \$706/\$3.056M, (7) Studies to Improve the Precision and Accuracy of Network Tomography, IC \$240K, (8) Advanced Data Fusion Methods for Veracity Scoring, IC \$240K, (9) Thwarting Online Deception and Phishing with Honeypots and DNS Analysis, LDRD \$200K, (10) Weigh in Motion (WIM) and the Automated In-Motion Vehicle Evaluation Environment (AIMVEE), DoD/ USTRANSCOM \$7.5M

General / Pgm Chair: Cyber Security and Information Intelligence Research Workshop [CSIIRW05-13]

### **Collaborators**

Drs. Brian Witten (Symantec), Anish Arora (Ohio State U.), Richard Brooks (Clemson Univ.), Sandeep Kulkarni (Michigan State U.), Christopher Griffin (Penn State U.), Masoud Amin (U. of Minn.), Al Hevner (USF), Michael Langston (U. Tenn.), Dennis Kafura (VA Tech.), Axel Krings and Paul Oman (U. of Idaho), Michael Hinchey (Lero), A. Mili (New Jersey Institute of Technology/Rutgers U.), and Stacy Prowell (CMU), Yoohwan Kim (UNLV).

### **Graduate Advisors**

Ph.D. advisor: Dr. K Krishna Kavi (currently at University of North Texas)

### **Advisees**

DHS Fellows (Steven McKinney and Joseph Calandrino), Ph.D. Advisor: Stefan Greiner; M.S. Advisor: David Dugan, Kshamta Jerath, Zhihe "Bill" Zhou, Hye Yeon Kim, Rick Mahoon, Shuren Wang, Wen Wei, Norb Gravelle, and David Owens.



## Biographical Sketch – Daniel Conte de Leon

Assistant Professor of Computer Science,  
Center for Secure and Dependable Systems and Computer Science Department,  
University of Idaho, Moscow, Idaho, 83844-1010, U.S.A.  
Phone (208) 885-6520. Email: dcontedeleon@uidaho.edu

### Professional Preparation

UCUDAL, Montevideo, Uruguay, Major: Informatics, Degree: Inf. Analyst, Year: 1998.  
Univ. of Idaho, Moscow, Idaho, Major: Computer Science, Degree: MS, Year: 2002.  
Univ. of Idaho, Moscow, Idaho, Major: Computer Science, Degree: PhD, Year: 2006.

### Appointments

Assistant Professor of Computer Science 2013 – Present  
Department of Computer Science, University of Idaho (UI), Moscow, Idaho, U.S.A.  
Associate Professor of Computer Science (Started as Visiting) 2007 – 2013  
Lewis-Clark State College, Lewiston, Idaho, U.S.A.  
Postdoctoral Researcher, 2006,  
Center for Secure and Dependable Systems, University of Idaho (UI), Moscow, Idaho, U.S.A.

### Products

1. Luay A. Whasheh, Daniel Conte de Leon, and Jim Alves-Foss, “Formal Verification and Visualization of Security Policies,” **Journal of Computers (Academy JCP)**, Volume 3, Issue 6, June 2008, pages 22-31, Academy Publisher, Oulu, Finland.  
<http://academypublisher.com/jcp/vol03/no06/jcp03062231.html>
2. Daniel Conte de Leon and Jim Alves-Foss, “Hidden Implementation Dependencies in High Assurance and Critical Computer Systems,” **IEEE Transactions on Software Engineering (IEEE-TSE)**, Volume 32, Number 10, October 2006, pages 342-349, IEEE Computer Society, Los Alamitos, CA, U.S.A. <http://dx.doi.org/10.1109/TSE.2006.103>
3. Daniel Conte de Leon, Jim Alves-Foss, and Paul W. Oman, “Implementation-Oriented Secure Architectures,” **Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS-40)**, 03-06 January 2007, Big Island, HI, U.S.A. IEEE Computer Society, 2007.  
<http://dx.doi.org/10.1109/HICSS.2007.264>.
4. Paul W. Oman, Axel Krings, Daniel Conte de Leon, and Jim Alves-Foss, “Analyzing the Security and Survivability of Real-time Control Systems,” **Proceedings of the 5th Annual IEEE Information Assurance Workshop (IAW’04)**, 10-11 June 2004, U.S. Military Academy, West Point, NY, U.S.A. IEEE Computer Society, 2004. <http://dx.doi.org/10.1109/IAW.2004.1437837>.
5. Daniel Conte de Leon and Jim Alves-Foss, “Experiments on Processing and Linking Semantically Augmented Requirement Specifications,” **Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37)**, 05-08 January 2004, Big Island, HI, U.S.A. IEEE Computer Society, 2004.

## Synergistic Activities

1. **IEEE Standards Voting:** As a voting member of the IEEE Standards Association, I have carefully reviewed and voted on more than 10 standards, in many cases, multiple votes on revisions are needed. Two examples are: “*ISO/IEC/IEEE Systems and Software Engineering – Architecture Description*” and “*IEEE Draft Recommended Practice for the Use of Probability Methods for Conducting a Reliability Analysis of Industrial and Commercial Power Systems.*”
2. **Hands-On Instructional Computing Laboratory:** I manage the Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) at the University of Idaho. RADICL is a specialized, and virtually air-gapped computing laboratory, built with external funding from NSF and the State of Idaho IGEM program. This laboratory enables hands-on teaching and research in cybersecurity.
3. **ACM/IEEE Computer Science Curricula 2013:** I participated in the development of the ACM/IEEE Computer Science Curricula 2013 by giving feedback on the Strawman and Ironman versions and by preparing the Course Exemplar for the Computer Security course.
4. **CAE and Cybersecurity and Computer Science Curriculum:** I collaborate in the development of curricular and assessment materials for the Computer Science degree program and the Cybersecurity and Information Assurance emphasis program at the University of Idaho.
5. **University of Idaho Cybersecurity Advisory Committee:** I am the faculty at large representative in the UI cybersecurity advisory committee. This committee is a forum for collaboration regarding UI Information Technology Cybersecurity issues, implementation, and policy decisions.

## Collaborators and Other Affiliations (Total: 53)

### Collaborators and Co-editors (50):

*University of Idaho (UI) (20):* James Alves-Foss; Jeffrey J. Bailey; Kevin Chang; Tim Frazier; Michael Haney; Robert B. Heckendorn; Kristin Haltinner; Herbert L. Hess; Clinton Jeffery; Brian K. Johnson; Axel W. Krings; Michael Lowry; Paul W. Oman; Robert E. Rinker; Yvonne Sertich; Jia Song; Terence Soule; Frederick T. Sheldon; Karen Thurston; Philip Watson.

*Alward Institute (Alward): (1):* Stephen Cooke.

*Harbrick, Inc. (Harbrick): (1):* Joshua Hartung.

*Idaho National Laboratory (INL) (1):* Craig G. Rieger.

*iSec Partners (iSec) (3):* Jason Bubolz; Rachel Engel; Justin Engler.

*Lewis-Clark State College (LCSC) (2):* Jason Blazzard; Nina Peterson.

*Norfolk State University (NSU) (1):* Lu'ay A. Wahsheh.

*North Carolina State University (NCSU) (1):* Aranya Chakraborty.

*Oak Ridge National Laboratory (ORNL) (1):* Robert K. Abercrombie.

*University of Memphis (UM) (4):* Mohd Hasan Ali; Dipankar Dasgupta; Sajjan Shiva; Edgar Wyatt.

*University of North Carolina, Charlotte (UNCC) (4):* Ehab Al-Shaer; Badrul Chowdhury; Johan H. R. Enslin; Madhav Manjrekar.

*Syracuse University (Syracuse) (1):* Sara Eftekharnjad.

*University of Texas, Austin (UTA) (1):* Surya Santoso.

*Virginia Commonwealth Univ. (VCU) (4):* Karl R. Elks; Carol Fung; Ram Gupta; Milos Manic.

*Virginia Tech (VT) (5):* Charles Clancy; Odge Hutton; Nathan Lau; Joseph M. Ernst; James S. Thorp.

**Graduate Advisor and Postdoctoral Sponsor (1):** James Alves-Foss, University of Idaho.

### Former Graduate Students (2 total):

Venkata Anirudh Bhandari: MS-CS, June 2015, Private Company in California.

Nathan Krussel, MS-CS, May 2014 at Pacific Northwest National Lab (PNL).

## **Biographical Sketch – Michael Haney**

Assistant Professor  
Computer Science, University of Idaho  
mhaney@uidaho.edu

Cybersecurity Researcher  
Idaho National Laboratory  
208-533-8209

### **Professional Preparation**

University of Kentucky, Lexington, KY, Mathematics, BS, 1998  
The University of Tulsa, Tulsa, OK, Computer Science, MS, 2013  
The University of Tulsa, Tulsa, OK, Computer Science, PhD, 2015

### **Appointments**

08/2015 – present: *Assistant Professor*, Computer Science, University of Idaho  
08/2015 – present: *Research Scientist*, Center for Advanced Energy Studies  
08/2013 – 05/2015: Technology/Cybersecurity Consultant – IRB, Univ. of Tulsa, Tulsa, OK.  
08/2011 – 07/2013: Sr. Security Consultant – True Digital Security, Tulsa, OK.  
10/2008 – 08/2011: Sr. Security Consultant – FishNet Security, Boston, MA  
11/2002 – 09/2008: Manager (Consultant) – Ernst & Young, LLP, Boston MA  
02/2001 – 11/2002: Sr. Security Consultant – WiTel Communications (Level 3), Tulsa, OK  
04/2000 – 01/2001: Security Administrator, FCI Web Hosting, Seattle, WA  
02/1999 – 04/2000: Network Technician, Mindspring/Earthlink, Seattle, WA

### **Relevant Publications**

1. Haney, Michael. "System, Method, and Apparatus for Computer Security Monitoring, Information Sharing, and Collective Intelligence." U.S. Patent Application No. 62/031,023, filed July 30, 2014.
2. Fellin, Conor, and Michael Haney, "Preventing Mistraining of Anomaly-Based IDSs through Ensemble Systems," IEEE Services 2014, 2<sup>nd</sup> Cloud Security Auditing Workshop, June 2014.
3. Haney, Michael and Mauricio Papa, "A Framework for the Design and Deployment of a SCADA Honeynet", Proceedings of the 9<sup>th</sup> Annual Cyber and Information Security Research Conference. pp. 121-124. ACM, 2014. – Received "Best Paper" award.
4. Hawrylak, Peter J., Chris Hartney, Michael Haney, Jonathan Hamm, & John Hale, "Techniques to Model and Derive a Cyber-Attacker's Intelligence", In Efficiency and Scalability Methods for Computational Intellect. Igel'nik, Boris, and Jacek M. Zurada, editors. Information Science Reference, 2013.
5. Hawrylak, Peter J., Michael Haney, Mauricio Papa, and John Hale. "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid." In Resilient Control Systems (ISRCS), 2012 5th International Symposium on. IEEE, 2012.

## **Synergistic Activities**

- Information Systems Security Association, Oklahoma Chapter President, 2014 - 2015
- BSidesOK, first annual BSides conference in Oklahoma, founder and speaker, Tulsa, OK, April 18, 2015
- Information Warfare Summit 7, InfraGard, invited speaker, “Advances in Honeypots for Critical Infrastructure Protection”, Oklahoma City, OK, October 1, 2014
- Information Warfare Summit 6, InfraGard, invited speaker, “Seeing Clearly through the Fog of War”, Oklahoma City, OK, October 2, 2013
- Instructor for cyber security courses taught to Walmart Stores, Inc., SPAWAR, US Secret Service, and UK Royal Military Police

## **Collaborators and Other Affiliations**

### **Collaborators and Co-Editors (15):**

Conor Fellin, GoDaddy, Inc.	Peter Hawrylak, professor, Univ. of Tulsa
Michael Fisher, grad. student, Univ. of Tulsa	Liang Kong, Peritus Resource Group
Rose Gamble, professor, Univ. of Tulsa	Jessica Lin, grad. student, Univ. of Tulsa
David Greer, Oklahoma Innovation Institute	George Louthan, Oklahoma Innovation Institute
John Hale, professor, Univ. of Tulsa	Mauricio Papa, professor, Univ. of Tulsa
Matt Hale, professor, Univ. of Nebraska, Omaha	Jason Staggs, grad. student, Univ. of Tulsa
Jonathan Hamm, undergrad., Univ. of Tulsa	Charlie Walter, grad. student, Univ. of Tulsa
Chris Hartney, Waterfield Energy	

### **Graduate Advisors and Postdoctoral Sponsors (5):**

Jerry Dawkins, True Digital Security	Peter Hawrylak, University of Tulsa
Rose Gamble, University of Tulsa	Mauricio Papa, University of Tulsa
John Hale, University of Tulsa	

### **Thesis Advisor and Postgraduate-Scholar Sponsor (0):**

None.

**Brian K. Johnson, Ph.D., P.E.**  
Professor of Electrical Engineering  
University of Idaho, GJL 201, Moscow, Idaho 83844-1023  
(208) 885-6902; bjohnson@uidaho.edu

### **Professional Preparation**

University of Wisconsin-Madison, Madison, WI	Electrical Engineering	BSEE, 1987
University of Wisconsin-Madison, Madison, WI	Electrical Engineering	MSEE, 1989
University of Wisconsin-Madison, Madison, WI	Electrical Engineering	PhD, 1992

### **Appointments**

2015-present: Schweitzer Engineering Laboratories Chair in Power Engineering  
2004-present: Professor Electrical Engineering, University of Idaho  
2006-2012: Chair, Department of Electrical and Computer Engineering  
1997-2004: Associate Professor, Electrical Engineering, University of Idaho  
1992-1997: Assistant Professor, Electrical Engineering, University of Idaho

### **Products**

#### Five Products Related to this Proposal

1. T. R. McJunkin, C. G. Rieger, B. K. Johnson, D. S. Naidu, L. H. Beaty, J. F. Gardner, I. Ray, K. L. Le Blanc, M. Guryan, "Interdisciplinary Education through "Edu-tainment": Electric Grid Resilient Control Systems Course," *Proceedings of the 2015 Annual Conference of the American Society for Engineering Education*, Seattle WA, 14-17, June 2015
2. J.M. Klein, H.L. Hess, and B.K. Johnson, "Cooperative Methodology for Successful Integration of Undergraduate and Graduate Research Projects," *Proceedings of the 2008 Annual Conference of the American Society for Engineering Education*, Pittsburgh, Pennsylvania, 22-25 June 2008.
3. M. Alahmad, H. Hess, B. Johnson, "Project Based Approach to Introduce Building System Design in an Electrical Engineering Curriculum," *ASEE Annual Conference Proceedings*. Honolulu, Hawaii, June 24-27, 2007.
4. B. Johnson, H. Hess, J. Law, and V. Yedidi, "Creating Power Engineering Laboratory Experiences for Distance Education Students," *ASEE Annual Conference Proceedings*. June 2005, Session 1133, Portland, Oregon, June 12-15, 2005.
5. K. Eshghi, B.K. Johnson, C.G. Rieger, "Power System Protection and Resilient Metrics" *Proceedings of the 2015 Resilience Week*, Philadelphia, PA, August 18-20, 2015

#### Five Other Significant Products

1. M.P. Bahrman and B.K. Johnson, "The ABCs of HVDC Transmission Technologies," *IEEE Power and Energy*. Vol. 5, No. 2, pp. 32-44, March-April 2007.
2. W.V. Hassenzahl, D.W. Hazelton, B.K. Johnson, P. Komarek, M. Noe, and C.T. Reis, "Electric Power Applications of Superconductivity," *Proceedings of the IEEE*. Vol. 92, No. 10, pp. 1655-1674, October 2004.
3. P.F. Ribeiro, B.K. Johnson, M.L. Crow, A. Arsoy, and Y. Liu, "Energy Storage Systems for Advanced Power Applications," *Proceedings of the IEEE*. Vol. 89, No. 12, December 2001, pp 1744-1756.
4. S. Samineni, B.K. Johnson, H.L. Hess, and J.D. Law, "Modeling and Analysis of a Flywheel Energy Storage System for Voltage Sag Correction," *IEEE Transactions on Industry Applications*. Vol. 42, No. 1, pp. 42-52, January/February 2006.

## **Synergistic Activities**

1. IEEE Power and Energy Society (PES) Representative on the IEEE Council on Superconductivity (2006- present)
2. IEEE PES: Power and Energy Education Committee, (chair 2014-2015)
3. IEEE PES: Power and Energy Education Research Subcommittee, (chair 2010-2011)
4. IEEE PES: DC and FACTS Subcommittee, (secretary 2012-2014, vice-chair 2015-present)
5. Board of Governors, IEEE Intelligent Transportation Systems Society (2004-2008)

## **Collaborators & Other Affiliations**

### Collaborators and Co-Editors (52 total)

Ahmed Abdel-Rahim (UI), Katherine Aiken (UI), Lillian Allessa; (UI), John W. Anderson; (UI), James Alves-Foss (UI), Michael Bahrman (retired), Jeffrey J. Bailey (UI), Lyudmyla Barannyk; (UI), Fred D. Barlow (University of Alaska-Anchorage), Denise Bauer (UI), Ronald Boring (INL), Cliff Chapman (US Air Force), Karen Den Braven (South Carolina Gov.'s School for Science and Math), Gregory Donohoe (UI), Sara Eftekharnjad (Syracuse Univ), Donald Elger (UI), Hatim El-Sayed (Gulf Consolidated Countries Electricity Interconnection Authority), Normann Fischer (SEL), John Gardner (Boise State University), Mohsen Guizani (UI), William Hassenzahl (Advanced Energy Associates), Herbert L. Hess (UI), Rishabh Jain (NC State), Andrew Klisky (UI), Axel Krings (UI), Michael Lowry (UI), Michael Kyte (UI), Loi Lei Lai (State Grid Energy Res. Inst., Beijing), Joseph Law (UI), Jim C.P. Liou (UI), Leo Luckose (Burns & McDonnell), Milos Manic (VCU), Stephen Marx (BPA), Tim McJunkin (INL), Ali Mehrizi-Sani (Wash. State Univ.), Kyle Morse (UI), Greg Parker (Micron Technologies), Craig Rieger (INL), Mark Roberts (NSWC-CCD), Mark Roll (UI), Michael Santora (UI), Yvonne Sertich (UI), Sunil Sharma (UI), Veselin Skendzic (SEL), Terence Soule (UI), Nicholas Urlaub (POWER Engineers), Douglas I. Taylor (SEL), Ivo Uglesic (University of Zagreb), Steffern Werner (UI), Cat Wong (Entergy), Richard W. Wall (UI), Quanyan Zhu (NYU)

### Graduate Advisors and Postdoctoral Sponsors (1 total)

Robert H. Lasseter (University of Wisconsin-Madison)

### Thesis Advisor and Postgraduate-Scholar Sponsor (42 total in last five years)

Mohamed Abuagreb (UI), Fahad Alhajeri (UI), Mohammed Allehyani (UI), AlMutaim AlSammari (Texas A&M), Alaap Anujan (UI), Mahipathi Appannagari (SEL), Arturo Barradas (Ivesco), Hussain Beleed (UI), Amrit Dahal (UI), Nathan Davis (UI), Abosalah El Medhi (Azzaytuna University, Libya), Oluwaseun Fasanya (UI), E. E. Héctor Esponda Hernández; (UANL), Armando Guzman (SEL), Li Hang (SEL), Shawn Holder (PG&E), Daniel Johnston (Idaho Power), Achyut Lamichhane, Jon Leman (POWER Engineers), Babak Malek (American Electric Power), Andrew Miles (UI), Ahmed Momen (UI), M. Venkat Mynam (SEL), Trung Nguyen (SEL), Pavan Penkey (UI), Peter Pietramala (Eaton), Enrique Quintero (PG&E), Sherwood Polter (NSWC-CCD), Nathan Powell (Pacifcorp), Ankita R. Roy (SEL), Salah Jadid (SEL), Satish Samineni (SEL), Husam Samkari (UI), Alejandro Schnakofsky (ABB), Don Scoffield (Idaho National Laboratory), Julian Sotelo (CINVESTAV University), John Stubban (POWER Engineers), Nathan Wiedeback (POWER Engineers), Michael West (UI), Yu Xia (SEL), Vinod Yedidi (SEL), Liman Zhuang (Seattle City Light).

## **Current and Pending Support: [Brian K. Johnson, University of Idaho]**

### **Support: Current**

Project/Proposal Title: Online Synchronous Machine Parameter Estimation  
Source of Support: Schweitzer Engineering Laboratories, Inc.  
Total Award Amount: \$155,037  
Total Award Period Covered: 08/15/2014 to 07/31/2016  
Location of Project: Moscow, ID  
Role in Project: PI  
Person-Months per Year Committed to the Project: Cal: 0.0 Acad: 1.00 Sumr: 0.46

Project/Proposal Title: University of Idaho College Engineering Career Launch  
Source of Support: National Science Foundation – DUE – S-STEM  
Total Award Amount: \$631,482  
Total Award Period Covered: 06/01/2015 to 05/31/2020  
Location of Project: Moscow, ID  
Role in Project: PI  
Person-Months per Year Committed to the Project: Cal: 0.0 Acad: 0.18 Sumr: 0.0

Project/Proposal Title: TWC: Small: Securing Smart Power Grids under Data Measurement Cyber Threats  
Source of Support: Syracuse University (subaward from NSF SaTC Small)  
Total Award Amount: \$210,680  
Total Award Period Covered: 09/01/2015 to 08/31/2018  
Location of Project: Moscow, ID  
Role in Project: PI  
Person-Months per Year Committed to the Project: Cal: 0.70 Acad 0.0 Sumr: 0.00

Project/Proposal Title: Smart Wires for Increasing Transmission and Distribution Efficiency  
Source of Support: Avista Corporation  
Total Award Amount: \$75,044  
Total Award Period Covered: 09/01/2015 to 08/31/2016  
Location of Project: Moscow, ID  
Role in Project: PI  
Person-Months per Year Committed to the Project: Cal: 0.23 Acad: 0.0. Sumr: 0.0

Project/Proposal Title: Critical Load Serving Capability by Optimizing Microgrid Operation  
Source of Support: Avista Corporation  
Total Award Amount: \$79,855  
Total Award Period Covered: 09/01/2015 to 08/31/2016  
Location of Project: Moscow, ID  
Role in Project: co-PI  
Person-Months per Year Committed to the Project: Cal: 0.175 Acad: 0.0 Sumr: 0.0

Project/Proposal Title: Smart RPM Integration with Traffic Signal Systems  
Source of Support: Idaho Department of Commerce-IGEM  
Total Award Amount: \$350,000  
Total Award Period Covered: 10/19/2015 to 05/15/2017  
Location of Project: Moscow, ID  
Role in Project: co-PI  
Person-Months per Year Committed to the Project: Cal: 0.93 Acad: 0.0 Sumr: 0.0

**Support: Pending**

Project/Proposal Title: Critical Infrastructure Resilience as an Edutainment Platform to Excite Students and Advance Multidisciplinary Education Studies  
Source of Support: National Science Foundation – IUSE  
Total Award Amount: \$499,133  
Total Award Period Covered: 08/15/2016 to 08/14/2019  
Location of Project: Idaho Falls, ID/Moscow, ID  
Role in Project: PI  
Person-Months per Year Committed to the Project: Cal: 0.23 Acad: 0.0. Sumr: 0.93



## **Appendix C Letters of Support**

Idaho National Laboratory

Boise State University

Micron Technology, Inc.

Schweitzer Engineering laboratories, Inc.

Idaho Forest Group

Idaho Falls Power

Power Engineers

Community Security Coalition

Kootenai Health

Avista

Hewlett Packard

Idaho Power

March 24, 2016

CCN 237866

Dr. John "Jack" McIver, Vice President for Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

SUBJECT: Support for the Idaho Global Entrepreneurial Mission (IGEM) Initiative Grant Proposal  
from the University of Idaho (UI)

Dear Dr. McIver:

Idaho National Laboratory (INL) is pleased to support UI's proposal to strengthen research and educational capacity in the area of security management of cyber physical control systems (CPCSs). The proposal will enable UI to build upon its existing foundation in cyber security research to develop transformative solutions specifically targeted to address the increasingly vulnerable CPCSs. This multidisciplinary, multiagency initiative will provide for better collaboration with INL and Idaho industry, accelerating economic development through research, development, demonstration, and deployment.

As one of the Department of Energy's seventeen multi-program laboratories and one of Idaho's largest employers, INL strongly advocates programs that improve science, technology, engineering, and math (STEM) skills. One of the three focuses of our new vision is to secure and modernize critical infrastructure. The research and curriculum proposed for this project is of great interest to both INL and industry. In particular, we support the collaboration with Boise State University on a more comprehensive cyber physical control systems laboratory.

Should this program come to fruition, INL will continue to collaborate with UI in areas of mutual interest, and where possible, provide financial resources to leverage or match UI's resources. These combined resources will provide course offerings that would accommodate participation by our personnel; advertise and encourage INL employees to take classes in future years; consider UI students for intern and postdoctoral assignments, and collaborate on joint research projects.

There is a significant and growing need to address the challenges presented by an aging workforce. Also noteworthy is the increasing skill levels required of individuals to be successful in the various disciplines that support the energy field. To meet the needs of the future workforce, it is vital that we increase the number of students entering energy, computer science, cybersecurity, and the computational sciences.

INL has a long history with UI and works closely with you on a variety of energy-related activities, programs, and projects. Programs proposed by UI encourage more students to pursue STEM careers and help further our goal of addressing INL's workforce needs.

INL looks forward to participating on the proposed efforts.

Sincerely,



Brent J. Stacey, Associate Laboratory Director  
National and Homeland Security



March 24, 2016

John McIver, Vice President for Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

The College of Engineering at Boise State University supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This project will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UI capabilities in cyber security and power engineering and enhance collaboration between our two programs.

The College of Engineering at Boise State University has a growing computer science program and has been awarded \$1 million from the legislature this year to establish a cyber physical control systems laboratory in partnership with the Idaho National Laboratory. If this attached UI proposal is funded, our two colleges can work together to build a more comprehensive and distributed laboratory, connecting both facilities through the IRON network. By connecting our facilities we can focus on our strengths and reduce duplication of effort. It will allow for more effective research and educational initiatives, supporting industry better together than either of us can do alone. The whole is greater than the sum of its parts, combining researchers, faculty and students from all three institutions creating greater flexibility, more diversity and leveraged opportunity.

In summary, I strongly support this proposal. We look forward to collaborating with the University of Idaho on this important project.

Sincerely,

Amy Moll, Dean  
College of Engineering  
Boise State University



March 16, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

Micron Technology strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UI capabilities in cyber security and develop solutions to address Idaho industries' increasingly vulnerable CPCSs.

As an Idaho industry leader, Micron employs 30,000 people around the world, about 6,000 of them in Idaho. As consumer products continue to evolve, our DRAM customer base and demand has shifted. We are constantly innovating and advancing into new markets, thoughtfully moving into the space of a customer-centric solutions provider. These evolutions in our business amplify the need for Micron to focus on cyber security research and deployment activities. This UI initiative would bring value to our industry and business.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idahoan stakeholders. Moreover, this multidisciplinary, multiagency initiative offers opportunity for better collaboration with Idaho National Laboratory (INL) and the UI which we expect will accelerate economic development in the State through research, development, demonstration and deployment (RDD&D); a process advocated by INL's National Innovation Center. This new way of operating has become essential within our industry.

Strategic workforce development is a high priority at Micron and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

In summary, I strongly support the activities described herein. Micron will benefit from this cyber security research and workforce development. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. Micron is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

A handwritten signature in black ink, appearing to read 'Trevor Schulze', with a long horizontal stroke extending to the right.

Trevor Schulze

Chief Information Officer

Micron Technology, Inc.



**SCHWEITZER ENGINEERING LABORATORIES, INC.**

2350 NE Hopkins Court • Pullman, WA 99163-5603 USA  
Phone: +1.509.332.1890 • Fax: +1.509.332.7990  
www.selinc.com • info@selinc.com

March 22, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

Schweitzer Engineering Laboratories supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UoI capabilities in cybersecurity and power systems and develop solutions to help ensure Idaho industries' CPCSs remain secure.

As an industry leader, Schweitzer Engineering Laboratories recognizes the importance of dependable electric power. With the proliferation of standardized communications and computer networks comes the exposure of critical infrastructures to cybersecurity risks. With R&D and manufacturing operations in Idaho and many locations throughout the world, SEL understands the need to focus on cybersecurity research and deployment activities. This UoI initiative would bring value to our industry and business.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idahoan stakeholders.

Strategic workforce development is a high priority at Schweitzer Engineering Laboratories and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cybersecurity expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

In summary, I strongly support the activities described herein. Schweitzer Engineering Laboratories will benefit from this cybersecurity research and workforce development. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. Schweitzer Engineering Laboratories is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

Bob Morris,  
Vice President, National Operations



171 Hwy 95N  
Grangeville, ID 83530  
208-983-4740

March 24, 2016

John McIver, Vice President for Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

Idaho Forest Group is very dependent upon reliable control systems in our facilities. Our state of the art mills are highly automated and power dependent while at risk due to cyber vulnerabilities. Thus we strongly support the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This project will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UI capabilities in cyber security and develop new solutions needed by Idaho industries such as ours.

Idaho Forest Group (IFG) grows, harvests, manufactures, and distributes wood products across the world. We were formed in 2008 when two regional timber interests – Riley Creek Lumber and Bennett Forest Industries – combined their resources. IFG continues to grow and invest in technology, most recently purchasing our mill in Lewiston in 2011, which we are in the midst of retooling. We are headquartered in Coeur d'Alene, heavily invested in the state of Idaho and are one of the largest lumber producers in the United States. In 2014, we were the inaugural recipient of the Zion Bank Idaho Pacesetter award.

We believe that better methods for assessment combined with more resilient systems design will help protect against the negative economic impact currently faced by us and other companies in our industry. We understand the need to focus on cybersecurity research and innovation to ensure reliable electric power and automation systems that our Company depends upon.



Strategic workforce development is a high priority at IFG and across Idaho. This project will strengthen Idaho's security literate workforce by deploying cyber security expertise and growing the technical talent pipeline. We have a strong need in our industry for engineers and scientists educated in Idaho, that want to live and work in Idaho, with these highly sought skills and expertise.

In summary, I strongly support the project and objectives described in this proposal. Idaho Forest Group will benefit from this cybersecurity research and workforce development. Our Company needs future employees with this technical expertise to remain competitive. We are excited to see the State of Idaho and the University of Idaho invest in this project.

Regards,



Shannon Fuchs, Plant Manager  
Grangeville Mill  
Idaho Forest Group

*Idaho Forest Group is an Equal Opportunity Employer and prohibits discrimination against individuals on the basis of race, gender, protected veteran status or disability.*





A Department of the City of Idaho Falls

“A community with its own kind of energy”

March 25, 2016



John McIver, Vice President  
Research and Economic Development  
University of Idaho  
PO Box 44101  
Moscow, ID 83844-3010

Dear Vice President McIver:

Idaho Falls Power strongly supports the University of Idaho’s proposal titled *Modeling Cyber Physical Systems*. This proposal is to develop and support an interdisciplinary core of faculty and staff at the university that will facilitate interdisciplinary research on complex systems in a wide variety of areas. This new core will build on existing capabilities. The goal of the core will be to significantly enhance the capability of the university to conduct interdisciplinary research requiring informatics and data sciences that will greatly benefit our industry and Idaho’s economy.

Idaho Falls Power is a public power system – we are a department of the City of Idaho Falls. There are 22 public power systems in Idaho (municipal and cooperative systems). We are the largest municipal system in Idaho. Even though we are a relatively small utility, we are subject to mandatory, enforceable cyber security standards. We have spent several years building staff knowledge, understanding cyber security risks and best management practices, and growing our capabilities in an area that prior to these standards was largely unknown to utilities – particularly of our size. Cyber security impacts everything we do – systems, processes, and staff from a variety of backgrounds supporting the interdisciplinary approach of the proposal. Today, we consider security and resiliency alongside safety in everything we do.

One characteristic in the proposed approach we like in particular is the faculty they are proposing to hire. Rather than searching to fill classical academic positions, they will be seeking particular critical skill sets. They will be striving to recruit expertise that is needed to address the issues associated with managing data to create information which leads to more informed decisions. We now have the ability to collect huge amounts of data but still struggle to make useful information from it in the most efficient and effective way. This new way of operating has become essential for the electric industry.

---

PO Box 50220  
140 S Capital  
Idaho Falls ID 83405


Phone: 208-612-8438  
Fax: 208-612-8435  
[www.ifpower.org](http://www.ifpower.org)

Mandatory standards have forced the electric industry to evolve in resiliency consideration faster than other industries. But the threat to other industries is as prominent. Those industries will be facing similar challenges as they work to increase their competencies and improve their systems to address risks.

In summary, I strongly recommend that this proposal be funded. I believe the electric industry as well as others will benefit from this workforce. Talent development is a critical need in all industries, especially for engineers and scientists with these types of new and emerging skills and expertise. The electric industry needs these future employees if we are to be competitive and adequately mitigate the risks.

I am pleased to see the State of Idaho investing in such a relevant initiative and happy to support the effort.

Sincerely:



Jackie Flowers  
General Manager



POWER ENGINEERS, INC.

1300 16TH AVENUE, SUITE 200  
CLARKSTON, WA 99403 USA

PHONE 509-758-6029  
FAX 509-758-6145

March 21, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

POWER Engineers strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UI capabilities in cyber security and power systems and develop solutions to address Idaho industries' increasingly vulnerable CPCSs.

As an Idaho industry leader, POWER employs over 2100 people in offices in Idaho, across the country, and in several foreign countries. A number of our employees and employee-owners are proud University of Idaho graduates. As power systems continue to evolve, our clients have come to depend on us increasingly to design secure communication and control systems physically housed in secure substations, power plants, and commercial facilities. We are constantly innovating and advancing, and depend on theoretic and practical advances in cyber and physical system security to meet our clients' and our nation's electric power system reliability objectives. These requirements amplify the need for POWER to focus on cyber security research and deployment through staff knowledgeable in these technical fields. This UI initiative would bring value to our industry and business through advances in the field and education of both new and working engineers.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idaho stakeholders in multiple fields and industries. Moreover, this multidisciplinary, multiagency initiative offers opportunity for better collaboration with Idaho National Laboratory (INL) and the UI which we expect will accelerate economic development in the State through research, development, demonstration and deployment (RDD&D); a process advocated by INL's National Innovation Center. This new way of operating has become essential within our industry.

Strategic workforce development is a high priority at POWER and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

March 21, 2016

In summary, I strongly support the activities described herein. POWER will benefit from this cyber security research and workforce development. Undoubtedly, our industry needs future employees with expertise in cyber and physical security to remain competitive. POWER is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

A handwritten signature in black ink, appearing to read "John J. Kumm". The signature is fluid and cursive, with the first name "John" being the most prominent.

John J. Kumm, P.E.  
Director – SCADA & Analytical Services  
POWER Engineers, Inc.  
Sincerely,

Studies/Log/901-1000



March 16, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

The Community Security Coalition strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UoI capabilities in cyber security and develop solutions to address Idaho industries' increasingly vulnerable CPCSs.

As an Idaho industry leader, the Community Security Coalition is a Pacific Northwest coalition of professionals, interested in advancing cyber security in our community. We have approximately 150 followers from a wide range of businesses from the Pacific Northwest. This UoI initiative would bring value to our industry and business and would directly contribute to the critical needs we hear of on a daily basis.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idahoan stakeholders. Moreover, this multidisciplinary, multiagency initiative offers opportunity for better collaboration with Idaho National Laboratory (INL) and the UI which we expect will accelerate economic development in the State through research, development, demonstration and deployment (RDD&D); a process advocated by INL's National Innovation Center. This new way of operating has become essential within our industry.

Strategic workforce development is a high priority at the Community Security Coalition and across the Pacific Northwest. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.



In summary, I strongly support the activities described herein; our community and the coalition will benefit from this cyber security research and workforce development. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. Kootenai Health is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Please do not hesitate to reach out to me with any questions, comments, or concerns.

Thank you,

A handwritten signature in black ink, appearing to read 'Michael Meline'.

Michael Meline, MsIA, CISSP, CEH, CFE, PCIP, TCNA  
President, Community Security Coalition



2003 Kootenai Health Way  
Coeur d'Alene, ID 83814  
208.625.4600

## KootenaiHealth

March 24, 2016

John McIver, Vice President for Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

I am delighted to write on behalf of Kootenai Health to say how much we support the University of Idaho's (UI) proposal entitled Security Management of Cyber Physical Control Systems (CPCSs). This proposal will strengthen research and educational capacity in the area of security management of CPCSs, computer science (CS) and electrical and computer engineering (ECE). Outcomes from this initiative will accelerate the development of solutions that address the risk posed by security threats toward restoring our economy's health and will lay the firm foundation for future growth.

Kootenai Health would also like to add that research into medical equipment vulnerabilities is a growing concern for the healthcare sector. The Food and Drug Administration has actually issued some guidance for securing these devices this year. In this guidance, they say, "Cybersecurity threats to medical devices are a growing concern. The exploitation of cybersecurity vulnerabilities presents a potential risk to the safety and effectiveness of medical devices. While manufacturers can incorporate controls in the design of a product to help prevent these risks, it is essential that manufacturers also consider improvements during maintenance of devices, as the evolving nature of cyber threats means risks may arise throughout a device's entire lifecycle." Here is a link to this guidance;  
<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm>

We recognize that our legislature faces many competing priorities as it addresses our state's economic situation. We applaud the objectives of this IGEM proposal as an essential investment for protecting our critical infrastructures and improving our capacities in CS, ECE and cybersecurity en route to fostering a workforce that will provide the best value for our economic future.

We look forward to working with you.

Sincerely,

Michael Gaul  
Interim Chief Information Officer



**Avista Utilities**  
1411 East Mission PO Box 3727  
Spokane, Washington 99220-3727  
Telephone 509-489-0500  
Toll Free 800-727-9170



March 25, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

Avista strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UoI capabilities in cyber security and power systems and develop solutions to address Idaho industries' increasingly vulnerable CPCSs.

As an industry leader, Avista employs about 1300 people, around 20% of them in Idaho. We are constantly innovating and advancing, moving into the space of a customer-centric solutions provider. These evolutions in our business amplify the need for Avista to focus on cyber security research and deployment activities. This UoI initiative brings value to our industry and business.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idahoan stakeholders. This multidisciplinary, multiagency initiative offers opportunity for better collaboration with Idaho National Laboratory (INL) and the UI which we expect will accelerate economic development in the State through research, development, demonstration and deployment (RDD&D); a process advocated by INL's National Innovation Center. This new way of operating has become essential within our industry.

Strategic workforce development is a high priority at Avista and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

In summary, I strongly support the activities described herein. Avista will benefit from this cyber security research and workforce development. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. Avista is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

  
Mr. Tracy Rolstad  
Avista System Planning  
(509) 495-4538  
tracy.rolstad@avistacorp.com





HP Inc.  
11311 Chinden Blvd  
Boise, ID 83714  
www.hp.com

March 24, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Mr. McIver:

HP Inc. strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing U of I capabilities in cyber security and develop solutions to address Idaho industries' increasingly vulnerable CPCSs.

As an Idaho industry leader, HP Inc. employs ~50K people around the world, about ~2.5K of them in Idaho. As consumer products continue to evolve, our customers' bases and demands are shifted. We are constantly innovating and advancing into new markets, thoughtfully moving into the space of a customer-centric solutions provider. These evolutions in our business amplify the need for HP Inc. to focus on cyber security research and deployment activities. This U of I initiative would bring value to our industry, while also adding more graduates with expertise in this area to the local talent pipeline.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idahoan stakeholders.

Strategic workforce development is a high priority at HP Inc. and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

In summary, HP Inc. strongly supports the U of I proposal for Security Management of CPCSs. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. HP Inc. is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

A handwritten signature in black ink, appearing to be 'Jim Nottingham', written over a horizontal line.

Jim Nottingham, VP Value Business

March 28, 2016

John McIver, Vice President  
Research and Economic Development  
University of Idaho  
875 Perimeter Drive MS 3010  
Moscow, ID 83844-3010

Dear Vice President McIver:

Idaho Power strongly supports the University of Idaho's (UI) proposal entitled *Security Management of Cyber Physical Control Systems (CPCSs)*. This proposal will strengthen research and educational capacity in the area of security management of CPCSs. Outcomes from this initiative will build upon existing UI capabilities in cyber security and power systems and develop solutions to address Idaho industries' CPCSs vulnerability to the increasing cyber-attacks perpetrated worldwide.

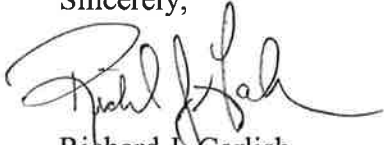
As an Idaho industry enabler and leader, Idaho Power employs 2,011 people, the majority of whom live and work in Idaho. Idaho Power utilizes a significant amount of technology that is integral to the operation of the facilities that provide safe, reliable, and cost competitive utility service to the company's 515,763 customers. Physical and Cyber security is a priority for Idaho Power. This UI initiative would bring value to our industry and business by providing research and deployment strategies to address the threat environment today and into the future.

We support, in particular, the new faculty the UI proposes to hire. They will be seeking critical skill sets; striving to recruit expertise to enable transformative solutions specifically targeted to address pervasive security management needs. We agree that better methods for assessment combined with more resilient systems design will pave the way in protecting against potentially immense economic impact currently faced by Idaho stakeholders. Moreover, this multidisciplinary, multiagency initiative offers opportunity for better collaboration with Idaho National Laboratory (INL) and the UI which we expect will accelerate economic development in the State through research, development, demonstration and deployment (RDD&D); a process advocated by INL's National Innovation Center. This new way of operating has become essential within our industry.

Strategic workforce development is a high priority at Idaho Power and across Idaho. This initiative will certainly strengthen Idaho's high-tech workforce by deploying cyber security expertise and improving the computer science pipeline. Talent development is a critical need in our industry, especially for engineers and scientists with these highly sought emerging skills and expertise.

In summary, we strongly support the activities described herein. Idaho Power will benefit from this cyber security research and workforce development. Undoubtedly, our industry needs future employees with expertise in security management to remain competitive. Idaho Power is pleased to see the State of Idaho investing in such a relevant and impactful initiative.

Sincerely,

A handwritten signature in black ink, appearing to read "Rich Garlish", written in a cursive style.


Richard J. Garlish  
General Manager Security, Risk  
& Compliance  
Idaho Power Company

A handwritten signature in black ink, appearing to read "Jeff Glenn", written in a cursive style.

Jeff Glenn  
Vice President and CIO  
Idaho Power Company

## Appendix D: Budget Summary and Justification

SUMMARY PROPOSAL BUDGET				Three-Year Summary		
Name of Institution: University of Idaho						
Name of Project Director: Larry Stauffer						
A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)						
Name/ Title		Salary/Rate of Pay	Fringe	Dollar Amount Requested		
Larry Stauffer, Lead PI and Project Director 5% FY	Base Salary: \$208,060	\$ 32,155	31.1%	\$ 42,155		
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$ 14,626	31.1%	\$ 19,275		
TT, Associate Prof, Security, CS AY	Base Salary: \$115,000	\$290,950	31.1%	\$ 381,435		
TT, Assistant Prof, Power Security, EE AY	Base Salary: \$ 95,000	\$240,350	31.1%	\$ 315,099		
TT, Assistant Prof, Physical Security, CS Idaho Falls AY	Base Salary: \$ 95,000	\$192,850	31.1%	\$ 252,826		
TT, Assistantt Prof, SCADA, Power Systems, Idaho Falls AY	Base Salary: \$ 95,000	\$192,8502	31.1%	\$ 252,826		
Graduate Student RAs		\$ 150,000	2.0%	\$ 153,000		
<b>% OF TOTAL BUDGET:</b>		67.485%	<b>SUBTOTAL:</b>		\$ 1,416,516	
B. EQUIPMENT: (List each item with a cost in excess of \$1000.00.)						
Item/Description				Dollar Amount Requested		
VT Equipment (improved VT facilities, Moscow, Boise, and Idaho Falls) in Year One				\$ 117,000		
Enhance Power Lab (computing and test equipment, software) in Year One				\$ 180,000		
<b>SUBTOTAL:</b>				\$ 297,000		
C. TRAVEL:						
Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging	Per Diem	Dollar Amount Requested
Attend Conferences						\$ 18,500
Visit Agencies						\$ 10,000
Visit Industry						\$ 10,000
<b>SUBTOTAL:</b>						\$ 38,500
D. Participant Support Costs:						
1. Stipends						
2. Other						
<b>SUBTOTAL:</b>						

E. Other Direct Costs:		Dollar Amount Requested
1. Materials and Supplies (includes research supplies and software)		\$ 34,200
2. Publication Costs/Page Charges		\$
3. Consultant Services (Include Travel Expenses)		\$
4. Computer Services		\$
5. Subcontracts		\$
6. Other (specify nature & breakdown if over \$1000)		
Start-up/search funds—specified by hire to initiate research \$205,600		
Moving expenses in year one (maximum 10% of bases salary) \$ 21,000		\$ 312,800
Moving expenses in year two (maximum 10% of bases salary) \$ 19,000		
Grad student tuition/fees \$ 67,200		
SUBTOTAL:		\$ 347,000
J. Total Costs: (Add subtotals, sections A through I)		\$ 2,099,016
K. Amount Requested:		\$ 2,099,016
Project Director's Signature: 		Date: 04/01/2016

INSTITUTIONAL AND OTHER SECTOR SUPPORT (add additional pages as necessary)	
A. INSTITUTIONAL / OTHER SECTOR DOLLARS	
Source / Description	Amount
Internship opportunities to COE students from industry partners.	TBD
Industry partners will provide time and talent for assessments pertaining to CPCS Security Management.	TBD
Faculty start-up offers are negotiated to be \$100,000 to \$300,000 in computer science to attract quality assistant or associate professor candidates. The UI will likely be providing \$200,000 to \$400,000 of additional funds over three-years for the new faculty start-up packages. Faculty start-up Includes funds for student support, summer salary, individual travel, supplies, software, etc.	\$200,000 to \$400,000
B. FACULTY / STAFF POSITIONS	
Description	
The Co-PIs in this project will provide support in managing and executing the project plan including limited assistance from outside faculty including the CSDS. The COE including the CS and ECE Departments will offer both Administrative and Sys-admin (IT) support.	
C. CAPITAL EQUIPMENT	
Description	
There exists VTC facilities/equipment and technical personnel that support the UI and COE that will be utilized on an as needed basis. The equipment described in Section 4 and Appendix A (e.g., PAL, RADICL and ICCL) will also be provided as needed and/or upgraded to ensure the successful implementation of this project including existing computers, printers and other general purpose office equipment.	
D. FACILITIES & INSTRUMENTATION (Description)	
Please see relevant comments above in "C. CAPITAL EQUIPMENT"	

### **Budget Summary**

We request \$2,099,016 to cover most project expenses over a three year period. The rest of the expenses will be provided by the university. The above table provides a three-year budget summary for FY17, FY18, and FY19. The following provides a budget justification and budget details for years one, two, and three.

### **Budget Justification Details**

**Larry Stauffer, COE Dean and Lead PI:** Total requested funds in the amount of \$32,155 at 5% effort each year to provide overall project management and ensure project success. Base salary is \$208,060 and includes an expected 3% increase for year one and assuming a 3% increase in years two and three.

**Fredrick Sheldon, Chair CS Dept and Co-PI:** Total requested funds in the amount of \$14,626 at 10% effort in year one to provide technical management of the project. He will be responsible for hiring the personnel and delegating responsibilities to existing faculty and staff to assure successful execution of the project plan. Base salary is \$146,260 and includes an expected 3% increase for year one.

**Tenure Track, Associate Professor, Security, Computer Science:** Total requested funds in the amount of \$290,950. In year one \$57,500 spring semester; in year two \$115,000 at 100% effort; and in year three at 100% effort \$118,450. Base salary is \$115,000 assuming a 3% increase in year three. This person will have expertise in cyber physical control system detection and penetration modeling methods.

**Tenure Track, Assistant Professor, Power Systems Planning and Power System Security, Electrical Engineering:** Total requested funds in the amount of \$240,350. In year one \$47,500 spring semester; in year two \$95,000 at 100% effort; and in year three \$97,850 at 100% effort.



Base salary is \$115,000 assuming a 3% increase in year three. This person will have expertise and experience with power system planning and vulnerability analysis.

**Tenure Track, Assistant Professor, Physical Security, Computer Science in Idaho Falls:**

Total requested funds in the amount of \$192,850. In year two \$95,000 at 100% effort; and in year three \$97,850 at 100% effort. Base salary is \$95,000 assuming a 3% increase in year three.

This person will have expertise in cyber physical control system vulnerability assessment methods.

**Tenure Track, Assistant Professor, Advanced SCADA Systems for Power Systems in Idaho**

**Falls:** Total requested funds in the amount of \$192,850. In year two \$95,000 at 100% effort; and in year three \$97,850 at 100% effort. Base salary is \$95,000 with a 3% increase in year three. This person will have expertise and experience with SCADA and vulnerability assessment of power control and communication systems.

**Graduate Students:** Total requested funds in the amount of \$150,000. In year one \$50,000; in year two \$50,000; and in year three \$50,000. These funds are to support graduate student research assistantships and support faculty research efforts.

**Fringe Benefits:** Total requested funds in the amount of \$302,736. The faculty consolidated fringe benefit rate is 31.1% for a total of \$299,736 and the student consolidated fringe rate is 2% for a total of \$3,000.

**Equipment:** Total requested funds in the amount of \$297,000 for:

**\$117,000 Total in Year One for VT Equipment for Remote Course Delivery for**

**Moscow, Boise and Idaho Falls. The following are components:**

- CISCO/Tandberg Video Conference Unit (2-locations, \$10,000 at  
each location) \$ 20,000

• Rear camera and cables (2-locations, \$1,000 at each location)	\$ 2,000
• Microphones and cables (2-locations @ \$5,000 at each location)	\$ 10,000
• 8-Displays (2-locations, \$10,000 at each location)	\$ 20,000
• Installation, retrofitting, and sound proofing (2-locations, \$10,000 at each location)	\$ 20,000
• Speakers (2-locations, \$2,500 at each location)	\$ 5,000
• Instructor station and operating console (2-locations, \$10,000 at each location)	<u>\$ 20,000</u>
	\$ 117,000

**\$180,000 Total in Year One for Enhanced Power Lab. The following are components:**

• Substation remote terminal units from different vendors (4)	\$ 8,000
• Substation real-time automation controllers (2)	\$ 8,000
• Protective relays, power equipment controllers (6)	\$ 20,000
• Integrated substation communication controllers	\$ 6,000
• Managed network switches	\$ 8,000
• Computers and monitors (4)	\$ 8,000
• VPN server (allow secure access for non-UI personnel)	\$ 5,000
• Standard 42U equipment racks (4)	\$ 8,000
• Power and communication wiring plus installation	\$ 6,000
• Expanded realtime digital simulation analog I/O card	\$ 1,800
• Expanded real time digital simulation digital I/O cards	\$ 2,700



- Upgraded RTDS GTNET interface cards plus firmware \$ 25,000
  - Upgrade real time digital simulator processing capability \$ 73,500
- \$ 180,000

**Travel:** Total requested funds in the amount of \$38,500 to attend conferences (\$18,000); to visit agencies (\$10,000); and to visit industry (\$10,000).

**Materials and Supplies:** Total requested funds in the amount of \$34,200 for items such as laboratory consumables, software, and misc. supplies.

**Start-Up/Search Funds:** Total requested funds in the amount of \$205,600 to attract quality faculty candidates and help them establish a competitive research program. The faculty have some discretion on how these are budgeted pending approval of the university administration. Typical budget items are for student support, travel, supplies, software, etc for project expenses over a three year period.

**Moving Expenses:** Total requested funds in the amount of \$40,000 to support moving expenses for the new tenured track faculty positions. Maximum moving expenses for each new position is 10% of base salary. In year one, moving expenses are \$21,000 and in year two \$19,000.

**Grad Student Tuition:** Total requested funds in the amount of \$67,200. In year one \$21,300; in year two \$22,400, and in year three \$23,500. There is a 5% increase in years two and three.

## **Institutional and Other Sector Support**

### **Institutional/Other Sector Dollars:**

- Dollar amount TBD over three-years for internship opportunities with industry.
- Dollar amount TBD over three-years from industry partners to provide time and talent for assessments pertaining to CPCS Security Management.

- \$200,000 to \$400,000 over three-years. Faculty start-up offers are negotiated to be \$100,000 to \$300,000 in computer science to attract quality assistant or associate professor candidates. The UI will likely be providing \$200,000 to \$400,000 of additional funds over three-years for the new faculty start-up packages. Faculty start-up includes funds for student support, summer salary, individual travel, supplies, software, etc.


**Facility/Staff Positions:** The Co-PIs in this project will provide support in managing and executing the project plan including limited assistance from outside faculty including the CSDS. The COE including the CS and ECE Departments will offer both Administrative and Sys-admin (IT) support.

**Capital Equipment:** There exists VTC facilities/equipment and technical personnel that support the UI and COE that will be utilized on an as needed basis. The equipment described in Section 4 and Appendix A (e.g., PAL, RADICL and ICCL) will also be provided as needed and/or upgraded to ensure the successful implementation of this project including existing computers, printers and other general purpose office equipment.


**Facilities & Instrumentation:** See relevant comments in the “Capital Equipment” section.

**The following tables provide details for FY17 Year One, FY18 Year Two, and FY19 Year Three.**


SUMMARY PROPOSAL BUDGET				FY17 Year One		
Name of Institution: University of Idaho						
Name of Project Director: Larry Stauffer						
A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)						
Name/ Title		Salary/Rate of Pay	Fringe	Dollar Amount Requested		
Larry Stauffer, Lead PI and Project Director 5% FY	Base Salary: \$208,060	\$ 10,403	31.1%	\$ 13,637		
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$ 14,626	31.1%	\$ 19,175		
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$ 57,500	31.1%	\$ 75,383		
TT, Associate Prof, Security, CS AY	Base Salary: \$115,000	\$ 47,500	31.1%	\$ 62,273		
TT, Assistant Prof, Power Security, EE AY	Base Salary: \$ 95,000	\$ -	31.1%	\$ -		
TT, Assistant Prof, Physical Security, CS Idaho Falls AY	Base Salary: \$ 95,000	\$ -	31.1%	\$ -		
Graduate Student RAs		\$ 50,000	2.0%	\$ 51,000		
<b>% OF TOTAL BUDGET:</b>		Year One = 31.640%	<b>SUBTOTAL:</b>		\$ 221,468	
B. EQUIPMENT: (List each item with a cost in excess of \$1000.00.)						
Item/Description				Dollar Amount Requested		
VT Equipment (improved VT facilities, Moscow, Boise, and Idaho Falls) in Year One				\$ 117,000		
Enhance Power Lab (computing and test equipment, software) in Year One				\$ 180,000		
<b>SUBTOTAL:</b>				\$ 297,000		
C. TRAVEL:						
Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging	Per Diem	Dollar Amount Requested
Attend Conferences						\$ 10,500
Visit Agencies						\$ 4,000
Visit Industry						\$ 4,000
<b>SUBTOTAL:</b>						\$ 18,500
D. Participant Support Costs:						
1. Stipends						
2. Other						
<b>SUBTOTAL:</b>						

E. Other Direct Costs:		Dollar Amount Requested
1. Materials and Supplies (includes research supplies and software)		\$ 27,700
2. Publication Costs/Page Charges		\$
3. Consultant Services (Include Travel Expenses)		\$
4. Computer Services		\$
5. Subcontracts		\$
6. Other (specify nature & breakdown if over \$1000)		
Start-up/search funds—specified by hire to initiate research	\$ 93,000	
Moving expenses in year one (maximum 10% of bases salary)	\$ 21,000	
Grad student tuition/fees	\$ 21,300	\$ 139,300
SUBTOTAL:		\$ 163,000
J. Total Costs: (Add subtotals, sections A through I)		\$ 699,968
K. Amount Requested:		\$ 699,968
Project Director's Signature: 		Date: 04/01/2016

SUMMARY PROPOSAL BUDGET				FY18 Year Two		
Name of Institution: University of Idaho						
Name of Project Director: Larry Stauffer						
A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)						
Name/ Title	Salary/Rate of Pay	Fringe	Dollar Amount Requested			
Larry Stauffer, Lead PI and Project Director 5% FY	Base Salary: \$208,060 \$ 10,715	31.1%	\$ 14,047			
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260 \$ -	31.1%	\$ -			
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260 \$115,000	31.1%	\$ 150,765			
TT, Associate Prof, Security, CS AY	Base Salary: \$115,000 \$ 95,000	31.1%	\$ 124,545			
TT, Assistant Prof, Power Security, EE AY	Base Salary: \$ 95,000 \$ 95,000	31.1%	\$ 124,545			
TT, Assistant Prof, Physical Security, CS Idaho Falls AY	Base Salary: \$ 95,000 \$ 95,000	31.1%	\$ 124,545			
Graduate Student RAs	\$ 50,000	2.0%	\$ 51,000			
<b>% OF TOTAL BUDGET:</b>		Year Two = 84.273%	<b>SUBTOTAL:</b>	\$ 589,447		
B. EQUIPMENT: (List each item with a cost in excess of \$1000.00.)						
Item/Description				Dollar Amount Requested		
<b>SUBTOTAL:</b>						
C. TRAVEL:						
Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging	Per Diem	Dollar Amount Requested
Attend Conferences						\$ 5,000
Visit Agencies						\$ 2,500
Visit Industry						\$ 2,500
<b>SUBTOTAL:</b>						\$ 10,000
D. Participant Support Costs:					Dollar Amount Requested	
1. Stipends						
2. Other						
<b>SUBTOTAL:</b>						

E. Other Direct Costs:		Dollar Amount Requested
1. Materials and Supplies (includes research supplies and software)		\$ 6,000
2. Publication Costs/Page Charges		\$
3. Consultant Services (Include Travel Expenses)		\$
4. Computer Services		\$
5. Subcontracts		\$
6. Other (specify nature & breakdown if over \$1000)		
Start-up/search funds—specified by hire to initiate research		\$ 52,600
Moving expenses in year two (maximum 10% of bases salary)		\$ 19,000
Grad student tuition/fees		\$ 22,400
SUBTOTAL:		\$ 100,000
J. Total Costs: (Add subtotals, sections A through I)		\$ 699,447
TOTAL:		
100		
K. Amount Requested:		TOTAL: \$ 699,447
Project Director's Signature: 		Date: 04/01/2016

SUMMARY PROPOSAL BUDGET				FY19 Year Three
Name of Institution: University of Idaho				
Name of Project Director: Larry Stauffer				
A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)				
Name/ Title	Salary/Rate of Pay	Fringe	Dollar Amount Requested	
Larry Stauffer, Lead PI and Project Director 5% FY	Base Salary: \$208,060	\$ 11,037	31.1%	\$ 14,470
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$ -	31.1%	\$ -
Fredrick Sheldon, Co-PI 10% Year One AY	Base Salary: \$146,260	\$118,450	31.1%	\$ 155,288
TT, Associate Prof, Security, CS AY	Base Salary: \$115,000	\$118,450	31.1%	\$ 128,281
TT, Assistant Prof, Power Security, EE AY	Base Salary: \$ 95,000	\$118,450	31.1%	\$ 128,281
TT, Assistant Prof, Physical Security, CS Idaho Falls AY	Base Salary: \$ 95,000	\$118,450	31.1%	\$ 128,281
Graduate Student RAs		\$ 50,000	2.0%	\$ 51,000
<b>% OF TOTAL BUDGET:</b>		Year Three = 86.564%		<b>SUBTOTAL:</b>
				\$ 605,601
B. EQUIPMENT: (List each item with a cost in excess of \$1000.00.)				
Item/Description				Dollar Amount Requested
<b>SUBTOTAL:</b>				
C. TRAVEL:				
Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging
				Per Diem
Attend Conferences				
Visit Agencies				
Visit Industry				
<b>SUBTOTAL:</b>				\$ 10,000
D. Participant Support Costs:				
1. Stipends				
2. Other				
<b>SUBTOTAL:</b>				

E. Other Direct Costs:		Dollar Amount Requested
1. Materials and Supplies (includes research supplies and software)		\$ 500
2. Publication Costs/Page Charges		\$
3. Consultant Services (Include Travel Expenses)		\$
4. Computer Services		\$
5. Subcontracts		\$
6. Other (specify nature & breakdown if over \$1000)		
Start-up/search funds—specified by hire to initiate research \$ 60,000		\$ 83,500
Grad student tuition/fees \$ 23,500		
SUBTOTAL:		\$ 84,000
J. Total Costs: (Add subtotals, sections A through I)		\$ 699,601
TOTAL:		
K. Amount Requested:		\$ 699,601
Project Director's Signature: 		Date: 04/01/2016